U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371 AND 37 CFR 1.491

ATTORNEY DOCKET NO.	
P3714US	
U.S. APPLICATION NO.	
Unassigned	

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR2009/051228	26 June 2009 (26.06.2009)	30 June 2008 (30.06.2008)

TITLE OF INVENTION
A METHOD OF RECEIVING A DATA PACKET COMING IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE, AND AN ASSOCIATED HOME GATEWAY

APPLICANT(S) FOR DO/EO/US
BOUCADAIR, Mohamed ; GRIMAULT, Jean-Luc

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371 and 37 CFR 1.491.

2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371 and 37 CFR 1.491.

3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)).

4. ☐ The US has been elected (PCT Article 31).

5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).

6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).

7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

11. Nucleotide and/or Amino Acid Sequence Submission
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper Copy
   c. ☐ Statement verifying identity of above copies

Items 12 to 19 below concern other document(s) or information included:

12. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
   ☐ Form PTO-1449
   ☐ Copies of Listed Documents

13. ☐ An assignment for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

14. ☒ A FIRST preliminary amendment.
   ☐ A SECOND or SUBSEQUENT preliminary amendment.

15. ☐ A substitute specification.

16. ☐ A change of power of attorney and/or address letter.

17. ☒ Application Data Sheet Under 37 CFR 1.76

18. ☐ Return Receipt Postcard

19. ☒ Other items or information: Replacement Abstract; Copy of International Search Report; Copy of Written Opinion; Certification of Translation

Juniper Exhibit 1002, page 1

U.S. APPLICATION NO.	INTERNATIONAL APPLICATION NO.	ATTORNEY DOCKET NO.
Unassigned	PCT/FR2009/051228	P3714US

20. The following fees are submitted:	Calculations	PTO Use Only
☒ a) Basic national fee……$330.00	$330.00	
☒ b) Examination fee If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)……$0.00 All other situations ……..$220.00	$220.00	
☒ c) Search fee If the written opinion of the ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)……$0.00 Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority…… $100.00 International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB……..$430.00 All other situations……$540.00	$430.00	
TOTAL OF ABOVE CALCULATIONS =	**$980.00**	

☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing or computer program listing filed in an electronic medium). The fee is **$250.00** for each additional 50 sheets of paper or fraction thereof.

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round **up** to a whole number)	RATE		
-100=	/50=		x **$270.00**	$0.00	

Surcharge of **$130.00** for furnishing the oath or declaration later than 30 months from the earliest claimed priority date (37 CFR 1.492(e)). $0.00

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total Claims	10 -20=	0	x $52.00	$0.00	
Independent Claims	2 - 3 =	0	x $220.00	$0.00	
☐ Multiple Dependent Claim(s) (if applicable)			+ $390.00	$0.00	

TOTAL OF ABOVE CALCULATIONS=	$980.00	
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.	$	
SUBTOTAL=	$980.00	
Processing fee of **$130.00** for furnishing English Translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date.	$	
TOTAL NATIONAL FEE=	$980.00	
Fee for recording the enclosed assignment. The assignment must be accompanied by an appropriate cover sheet. **$40.00** per property +	$	
TOTAL FEE ENCLOSED=	$980.00	
	Amount to be: refunded	$
	charged:	$

a. ☐ A check in the amount of $ to cover the above fee is enclosed.
b. ☒ Please charge Deposit Account No. 07-0181 in the amount of $980.00 to cover the above fees. A duplicate copy of this sheet is enclosed.
c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 07-0181. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Customer Number: 08968
Drinker Biddle & Reath LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698

/brian c. rupp/

Brian C. Rupp, Registration No. 35,665

Date: December 29, 2010

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371 AND 37 CFR 1.491

ATTORNEY DOCKET NO.: P3714US

U.S. APPLICATION NO.: Unassigned

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/FR2009/051228	26 June 2009 (26.06.2009)	30 June 2008 (30.06.2008)

TITLE OF INVENTION
A METHOD OF RECEIVING A DATA PACKET COMING IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE, AND AN ASSOCIATED HOME GATEWAY

APPLICANT(S) FOR DO/EO/US
BOUCADAIR, Mohamed ; GRIMAULT, Jean-Luc

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371 and 37 CFR 1.491.

2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371 and 37 CFR 1.491.

3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)).

4. ☐ The US has been elected (PCT Article 31).

5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is attached hereto (required only if not communicated by the International Bureau).
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).

6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154(d)(4).

7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).

9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).

10. ☐ An English language translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

11. Nucleotide and/or Amino Acid Sequence Submission
   a. ☐ Computer Readable Form (CRF)
   b. Specification Sequence Listing on:
      i. ☐ CD-ROM or CD-R (2 copies); or
      ii. ☐ Paper Copy
   c. ☐ Statement verifying identity of above copies

Items 12 to 19 below concern other document(s) or information included:

12. ☐ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
   ☐ Form PTO-1449
   ☐ Copies of Listed Documents

13. ☐ An assignment for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

14. ☒ A FIRST preliminary amendment.
   ☐ A SECOND or SUBSEQUENT preliminary amendment.

15. ☐ A substitute specification.

16. ☐ A change of power of attorney and/or address letter.

17. ☒ Application Data Sheet Under 37 CFR 1.76

18. ☐ Return Receipt Postcard

19. ☒ Other items or information: Replacement Abstract; Copy of International Search Report; Copy of Written Opinion; Certification of Translation

U.S. APPLICATION NO.	INTERNATIONAL APPLICATION NO.	ATTORNEY DOCKET NO.
Unassigned	PCT/FR2009/051228	P3714US

20. The following fees are submitted:	Calculations	PTO Use Only
☒ a) Basic national fee……$330.00	$330.00	
☒ b) Examination fee If the written opinion prepared by ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)……$0.00 All other situations ……..$220.00	$220.00	
☒ c) Search fee If the written opinion of the ISA/US or the international preliminary examination report prepared by IPEA/US indicates all claims satisfy provisions of PCT Article 33(1)-(4)……$0.00 Search fee (37 CFR 1.445(a)(2)) has been paid on the international application to the USPTO as an International Searching Authority…… $100.00 International Search Report prepared by an ISA other than the US and provided to the Office or previously communicated to the US by the IB……..$430.00 All other situations……$540.00	$430.00	
TOTAL OF ABOVE CALCULATIONS =	**$980.00**	

☐ Additional fee for specification and drawings filed in paper over 100 sheets (excluding sequence listing or computer program listing filed in an electronic medium). The fee is **$250.00** for each additional 50 sheets of paper or fraction thereof.

Total Sheets	Extra Sheets	Number of each additional 50 or fraction thereof (round **up** to a whole number)	RATE		
-100=	/50=		x **$270.00**	$0.00	

Surcharge of **$130.00** for furnishing the oath or declaration later than 30 months from the earliest claimed priority date (37 CFR 1.492(e)). $0.00

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total Claims	10 -20=	0	x $52.00	$0.00	
Independent Claims	2 - 3 =	0	x $220.00	$0.00	
☐ Multiple Dependent Claim(s) (if applicable)			+ $390.00	$0.00	

TOTAL OF ABOVE CALCULATIONS=	$980.00	
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.	$	
SUBTOTAL=	$980.00	
Processing fee of **$130.00** for furnishing English Translation later than ☐ 20 ☐ 30 months from the earliest claimed priority date.	$	
TOTAL NATIONAL FEE=	$980.00	
Fee for recording the enclosed assignment. The assignment must be accompanied by an appropriate cover sheet. **$40.00** per property +	$	
TOTAL FEE ENCLOSED=	$980.00	
	Amount to be: refunded	$
	charged:	$

a. ☐ A check in the amount of $ to cover the above fee is enclosed.
b. ☒ Please charge Deposit Account No. 07-0181 in the amount of $980.00 to cover the above fees. A duplicate copy of this sheet is enclosed.
c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 07-0181. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Customer Number: 08968
Drinker Biddle & Reath LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698

/brian c. rupp/

Brian C. Rupp, Registration No. 35,665

Date: December 29, 2010

Application Data Sheet

APPLICATION INFORMATION

Application Number::	
Filing Date::	December 29, 2010
Application Type::	Regular
Subject Matter::	Utility
Suggested classification::	
Suggested Group Art Unit::	
CD-ROM or CD-R?::	None
Number of CD Disks::	
Sequence Submission?::	
Computer Readable Form (CRF)?::	No
Number of Copies of CRF::	
Title::	A METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE, AND AN ASSOCIATED HOME GATEWAY
Attorney Docket Number::	P3714US
Request for Early Publication?::	No
Request for Non-Publication?::	No
Suggested Drawing Figure::	Fig. 3
Total Drawing Sheets::	9
Small Entity?::	No
Latin Name::	
Variety denomination name::	
Petition Included?::	No
Petition Type::	
Licensed US Govt. Agency::	
Contract or Grant Numbers::	
Secrecy Order in Parent Appl.?::	No

APPLICANT INFORMATION

Applicant Authority Type::	Inventor
Primary Citizenship Country::	FR
Status::	Full Capacity
Given Name::	Mohamed
Middle Name::	
Family Name::	Boucadair
City of Residence::	Rennes
State or Prov. of Residence::	
Country of Residence::	France
Street of mailing address::	1, Square Louis Harel de la Noë
City of mailing address::	Rennes
State or Province of mailing address::	
Country of mailing address::	France
Postal or Zip Code of mailing address::	35000

Applicant Authority Type::	Inventor
Primary Citizenship Country::	FR
Status::	Full Capacity
Given Name::	Jean-Luc
Middle Name::	
Family Name::	Grimault
City of Residence::	Mondeville
State or Prov. of Residence::	
Country of Residence::	France
Street of mailing address::	7, Impasse de l'Europe
City of mailing address::	Mondeville
State or Province of mailing address::	
Country of mailing address::	France
Postal or Zip Code of mailing address::	14120

CORRESPONDENCE INFORMATION

Correspondence Customer Number::	08968
Phone:	312-569-1000
Fax:	312-569-3000
E-mail Address:	ipdocketchicago@dbr.com

REPRESENTATIVE INFORMATION

Representative Customer Number: 08968

Representative Designation:	Registration Number:	Representative Name:

DOMESTIC PRIORITY INFORMATION

Application:	Continuity Type:	Parent Application:	Parent Filing Date:
This application	National Stage of	PCT/FR2009/051228	26 June 2009

FOREIGN APPLICATION INFORMATION

Country:	Application Number:	Filing Date:	Priority Claimed
France	08 54405	30 June 2008	Yes

ASSIGNEE INFORMATION

Assignee name::	France Telecom
Street of mailing address::	6 place d'Alleray
City of mailing address::	Paris
State or Province of mailing address::	
Country of mailing address::	France
Postal or Zip Code of mailing address::	75015

A METHOD OF RECEIVING A DATA PACKET IN AN IPv6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

FIELD OF THE INVENTION

The field of the invention is that of telecommunications networks, in particular IP telecommunications networks transporting data packets from a source equipment identified by a source address to a destination equipment identified by a destination address.

This kind of telecommunications network combines a plurality of equipments, connections, and functions dedicated to transporting data coming from terminal equipments connected to the network. In particular, the transport functions may be implemented by activating routing and transmission protocols. A telecommunications network administered by an operator is also referred to as a domain.

An IP connectivity service provider deploys a dedicated architecture to enable terminal equipment users to be contacted. Access to the IP connectivity service is managed by the service provider using the telecommunications network of an operator to route data packets sent by the terminal equipments to their final destinations. In some circumstances, said service provider is also the telecommunications network operator.

This kind of service provider assigns an IP address, generally a public IP address, to a home gateway between a home network and the public network or IP domain of the operator. The home gateway generally assigns private IP addresses to the terminals of its home network.

Below, the expression "home gateway" refers to any equipment for interconnecting a private network and a network operated by a service provider, the private network being either a home network or a business network.

The network operated by the service providers is also referred to below as a public network.

Located on the path of data packets between a terminal of its private home network and the IP domain of the operator, the home gateway includes, as known in the art, a table in which it associates the private IP address and the port associated with that terminal with a public IP address of Ipv4 type and, with a port of the same gateway on the public network.

This table is known to the person skilled in the art as a NAT (network address translation) table. There are different types of network address translation e.g. symmetrical, Full Cone, and Port Restricted.

It is commonly accepted in the IP service provider community that IPv4 public addresses are going to run out. To avoid this problem the community has in the past taken action leading to the definition of a new protocol known as the Internet Protocol version 6 (IPv6). This new version of the Internet Protocol provides a large number of IP addresses and a hierarchical routing mechanism offering improved performance. Providers are not indifferent to warnings recently emanating from the Internet Engineering Task Force (IETF), notably in reports presented to the Global Routing Operations Working Group (GROW) concerning the risk of the Internet Assigned Numbers Authority (IANA) running out of IPv4 addresses by the end of 2010.

However, in practice, this IPv6 solution has not as yet been widely adopted by operators, for financial, strategic, and technical reasons linked to managing the complexity of transition and migration.

To limit the number of IPv4 public addresses necessary to provide an IP connectivity service to an installed base of clients, a solution known as Double NAT or Operator NAT has been proposed and implemented. It entails activating a NAT function within the telecommunications network of the operator so that the

home gateways use a private address (instead of a public address) in their outgoing NAT tables. Thus the Operator NAT function translates home gateway private addresses into public addresses, which enables a service provider to economize on a non-negligible number of IPv4 public addresses required to provide the IP connectivity service.

DRAWBACKS OF THE PRIOR ART

The Operator NAT solution has drawbacks including:

· IP data packet processing is made more complex; because of the introduction of a second level of address translation, data packets must be modified twice;

· the necessity to adapt the implementation of conventional Application Level Gateway (ALG) signaling protocols such as the Domain Name System (DNS) protocol, the File Transfer Protocol (FTP), and the Session Initiation Protocol (SIP). Taking the SIP, for example, to keep the NAT table of a home gateway up to date, setting up and maintaining a voice over IP session requires frequent exchanges of signaling between the user terminal and the public network via re-registration requests so that the NAT sessions remain active; with Double NAT, such a mechanism must also be provided in the equipment hosting the Operator NAT function; furthermore, the public address and the public port actually being used for the terminal must be communicated to the SIP application;

· the public telecommunications network operator offering a degraded IP connectivity service can only be deplored, in particular because functions such as port forwarding and DynDNS are not supported in Operator NAT.

What is more, such a solution cannot prevent, but can only delay, the phenomenon of IPv4 addresses running out. It is therefore necessary to provide for a changeover to IPv6 in the medium term. Such a changeover will necessarily lead to a period of transition during

which IPv6 domains will have to interconnect with IPv4 domains. There is no provision in current networks for facilitating such interconnection efficiently, optimally, and without instantiation of additional states in the network nodes used to provide an IP connectivity service.

Nor is there any provision for progressive migration from IPv4 addressing to IPv6 addressing based on simple interconnection mechanisms between an IPv6 and an IPv4 domain, in particular solutions that do not require client terminals implementing both IPv4 and IPv6.

SUMMARY OF THE INVENTION

The invention improves upon the above situation by providing a receiving method for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet including an IPv6 destination address and an IPv6 source address.

According to the invention, said method is executed in a home gateway adapted to connect a user terminal to said IPv6 domain and includes the following steps:

· identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address and a destination port number;

· if necessary, regularizing at least one address of the data packet by replacing said address, the replacement process belonging to a group comprising replacement of a constructed address with a native address and replacement of a native address with a constructed address, and modifying the data packet using the regularized address; and

· routing the modified data packet to its destination.

In the context of migration from IPv4 to IPv6, consider a first terminal equipment of an IPv4 domain that can send and receive only IPv4 data packets. In parallel with this, a second terminal equipment of the IPv6 domain can send and receive only IPv6 data packets.

According to the invention, if one of these equipments is seeking to send a data packet to the other, it uses its own protocol, but the data is routed in the IPv6 domain using the IPv6 protocol.

The data packet is therefore sent in IPv4 or IPv6, transformed if necessary into an IPv6 data packet to route it in the IPv6 domain, and if necessary transformed back into an IPv4 data packet.

Such transformation relies on a mechanism for constructing an IPv6 destination address from an IPv4 destination address of the first terminal by concatenating an operator prefix, this IPv4 destination address, and the packet destination port number. Considered the situation where an equipment for interconnecting the IPv6 domain and the IPv4 domain constructs an IPv6 destination address from the IPv4 destination address and the destination port. The constructed IPv6 destination address can be routed in the IPv6 domain and contains the payload information carried by the IPv4 data packet.

This transformation requires the second user terminal, although using the IPv6 protocol, to have available a "dummy" IPv4 address, which may be its own IPv4 address or that of a home gateway that administers a home network to which it is connected. This address, used as the destination address of an IPv4 packet coming from the IPv4 domain, is used by the interconnection equipment to construct the IPv6 destination address referred to above.

Conversely, it is possible to retrieve the IPv4 address and the source port number from an IPv6 address constructed using such a mechanism (i.e. conforming to the IPv6 address construction formalism just referred to). It is therefore unnecessary to store an IPv4 to IPv6 address translation table or to maintain states relating to sessions in the access node (interconnection node) of both the IPv4 and IPv6 domains. The invention

Juniper Exhibit 1002, page 12

therefore makes it possible, in the IPv4 to IPv6 direction and in the IPv6 to IPv4 direction, to route the IPv4 data packet towards its destination in the form of an IPv6 data packet and to deliver payload information contained in the packet towards its destination without having recourse to state tables that are laborious to maintain.

Thus neither the IPv6 user terminal receiving or sending the data packet, nor, where applicable, the home gateway that manages it, nor the routers responsible for routing the packet to its destination need to interpret the IPv4 protocol.

However, for it to be possible to route the IPv6 data packet resulting from such a transformation like a native IPv6 packet, it is necessary to verify its source and destination addresses against the IPv6 address construction formalism referred to above. The method of the invention therefore proposes a solution identifying the destination or the source of the packet as belonging to an IPv4 domain and consequently applying to it appropriate verification processing.

According to one aspect of the invention, when the data packet comes from said user terminal and goes to the IPv4 domain, the step of regularizing the source address further includes the following steps:

· identifying an IPv6 native source address;

· creating an entry in an address translation table, said entry associating said native source address with a source address constructed by concatenating an operator prefix, an IPv4 address assigned to the gateway, and a source port number belonging to a range of port numbers authorized for said gateway; and

· replacing the native source address of the data packet with the constructed source address.

This relates to an outgoing call. If a constructed destination address has been identified, it may be deduced that the data packet is for a user terminal of

the IPv4 domain. In this situation, its source address must be a constructed address in order for an IPv6/IPv4 domain interconnection equipment to be able thereafter to recover the source IPv4 address and to transform the IPv6 data packet back into an IPv4 data packet. If no processing is effected, it is not possible for the interconnection node to process the packet, since the native source address contains no information relating to the IPv4 source address, i.e. the dummy IPv4 address of the terminal that sent the packet.

If the source address is a native source address, the method of the invention makes it possible to replace it with a constructed source address belonging to a prefix or IPv6 source address range authorized for the gateway.

In expectation of receiving a response to this data packet, an association between the native source address and the constructed source address is added to an address translation table of the home gateway.

Thus a response data packet may be routed to the user terminal of the home network that sent the first data packet.

An advantage of the invention is that it enables an IPv6 user terminal to use the source address of its choice to send data packets to an IPv4 domain, as the gateway of the invention does what is necessary for the packets to be routed to their destination.

According to one aspect of the invention, address identification uses an identifier contained in the destination address.

This identifier may have different values depending on whether it is a native IPv6 address or an IPv6 address constructed from an IPv4 address. One advantage of this is making it possible to identify the nature of the address of the data packet simply and quickly. This kind of solution also enables mutualisation of IPv4/IPv6 interconnection equipments between operators.

According to another aspect of the invention, the receiving method further includes a step of verifying that the source port number of the data packet and the source port number of the constructed source address match.

The data packet contains indeed a source port number in the transport layer of the ISO model. For a response to be routed by the network to the terminal that sent the first packet, it is important for this transport level source port number to match with the source port number contained in the constructed source address of the data packet. If this is not so, the method of the invention enables matching of the two source port numbers.

Note that the verification step and the source address regularization step may be carried out simultaneously. For example, choosing a constructed source address in the prefix of the gateway may incorporate the constraint of having a source port number equal to the transport level source port number.

According to one aspect of the invention, when the data packet comes from the IPv4 domain and goes to user terminal connected to the IUPv6 domain by said home gateway, the step of regularizing the source address includes the following steps:

· searching an address translation table of said gateway for an entry associating with said destination address a native destination address;

· if an entry is found, replacing the constructed destination address of the data packet with the native destination address from that entry.

Note that the destination port number is also replaced by that in the port and address translation table maintained by the home gateway.

The above remarks relate to an incoming call. The IPv6 data packet was constructed from an IPv4 packet by an equipment for interconnecting the IPv6 domain and the IPv4 domain. It may be a response to a data packet sent

beforehand by the user terminal connected to the home gateway. The gateway therefore consults its address translation table. If it finds therein an association between the destination address extracted from the received data packet and an IPv6 native destination address, it replaces the constructed destination address and potentially the constructed destination port number of the data packet with the IPv6 native address of this table entry and routes the modified packet to the destination terminal.

According to another aspect of the invention, the receiving method further includes a step of verifying that the destination port number of the data packet and the destination port number contained in the constructed destination.

Such verification makes it possible to be sure that the destination port number of the data packet at the transport level coincides with the number from the constructed destination address of the packet. This verification is of particular benefit if the dummy IPv4 address assigned to the home gateway is shared with a other terminals or home gateways. In this situation, discriminating between these equipments is based on the range of port numbers used. According to the invention, a packet sent by the IPv4 terminal to said dummy address may be routed to the gateway concerned without encountering any routing problems.

The receiving method may be used in a device for receiving a data packet in an IPv6 domain connected to an IPv4 domain, said packet including an IPv6 destination address and an IPv6 source address, characterized in that it includes the following steps:

· identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address, and a destination port number;

· if necessary, regularizing at least one address of the data packet and modifying the data packet using the regularized address; and

· routing the modified data packet to its destination.

In one particular implementation of the invention, the steps of the method of receiving a data packet are determined by computer program instructions.

Consequently, the invention also provides a computer program on an information medium, adapted to be executed in a receiving device or more generally in a computer, this program including instructions for executing the steps of a sending, receiving or routing method as described above.

This program may use any programming language and take the form of source code, object code or a code intermediate between source code and object code, such as a partially-compiled form, or any other desirable form.

The invention also provides a computer-readable information medium containing instructions of a computer program as referred to above.

The information medium may be any entity or device capable of storing the program. For example, the medium may include storage means, such as a ROM, for example a CD ROM or a micro-electronic circuit ROM, or magnetic storage means, for example a floppy disk or a hard disk.

Moreover, the information medium may be a transmissible medium such as an electrical or optical signal, which may be routed via an electrical or optical cable, by radio or by other means. The program of the invention can in particular be downloaded over an Internet-type network.

Alternatively, the information medium may be an integrated circuit in which the program is incorporated, the circuit being adapted to execute the method in question or to be used in its execution.

The invention further provides a home gateway adapted to connect user terminals to an IPv6 domain connected to an IPv4 domain.

According to the invention such a gateway includes:

· means for obtaining an IPv4 address, a range of port numbers authorized for said gateway, and a range of IPv6 addresses authorized for said gateway, said range of IPv6 addresses being constructed by concatenating an operator prefix, said IPv4 address, and the range of authorized IPv4 port numbers; and

· a device of the invention for receiving an IPv6 data packet in the IPv6 domain connected to the IPv4 domain.

According to the invention, such a gateway processes only IPv6 data packets. However, it is assigned an IPv4 address, so that it may be identified and contacted by senders in the IPv4 domain. Said address is not used by the home gateway to send IP packets.

The home gateway may hold an address translation table containing entries associating at least one source address for a communications session involving a user terminal of its home network. According to the invention, said gateway is adapted to store in said entry an IPv6 constructed source address and an IPv6 native source address.

BRIEF DESCRIPTION OF THE DRAWINGS

Other advantages and features of the invention become more clearly apparent on reading the following description of one particular implementation of the invention, provided by way of illustrative and non-limiting example only, and the appended drawings, in which:

· Figure 1 shows diagrammatically an IPv6 domain and an IPv4 domain interconnected according to the invention;

· Figure 2 shows the structure an IPv6 address prefix constructed according to the invention;

· Figure 3 shows diagrammatically steps of the method of receiving data packets in an IPv6 domain interconnected according to the invention with an IPv4 domain;

· Figure 4 shows the structure in a first implementation of the invention of an IPv6 address constructed from an IPv4 destination address and a destination port;

· Figure 5 shows the structure according to the invention of an IPv6 destination address constructed from an IPv4 address and a destination port for implementing the receiving method of the first implementation of the invention;

· Figure 6 shows the structure of an IPv6 source address constructed from an IPv4 source address and a source port for implementing the receiving method of the first implementation of the invention;

· Figure 7 shows the structure in a second implementation of the invention of an IPv6 address constructed from an IPv4 address and a destination port;

· Figure 8 shows diagrammatically steps of receiving a data packet in an IPv6 domain interconnected with an IPv4 domain in the second implementation of the invention; and

· Figure 9 shows diagrammatically the structure of a device of the invention for receiving a data packet in an IPv6 domain.

DESCRIPTION OF ONE PARTICULAR IMPLEMENTATION OF THE INVENTION

The general principle of the invention relies on constructing an IPv6 address from an IPv4 address, a predetermined operator prefix, and a port number. This enables transformation of an IPv4 packet entering an IPv6 domain and an IPv6 packet leaving an IPv6 domain to go to an IPv4 domain without it being necessary to maintain a

table of correspondence between the IPv4 and IPv6 addresses in an access node to the IPv6 domain.

It will be recalled that IPv6 addresses comprise 16 bytes (128 bits), compared to the 4 bytes (32 bits) of IPv4 addresses. There is therefore an extremely large potential number of IPv6 addresses compared to the number of IPv4 addresses. An IPv6 address has two parts:

· a left-hand part (the prefix) that identifies a subnetwork of the domain;

· a right-hand part that identifies a machine connected to the subnetwork.

The longest prefixes assigned to a subnetwork are generally "/64" prefixes, i.e. contain 64 bits for identifying the subnetwork. The right-hand 64 bits of the address are then used to identify a particular machine belonging to the subnetwork. Shorter prefixes (for example "/56" or even "/48") enable identification of larger subnetworks, themselves often including "/64" subnetworks. Nevertheless, there is nothing in the IPv6 standard to prohibit the use of prefixes longer than "/64" and it is therefore possible to conceive of a "/116" prefix, for example, identifying a subnetwork that may include 4096 machines.

Note that the only restriction on prefixes longer than "/64" is simply that the machines behind the corresponding subnetwork will not be able to use the autoconfiguration mechanism described in Document RFC 2462. This mechanism enables a machine knowing its level 2 address (for example its MAC Ethernet address) to configure for itself, subject to certain conditions, the right-hand 64 bits of its IPv6 address, deriving its level 2 address therefrom using a precise algorithm. This autoconfiguration mechanism is not obligatory, however, and other mechanisms may be preferable, for example that corresponding to the DHCPv6 protocol (see RFC 3315) that among other things makes it possible to obtain an IPv6 address from a DHCPv6 server.

Turning now from a simple IPv6 machine to an IPv6 router (for example an IPv6 home gateway), it is known that such an equipment must have one or more IPv6 prefixes representing the subnetworks whose packets it routes. An IPv6 router must therefore be configured with one or more prefixes.

An extension of the DHCPv6 protocol enables a router requiring one or more IPv6 prefixes (for example a home gateway) to request them from an equipment that is able to delegate prefixes (typically an upstream router). This extension is described in RFC 3633 (IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6) and specifies an identity association for a prefix delegation option in DHCPv6 messages for passing on the delegated prefix or prefixes. Once the requesting router has been delegated one or more IPv6 prefixes, it routes all IPv6 packets going to or coming from machines whose addresses are inscribed the prefix or prefixes that it manages.

There is described below with reference to Figure 1 an IPv6 domain 1 including an equipment for interconnecting the IPv6 domain 1 and an IPv4 domain 2 or IPv6/IPv4 access node 40 to an IPv4 domain 2 and an access router 30 adapted to route data packets going to or coming from a home gateway 20 connected to the IPv6 domain 1. This kind of gateway administers a home network 2 to which the terminals 21 and 22 are connected.

In the context of the invention, a home gateway is considered that implements only the IPv6 protocol. Accordingly, such a gateway is able to process (in particular to send and receive) only IPv6 data packets.

The terminals 21 and 22 are also mono-version IPv6 (or pure IPv6) terminals, meaning that they implement only the IPv6 protocol. How the invention enables interconnection of an IPv6 domain and at least one IPv4 domain for IPv6 terminals is described below.

The following "hybrid" circumstances are considered:

· routing an incoming IPv4 data packet sent by a user terminal of the IPv4 domain 3 to a user terminal 21, 22 of the home network of the gateway 20 connected to the IPv6 domain 1; and

· routing an outgoing IPv6 data packet sent by a user terminal 21, 22 of the IPv6 domain 1 to a user terminal of the IPv4 domain 3.

The details of sending pure IPv6 or pure IPv4 packets being known to the person skilled in the art, they are not described in more detail here.

To be able to connect to the IPv6 domain or network, the home gateway has IP connectivity elements provided by the connectivity service provider.

However, note that the invention is not limited to access to the IP connectivity service (Internet or Intranet, for example) via a home gateway, but also applies to user terminals in other Internet or Intranet network access contexts. One example is access to the IP connectivity service from a simple mobile terminal of a mobile network or from a sophisticated mobile terminal that could serve as a gateway, communicating with other terminals in its local area network, for example via Bluetooth.

According to the invention, the home gateway 20 has the following IP connectivity elements:

· a standard IPv4 address below designated "@IPv4"; if the gateway hosts in its home network pure IPv6 client terminals, this IPv4 address is referred to as a "dummy" address because it is not used by the gateway to send/receive IP traffic; the invention uses it to construct IPv6 addresses (see below);

· a range of authorized port numbers (ports_pattern/length_of_unvariable);

· a constructed IPv6 address prefix (IPv6_prefix_ports_range); and

· a native IPv6 address prefix (IPv6_prefix_native); this second prefix is not mandatory, however; the constructed IPv6 prefix is sufficient on its own.

The @IPv4, IPv6_prefix_ports_range and IPv6_prefix_native elements are standard information elements in the usual IPv4 and IPv6 context.

According to the invention, the information element IPv6_prefix_ports_range intrinsically contains the elements @IPv4 and ports_pattern/length_of_unvariable.

In one implementation of the invention, the IPv4 address @IPv4 is an address shared@IPv4 that is shared by a plurality of home gateways of the IPv6 domain 1 and the range of authorized port numbers for the home gateway 20 is a range of port numbers reserved for that gateway.

Clearly sharing the public address shared@IPv4 between home gateways makes it possible to economize on the number of IPv4 addresses used and to delay the phenomenon of running out of addresses. Moreover, its use is justified by the need to interconnect IPv4 domains and IPv6 domains. This interconnection is generally effected by means of representation addresses. If the installed base of IPv6 clients is large, then many IPv4 representation addresses are required.

The various home gateways that share the same address shared@IPv4 are uniquely identified by the port numbers that they use as each of them has the benefit of a range of contiguous port numbers, undoubtedly small, but nevertheless reserved to it.

The invention proposes interconnecting IPv6 and IPv4 domains in a manner that requires the assignment of IPv4 addresses to function and thus ensures in a transparent manner continuity of connectivity between heterogeneous terminals (i.e. terminals implementing different addressing protocols, such as IPv4 and IPv6).

An advantage of the implementation of the invention in which the IPv4 addresses are shared is therefore to facilitate migration to IPv6 addressing at the same time

as economizing on IPv4 addresses. In a context of transition between the IPv4 and IPv6 addressing modes, this can advantageously make it possible to avoid a penury of addresses until migration is completed. Another advantage is an immediate return on the investment in IPv6 plant (because the use of IPv6 capacity depends not on the behavior of the clients but on the operator).

In the remainder of the description the IPv4 address assigned to the gateway 20 is a shared address shared@IPv4.

Referring to Figure 1, the home gateway 20 is connected to the network of the operator via an access router 30. This is the first router that the IPv6 and IPv4 data packets encounter when they leave the home gateway.

According to the network architecture adopted at the IPv6 routing level, the access router 30 may advertise in the upstream direction of the network (i.e. towards the network 1 of the IP connectivity service provider) the IPv6 prefixes that it routes, i.e. the prefixes IPv6_prefix_ports_range and IPv6_prefix_native of the home gateways that it serves.

The access router 30 obtains the IPv6 prefixes of the home gateways that it serves in a manner that is entirely conventional in an IPv6 network environment. Two methods are described below:

1) it receives IPv6 routing advertisements (IPv6_prefix_ports_range and IPv6_prefix_native) from the home gateways that it serves; to this end each home gateway advertises its prefixes (IPv6_prefix_ports_range and IPv6_prefix_native) in the upstream direction; or

2) it obtains IPv6_prefix_ports_range and IPv6_prefix_native by prefix delegation as described in RFC 3633 (IPv6 Prefix Options For Dynamic Host Configuration Protocol (DHCP) version 6).

An example of an IPv6 address prefix constructed in accordance with the invention, such as the prefix IPv6_prefix_ports_range assigned to the home gateway 20, is described below with reference to Figure 2.

This IPv6 prefix combines the bits of the IPv4 public address shared_@IPv4 and the range of authorized port numbers (ports_pattern/length_of_unvariable) for the gateway 20 and makes it possible to route the incoming IPv6 packet to the destination home gateway unambiguously. It is an IPv6 prefix that is routable in an IPv6 network. It could even be routed in the IPv6 network if it were chosen to be a prefix inscribed in the prefix of the network operator providing the home gateway (especially if it were advertised in the Border Gateway Protocol (BGP)). In the Figure 2 example, this prefix comprises, from left to right:

· the IPv6 prefix assigned to the access node 40: IPv6/IPv4_Access_Node_prefix; this prefix is advantageously chosen so that it is inscribed in the IPv6 operator prefix IPv6-prov assigned to the IP connectivity service provide by its Regional Internet Registry (RIR) and thus includes this operator prefix in its first bits;

· the bits IPv6/IPv4_Access_Node_Service identifying the interconnection service IPv6/IPv4_Access_Node to the operator according to the present invention; the sequence made up of the bits of the operator prefix followed by the bits IPv6/IPv4_Access_Node_Service constitute the prefix IPv6/IPv4_Access_Node_Service_prefix that identifies the service;

· complementary bits identifying a particular access node IPv6/IPv4_Access_Node serving the home gateway; for load-balancing reasons, the prefix IPv6/IPv4_Access_Node_prefix may not be specific to only one access node;

· the 32 bits of the address shared@IPv4 of the gateway 20;

· optionally, 8 reserved bits set to 0; this byte may be used to distinguish between the different types of port (UDP, TCP, SCTP, etc.); it could take the value "X" for UDP processing, "Y" for TCP processing, etc.;

· the 16 bits representing the range of port numbers authorized for the gateway (ports_pattern), with a meaningful invariant part on the left in these 16 bits (the more significant bits), of length length_of_unvariable; note that if the IPv4 address of the gateway 20 is not shared by a plurality of home gateways, the range of authorized port numbers is of maximum and identical size for all the gateways.

The length of the prefix IPv6_prefix_ports_range is established as follows: [128 - 16(length of an IPv6 address - port coding address) = 112 bits plus length_of_unvariable (length of invariant bits representing the range of authorized source ports).]

Note that the prefix IPv6_prefix_ports_range constructed according to the invention is longer than the prefixes recommended by the IPv6 standard for IPv6 deployment. It nevertheless conforms to the IPv6 standards.

The IPv6 domain 1 described with reference to Figure 1 includes at least one access node 40 of the invention. Note that it may include other access nodes of the invention. The access node 40 (IPv6/IPv4_Access_Node) is a particular Dual-Stack (IPv4 and IPv6) router, i.e. it implements both the IPv4 protocol and IPv6 protocol.

The access node 40 (IPv6/IPv4_Access_Node) in the network 1 is typically upstream of the access router or routers 30 (i.e. towards the network core in an interconnection segment with adjacent networks), as shown in Figure 1. Said access node is also referred to as an interconnection node.

The method of receiving an IPv6 data packet in the IPv6 domain is described below with reference to

Figure 3. It is advantageously executed by a receiver device included in a home gateway connected to the IPv6 domain, such as the gateway 20, and processes data packets coming from the home gateway 2 and data packets coming from the IPv4 domain 3. This kind of method includes a step R1 of identifying the IPv6 destination address as being a IPv6 native destination address or an IPv6 destination address constructed by concatenating an access node prefix, an IPv4 destination address, and a destination IPv4 port number. It is assumed here that the gateway 20 has obtained this prefix beforehand, for example through configuration.

It then includes a step R2 of regularizing an address of the data packet. In the direction from the home gateway to an IPv6 domain, this address is the source address of the packet; in the direction from the IPv6 domain to a home network, this address is its destination address. This step may lead to modification of the data packet. The modified data packet is then routed to its destination (step R3).

Consider a first implementation of the invention in which an outgoing call is set up to an IPv4 destination, for example an IPv4 web server on the Internet. A user terminal of the home gateway 2, for example the IPv6 PC 22 connected to the gateway 20, sends a data packet to this party in the IPv4 domain 3. In this situation, the application executed on the PC is an IPv6 browser. It must be remembered that the source user terminal 22 is a pure IPv6 terminal.

The following situations arise:

· the user terminal 22 sends an IPv6 data packet using a source address equal to an IPv6 constructed address that has been assigned to it; or

· the user terminal 22 sends an IPv6 data packet using a source address equal to an IPv6 native address that has been assigned to it.

Clearly the data packet contains an IPv6 destination address corresponding to the IPv4 destination that the terminal must have recovered beforehand.

The browser of the terminal 22 thus needs to know the IPv6 address of the destination web server. The web server is accessible only in IPv4. The terminal 22 must therefore have an IPv6 address that it considers the address of the web server (even though in reality the web server has only an IPv4 address).

To this end, a function for translating an IPv4 address of the web server into an IPv6 address must be implemented by the IP connectivity service provider or a third party. This translation function must conform to an IPv6 address construction formalism such that it contains the IPv4 address of the other party (the web server in this example). This translation function is described below with reference to Figure 4.

This kind of translation function, here denoted DNS_IPv4toIPv6, may be executed by the access node 40 IPv6/IPv4_Access_Node of the IPv6 domain 1, for example, but on a more general level it is executed by a DNS server of the domain 1. The function DNS_IPv4toIPv6 is the default point of contact for any DNS resolution request sent by a requester terminal. By default, this function examines first IPv6 records of type "AAAA", in other words IPv6 native addresses. If a record is already present, a response is then sent to the requester terminal. If no record is present, a type A resolution request is then effected by the translation function DNS_IPv4toIPv6. On reception of a response from a DNS server containing the IPv4 address of the other party (the web server in this example), the function DNS_IPv4toIPv6 transforms the IPv4 address received in the response into an IPv6 address conforming to the formalism described with reference to Figure 4 and retains this information in its cache.

Note that the Figure 4 example merely represents one implementation of the invention, what is essential being that the IPv4 address of the other party (here the web server) is inscribed in an IPv6 address. An error message is sent to the requester terminal if no response is received from a DNS server.

The destination address (here that of the web server) transformed in this way into an IPv6 address is denoted IPv6_remoteAddress_out_to_IPv4 below. Note that the requested terminal may recover an IPv6 address from the remote machine to be contacted by other means, for example from a server.

In any event, the IPv6 address of the other party (here the web server) may be an IPv6 native address or an IPv6 address conforming to the formalism introduced by the present invention. In the circumstance of a constructed address IPv6_remoteAddress_out_to_IPv4, it is included in the prefix IPv6/IPv4_Access_Note_Service_prefix.

Referring to Figure 4, note that the sequence of 2 bytes farthest to the right is marked "reserved" and set to 0 by default. This location corresponds to that of the port bits in an IPv6 address IPv4inIPv6_dest_address for the packets intended for a user terminal. It is reserved in particular so that it is possible to indicate a port at which the other party (here the web server) wishes to be called. It could be an IPv4 other party that is also assigned an IPv4 address shared between a plurality of other parties and that would therefore not have access to all the available ports.

An IPv6 data packet containing the destination address IPv6_remoteAddress_out_to_IPv4 is then sent by the terminal 22.

The home gateway 20 of the invention includes a device of the invention for receiving a data packet. On receiving the IPv6 packet, this device is adapted to

execute the method of the first implementation of the invention of transmitting an IPv6 packet to an IPv6 address representing a machine connected to an IPv4 domain, as described below with reference to Figure 5.

This method executes the IPv6 destination address identification step R1 described above.

One aspect of the invention is that the length of the prefix IPv4_Access_Node_Service_prefix is known to the home gateway 20, which is able to determine its value easily by taking the corresponding bits in its IPv6_prefix_ports_range. This kind of identification classifies an IPv6 destination address that is inscribed in the prefix IPv4_Access_Node_Service_prefix as a constructed address and considers all addresses not in this prefix to be native addresses.

An advantage of this identification process is that it is simple.

This identification method is valid only in the context of a single operator, however. For deployment on a wide scale with mutualisation of IPv4 and IPv6 domain interconnection nodes this method is no longer appropriate.

This kind of identification may entail searching a destination address for an identifier or tag whose value may represent a native address or a constructed address. As indicated in Figure 4, for example, this kind of identifier ADDR_TYPE_TAG may have a length of only one bit having the value 0 or 1 to indicate that it is a native address or a constructed address. To facilitate reading, the identifier ADDR_TYPE_TAG may be placed at the beginning of the constructed IPv6 address, for example, or between IPv6/IPv4_Access_Node_Service_prefix and the IPv4 address.

An advantage of the identifier ADDR_TYPE_TAG is that it enables mutualisation of IPv4/IPv6 interconnection plant between operators and therefore costs sharing. Accordingly, an operator Oi may provide IPv4-IPv6

interconnection for a region Ri (with a set Pi of IPv4 prefixes). For the other operators Oj, only the addresses constructed by the operator Oi (based on the IPv4 prefixes) are visible, via BGP advertisements.

Clearly prefixes other than IPv6/IPv4 may exist, but they are not used to provide this connectivity service and the processing applied to them is that for an IPv6 native packet, i.e. they are routed directly to the IPv6 access router 30.

If the IPv6 destination address is classified as a constructed address, the transmission method of the invention executes a step R2 of regularizing the source address of the packet to be transmitted.

In this first implementation of the invention, this entails identifying in the step R_{21} if the source address is a constructed address or a native address. An address is considered constructed if it is an IPv6 source address inscribed in IPv6/IPv4_Acess_Node_Service_prefix, all addresses not in this prefix being considered native source addresses. If the identifier ADDR_TYPE_TAG is used, an address is identified as constructed if the identifier ADDR_TYPE_TAG is set to "1".

If the source address is constructed, the data packet is routed to its destination in the step R3.

If the source IPv6 address is classed as a native address, the method of the invention executes, before this routing step, a step R_{22} for choosing an IPv6 constructed source address whose source port number is in the authorized range ports_pattern/length_of_unvariable assigned to the gateway 20 and modifies the data packet by replacing the native source address with this constructed address. In the step R_{24}, the method of the invention creates an entry in the address translation table of the gateway associating the native source address and the source address constructed in this way.

The method of the invention may advantageously further verify in the step R_{23} that the source port number

contained in the constructed source address and the transport level source port number of the data packet match. Referring to Figure 6, it is seen that this entails taking any 128-bit IPv6 address IPv6_prefix_ports_range and copying into its 16 right-hand bits of the data packet to be transmitted the bits of the source port used (the TCP or UDP port of the IPv6 packet received from the terminal 22).

It is clear that this step is necessary for the IPv6/IPv4 access node 40 to be able to translate the IPv6 data packet into an IPv4 data packet before routing it to the destination IPv4 domain. This has another advantage if the IPv4 address assigned to the home gateway 20 is an address shared by a plurality of home gateways of the IPv6 domain 1. As mentioned above, the home gateway 20 can use only source port numbers belonging to a restricted range of port numbers reserved for it.

Note also that if the home gateway 20 constrains the source port to be in the range of authorized port numbers ports_pattern/length_of_unvariable, the constructed source address:

· is inscribed in IPv6_prefix_ports_range; and

· has its last 16 bits identical to the source port number of the IPv6 packet received by the gateway from the terminal.

The IPv6 source address formed in this way is denoted IPv6_address_source_ports_range below.

The IPv6 packet containing the constrained source IPv6 address IPv6_address_source_ports_range is routed to the IPv6 access router 30 that serves the gateway in the step R3.

The IPv6 access router 30 verifies that the IPv6 source address IPv6_address_source_ports_range is authorized for the home gateway 20. In other words, it verifies that there is no spoofing, i.e. that the home gateway 20 sends IPv6 packets in its authorized prefix range IPv6_prefix_ports_range. For this the IPv6 access

router 30 verifies that the IPv6 source address IPv6_address_source_ports_range of the IPv6 packet received from the gateway 20 is inscribed in the prefix IPv6_prefix_ports_range assigned to this home gateway. This verification is effected in a standard manner in accordance with a principle already used for IPv6 native traffic.

If the result of this verification is positive, the IPv6 access router 30 routes the IPv6 packet towards its destination.

Because the IPv6 destination address is inscribed in the prefix IPv6/IPv4_Access_Node_prefix characterizing the node IPv6/IPv4_Access_Node 40 providing access to the IPv6 domain, the data packet is routed towards that access node. It is assumed, for example, that a node of this kind is placed in the IPv6 domain 1 as close as possible to the IPv4 domain or domains that it serves in order to optimize the routing of data packets to these domains, but the invention is not limited to any such location of the access node 40, which may be located anywhere in the domain 1.

On reception of the IPv6 packet, the access node IPv6/IPv4_Access_Node 40 routes the outgoing data packet to an IPv4 domain the following manner:

· it extracts an IPv4 destination address and a destination port from the IPv6 destination address and an IPv4 source address and a source port from the IPv6 source address;

· it then translates the IPv6 packet into an IPv4 packet that has the following characteristics:

  · its IPv4 source address is the IPv4 address shared@IPv4 of the home gateway 20; it is this address shared@IPv4 that the destination of the transmitted IPv4 data packet (i.e. the web server) will see; remember that this IPv4 address shared@IPv4 is included in the prefix IPv6_prefix_ports_range and thus in the source IPv6 address IPv6_address_source_ports_range; referring to

Figure 8, the IPv4 address Shares_@IPv4 may be extracted from bits 24 to 55;

· its IPv4 destination address is the IPv4 address of the other party; referring to Figure 4, the IPv4 destination address may be extracted from bits 24 to 55 of the address IPv6_remoteAddress_out_to_IPv4 of the IPv6 data packet received by the access node 40;

· the source port number of the translated IPv4 data packet is the number of the source port of the IPv6 packet received;

· the destination port number of the translated IPv4 data packet is the same as that of the IPv6 packet;

· the payload part of the IPv6 packet is the payload part of the translated IPv4 packet;

· finally, it routes the translated IPv4 packet to its destination (the IPv4 web server in this example).

Note that the fields of the header of the IPv6 packet are translated into corresponding IPv4 fields in a standard manner, for example according to the principles of the Network Address Translation-Protocol Translation (NAT-PT) standard.

Clearly, if the IPv4 address assigned to the home gateway 20 is a public address shared between a plurality of gateways, it is necessary for the source port number contained in the IPv6 constructed source address of the received data packet to belong to the range of port numbers reserved for this gateway; if this were not so, the access node could translate the IPv6 packet to be transmitted into an IPv4 data packet, but any response packets sent by the destination entity would not reach the home gateway.

The access node 40 advantageously verifies that the source port belongs to the range of source port numbers assigned to the gateway 20 by checking that the last 16 bits of the IPv6 source address of the packet are identical to the 16 bits of the source port in the corresponding TCP or UDP field of the IPv6 packet. This

indirect verification may be carried out following verification by the access router that the home gateway has sent a packet whose source address is in its prefix. After these two steps, it is certain that the home gateway 20 has sent a data packet containing a source port included in its range of authorized ports and did not use that of another home gateway.

A second implementation of the invention addresses the situation of a data packet IPv4-in-pt entering an IPv6 domain from an IPv4 domain when the destination terminal, for example the user terminal 21, is in the IPv6 domain 1. The user terminal is behind the home gateway 20 that has an IPv4 address @IPv4 or shared@IPv4 and a range of authorized ports ports_pattern/length_of_unvariable.

If it is for the user terminal 21 of the home network of the home gateway 20, the incoming packet IPv4-in-pt contains the IPv4 destination address shared@IPv4 and a destination port inscribed in the range of authorized port numbers of the home gateway 20 ports_pattern/length_of_unvariable.

As mentioned above with reference to Figure 2, the address shared@IPv4 and the range of port numbers ports_pattern/length_of_unvariable are found in the prefix IPv6_prefix_ports_range of the home gateway 20.

The packet IPv4-in-pt is received by the access node 40. In a preliminary step, the IP connectivity provider advertises to the IPv4 domains with which it has an interface the IPv4 addresses assigned to home gateways of the domain 1 to which it is responsible for routing the IPv4 packets. It effects this advertisement either via the access node 40 itself or an Autonomous System Border Router (ASBR) using a technique known to the person skilled in the art.

The packet IPv4-in-pt contains a destination address @IPv4 or shared@IPv4 managed by the access node 40 and a destination port dest-port. The access node 40

constructs an IPv6 destination address IPv4inIPv6_dest_address by concatenating a prefix IPv6/IPv4_Access_Node_prefix of the access node 40, said IPv4 destination address shared@IPv4, and the destination port number dest-port, as described with reference to Figure 7.

The destination port number dest-port is inserted into the right-hand part of the IPv6 constructed destination address. It therefore inserts both the 32 bits of the destination IPv4 address of the received IPv4 packet and the 16 bits of the destination port dest-port to constitute an IPv6 constructed destination address IPv4inIPv6_dest_address.

The access node 40 thereafter generates an IPv6 data packet IPv4inIPv6-pt from the IPv6 constructed destination address IPv4inIPv6_dest_address and the received IPv4 data packet. In one implementation the received IPv4 packet is translated into an IPv6 packet:

· whose IPv6 source address is one of the IPv6 addresses available to the IPv6/IPv4_Access_Node 40 for itself (for one of its interfaces); and

· whose IPv6 destination address is the address IPv4inIPv6_dest_address.

In another implementation the received IPv4 packet IPv4-in-pt is translated into an IPv6 packet with which the construct IPv6 address is associated after first extracting from the received IPv4 packet its destination IPv4 address, its destination port, its source IPv4 address, and its source port.

The IPv6 data packet IPv4inIPv6-pt generated using the IPv6 constructed destination address is routed in the IPv6 domain 1. It then enters the IPv6 routing core of the access node 40 IPv6/IPv4_Access_Node.

By construction, its destination address IPv4inIPv6_dest_address is inscribed in the prefix IPv6_prefix_ports_range of the home gateway 20. The packet IPv4inIPv6-pt is routed to the interface of the

access node IPv6/IPv4_Access_Node 40 that serves the corresponding IPv6 route to the home gateway 20.

Note that if IPv4inIPv6_dest_address were not inscribed in any prefix IPv6_prefix_ports_range (or any encompassing prefix), the packet would be destroyed en route as it could not be routed to any prefix IPv6_prefix_ports_range and thus to any home gateway.

If the destination address IPv4inIPv6_dest_address is inscribed in the prefix IPv6_prefix_ports_range, the packet IPv4inIPv6-pt reaches the dual-stack access router 30 serving the home gateway 20 hosting the user terminal 21 in its home network 20. It is routed by the dual-stack access router 30 to the home gateway, which knows the route to the prefix IPv6_address_source_ports_range.

In this second implementation of the invention, the home gateway 20 includes a device using the method of the invention of receiving the data packet IPv4inIPv6-pt. A method of this kind is described below with reference to Figure 8.

When the packet IPv4inIPv6-pt reaches the home gateway 20, the gateway executes the step R'1 described above of identifying the destination address.

If a native destination address is identified, the data packet is routed directly to the destination user terminal in a step R'3.

If a constructed destination address is identified, for example with the aid of an identifier contained in the destination address, the step of regularizing the method of the invention of receiving a data packet includes a step R'_{21} of searching the translation table of the home gateway for an entry containing the constructed destination address. If the result of this search is positive, an entry of this kind associates with the constructed destination address a native destination address IPv6_address_native_Ue of the destination terminal. In the step R'_{23}, the method of the invention replaces the constructed destination address in the IPv6

data packet with this native address. This is particularly advantageous if the data packet IPv4-in-pt is part of a response to a data packet sent beforehand by the destination terminal 21 with its IPv6 native source address, for which the gateway stored this native address in its NAT table before sending it, as described with reference to the previous implementation of the invention. At that time it created the entry in its translation table and replaced the native address of the terminal 21 with the constructed address to enable the access node 40 to extract an IPv4 source address from it when transforming the outgoing IPv6 packet into an IPv4 packet.

The step of regularizing the method advantageously further includes a step R'22 of verifying that the transport level destination port of the data packet agrees with the destination port number contained in the destination address of the packet. If the two port numbers do not agree, the packet is rejected. This must not occur if the translation was effected by the access node but this step may be used for monitoring streams coming from the access node.

In the step R'3, the gateway routes the data packet to the destination terminal in its home network.

In the example described with reference to Figure 1, the home gateway 20 of the invention includes a device 25 that is described below with reference to Figure 10 for receiving a data packet in an IPv6 domain. It includes the hardware elements conventionally found in a standard computer or a dedicated router, namely a processor 25_1, a random-access memory (RAM) 25_2, a read-only memory (ROM) 25_3, and telecommunications means 25_4 for communicating with the network 1.

According to the invention, the device 25 includes a memory 25_5 containing a database in which is stored an address translation table (NAT table) for translating addresses between the domain 1 and its home network 3.

Note that this memory may equally well be external to the device 25 provided that said device can access it.

The read-only memory 25_5 constitutes a storage medium of the invention that stores the computer program of the invention. The program includes instructions for executing the steps of the method of the invention of receiving an incoming packet described above with reference to Figures 3, 5, and 8.

Note also that the receiver device may equally well be included in a user terminal connected directly to the network 1 of the connectivity service provider.

To summarize, the invention makes possible a second phase of migration of IP connectivity services towards IPv6 using packet routing mechanisms that takes the following factors into account:

· The final migration to IPv6 will take a plurality of years (a minimum timescale of 10 years), mainly because of the large number of participants to "convince" to go over to IPv6, the large number of autonomous systems (AS), of which there are more than 17,000, and the diversity of interconnection mechanisms. Moreover, it should be pointed out that the address problem is *a priori* of concern only to operators. Clients have no reason to modify the architecture of their local networks. An enterprise "John Doe" has no motivation for migrating its FTP, HTTP, etc. servers to IPv6. Operators must expect a long haul to accompany the changeover to IPv6.

· Service operators suffer a problem of running out of IPv4 addresses, as described above.

· Simply migrating a given domain to IPv6 does not solve the problem of global connectivity (contacting any remote machine present on the Internet). Interconnection with the IPv4 world must therefore be provided.

· A solution based on NAT-PT that is not stateless is not to be recommended. This would degrade the service provided as value-added services linked to port

forwarding configured by clients would not work and would depend on the behavior of the "black box" interconnecting an IPv4 cloud and an IPv6 cloud.

The mechanisms of the invention for routing IP packets make it possible to encourage the use of the IPv6 protocol in the following manner: activating IPv6 and providing a solution making it possible to encourage IPv6 traffic based on a stateless interconnection function placed in the network. The solution of the invention uses only the IPv6 connectivity of home gateways and implies the use of IPv6 home gateways and user terminals. Because of this, these equipments are in a position to process (send and receive) only IPv6 data packets.

The solution of the invention makes it possible:

· for the access network to be pure IPv6 and therefore the access operator not to have to manage access IPv4 routing;

· for the home gateways to have no concept of IPv4 and to manage only IPv6;

· for the terminals of the home network of the home gateway to use only IPv6.

The same IPv4 address may be assigned to a plurality of home gateways (or other equipments in contexts other than domestic Internet access). This means a dummy assignment at home gateway level, as home gateways do not manage IPv4 routing. The basic principles are as follows:

· range of authorized source ports at each gateway for outgoing calls;

· particular IPv6 prefix IPv6_prefix_ports_range.

IPv4 packets entering the IPv6 domain are translated into IPv6 packets, rather than being encapsulated by the IPv6/IPv4_Access_Node to be routed to the home gateway.

· For outgoing calls, on DNS resolution of an IPv4 called party, an IPv6 address is returned to the initiator user terminal that was constructed on the basis of the IPv4 address of the called party. The user

terminal then uses this IPv6 destination address to send data packets. It may use its IPv6 native or constructed source address to send packets.

· If it uses its native source address, the home gateway transforms the IPv6 native source address into an IPv6 constructed source address containing its own IPv4 address shared between the gateways (shared@IPv4) and the source port (inscribed in the authorized source range).

· An equipment interconnecting the IPv6 domain and the IPv4 domain verifies that the home gateway has used its range of authorized source ports by comparing the part of the source address that contains the source port bits and the source port in the port field of the IPv6 packet. It translates the IPv6 packet into an IPv4 packet to transmit it to the called party using:

· for the IPv4 source address, the bits in the IPv6 source address that contain shared@IPv4;

· for the IPv4 destination address, the bits in the IPv6 address that contain the IPv4 address of the called party.

CLAIMS

1. A receiving method for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet including an IPv6 destination address and an IPv6 source address, characterized in that, said method being executed in a home gateway adapted to connect a user terminal to said IPv6 domain, it includes the following steps:

· identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address and a destination port number;

· if necessary, regularizing at least one address of the data packet by replacing said address, the replacement process belonging to a group comprising replacement of a constructed address with a native address and replacement of a native address with a constructed address, and modifying the data packet using the regularized address; and

· routing the modified data packet to its destination.

2. A receiving method according to claim 1, characterized in that, when the data packet comes from said user terminal and goes to the IPv4 domain, the step of regularizing the source address further includes the following steps:

· identifying an IPv6 native source address;

· creating an entry in an address translation table, said entry associating said native source address with a source address constructed by concatenating an operator prefix, an IPv4 address assigned to the gateway, and a source port number belonging to a range of port numbers authorized for said gateway; and

· replacing the native source address of the data packet with the constructed source address.

3. A receiving method according to claim 2, characterized in that address identification uses an identifier contained in the destination address.

4. A receiving method according to claim 2, characterized in that it further includes a step of verifying that the source port number of the data packet and the source port number of the constructed source address match.

5. A receiving method according to claim 1, characterized in that, when the data packet comes from the IPv4 domain and goes to said user terminal, the step of regularizing the source address includes the following steps:

· searching an address translation table of the gateway for an entry associating with said constructed destination address a native destination address;

· if an entry is found, replacing the constructed destination address of the data packet with the native destination address from that entry.

6. A receiving method according to claim 5, characterized in that it further includes a step of verifying that the destination port number of the data packet and the destination port number contained in the constructed destination address match.

7. A device for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet including an IPv6 destination address and an IPv6 source address, characterized in that, said device being intended to be used in a home gateway adapted to connect a user terminal to said IPv6 domain, it includes:

· means for identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address, and a destination port number;

· means for regularizing, if necessary, at least one address of the data packet by replacing said address, the

replacement process belonging to a group comprising replacement of a constructed address with a native address and replacement of a native address with a constructed address, and modifying the data packet using the regularized address; and

· means for routing the modified data packet to its destination.

8. A home gateway adapted to connect user terminals of a home network to an IPv6 domain connected to an IPv4 domain, characterized in that it includes:

· means for obtaining an IPv4 address, a range of port numbers authorized for said gateway, and a range of IPv6 addresses authorized for said gateway, said range of IPv6 addresses being constructed by concatenating an operator prefix, said IPv4 address, and the range of authorized IPv4 port numbers; and

· a device according to claim 7 for receiving an IPv6 data packet in the IPv6 domain connected to the IPv4 domain.

9. A home gateway according to claim 8, including an address translation table containing entries associating at least one source address for a communications session involving a user terminal of its home network, characterized in that said gateway is adapted to store in said entry an IPv6 constructed source address and an IPv6 native source address.

10. A computer program product downloadable from a communications network and/or stored on a computer-readable medium and/or executable by a microprocessor, characterized in that it includes program code instructions for executing the method according to claim 1 of receiving a data packet in an IPv6 domain.

A B S T R A C T

A METHOD OF RECEIVING A DATA PACKET IN AN IPv6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

The invention provides a method of receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet including an IPv6 destination address and an IPv6 source address. According to the invention, such a method includes the following steps:

· identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address, and a destination port number;

· if necessary, regularizing at least one address of the data packet and modifying the data packet; and

· routing the modified data packet to its destination.

Translation of the title and the abstract as they were when originally filed by the Applicant. No account has been taken of any changes that might have been made subsequently by the PCT Authorities acting ex officio, e.g. under PCT Rules 37.2, 38.2, and/or 48.3.

Juniper Exhibit 1002, page 45

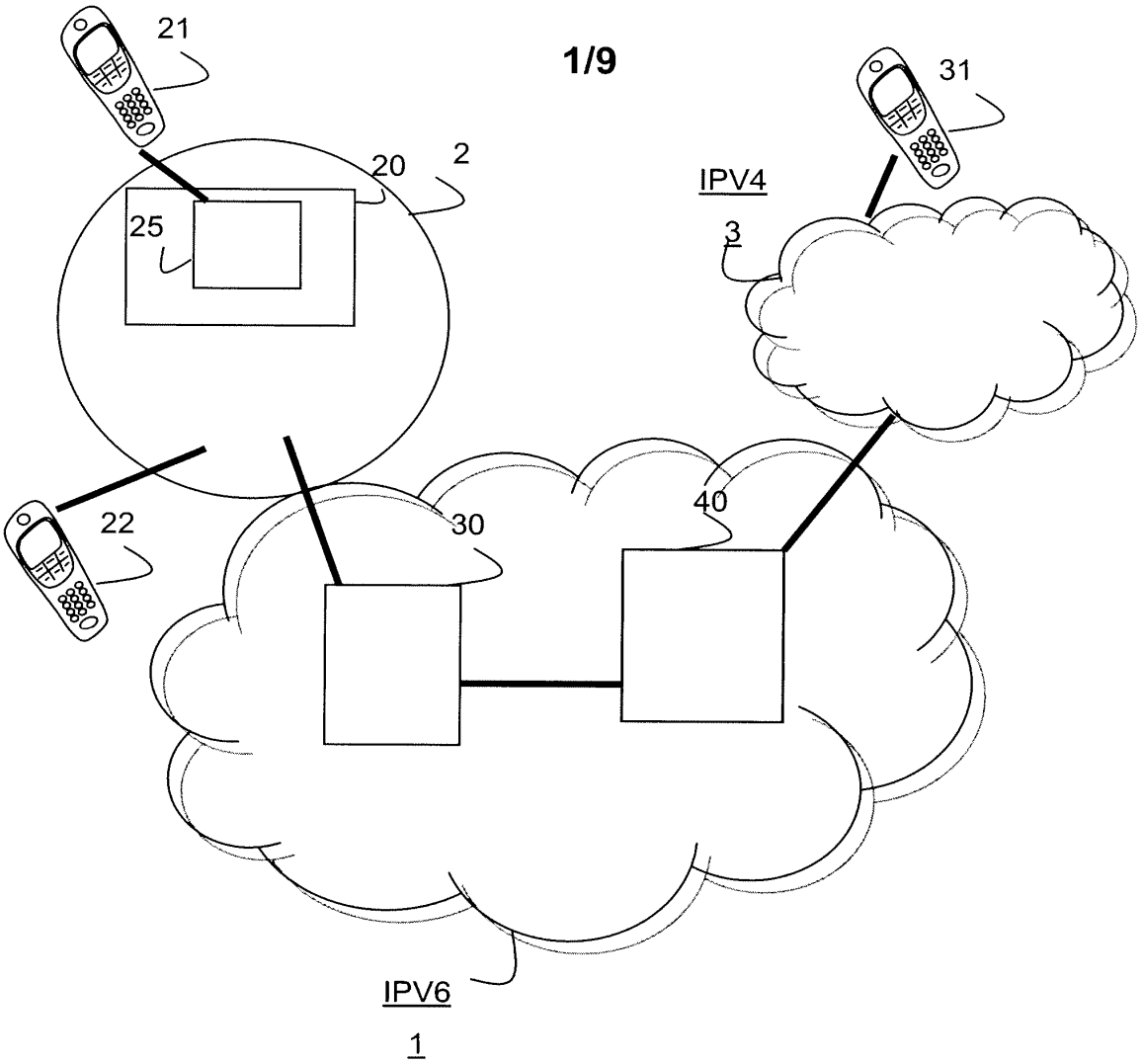


FIG. 1

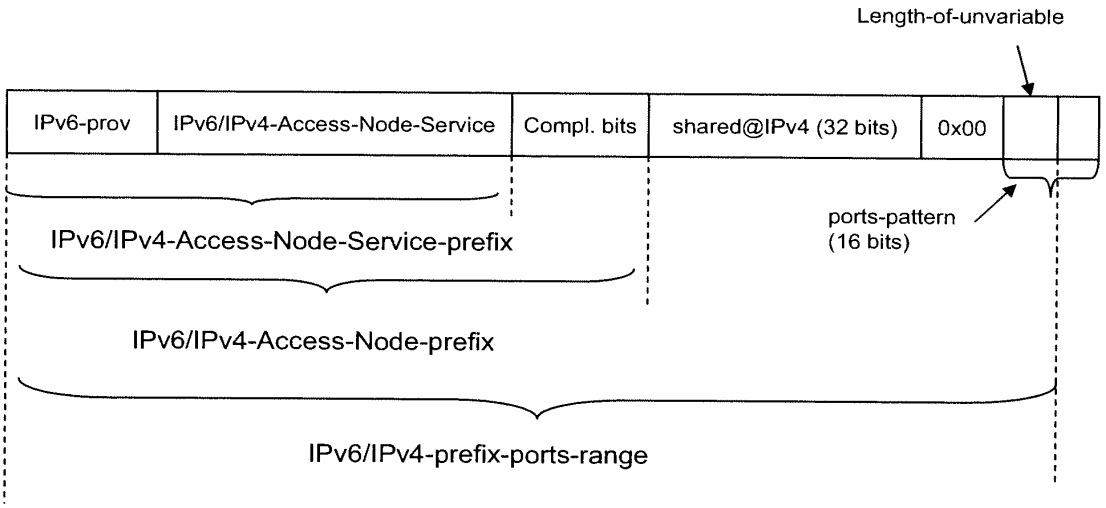

Length-of-unvariable
IPv6-prov
IPv6/IPv4-Access-Node-Service
Compl. bits
shared@IPv4 (32 bits)
0x00
ports-pattern
(16 bits)
IPv6/IPv4-Access-Node-Service-prefix
IPv6/IPv4-Access-Node-prefix
IPv6/IPv4-prefix-ports-range

FIG. 2

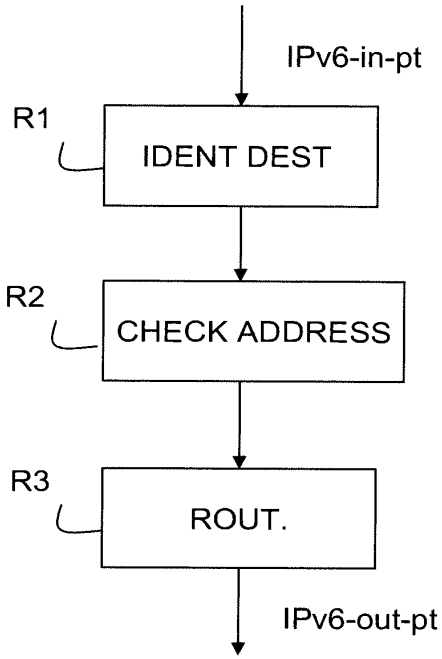


FIG. 3

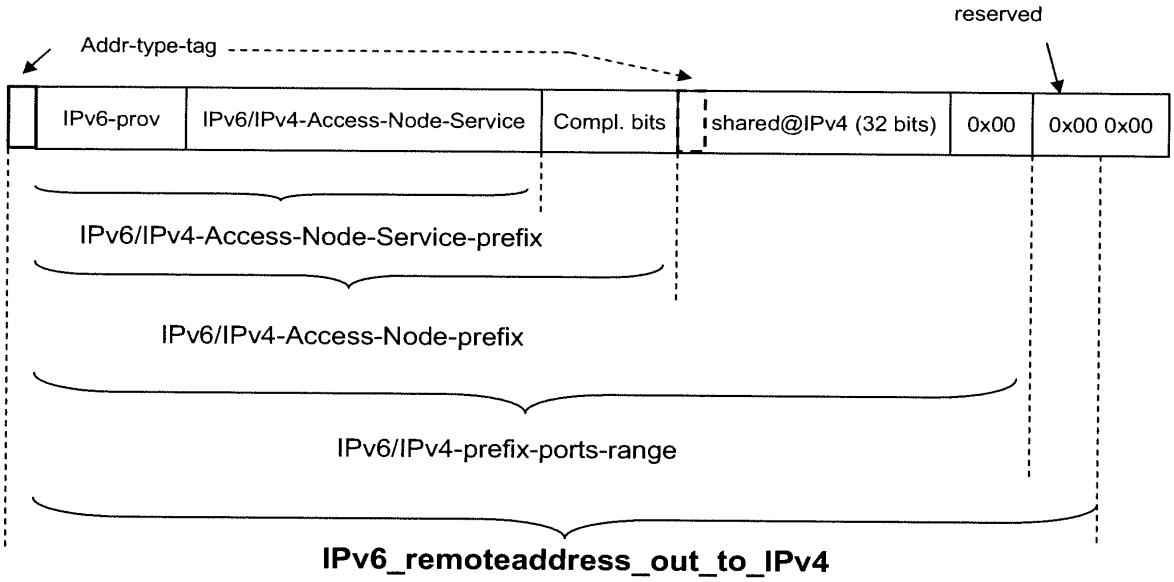

reserved
Addr-type-tag
IPv6-prov
IPv6/IPv4-Access-Node-Service
Compl. bits
shared@IPv4 (32 bits)
0x00
0x00 0x00
IPv6/IPv4-Access-Node-Service-prefix
IPv6/IPv4-Access-Node-prefix
IPv6/IPv4-prefix-ports-range
IPv6_remoteaddress_out_to_IPv4

FIG. 4

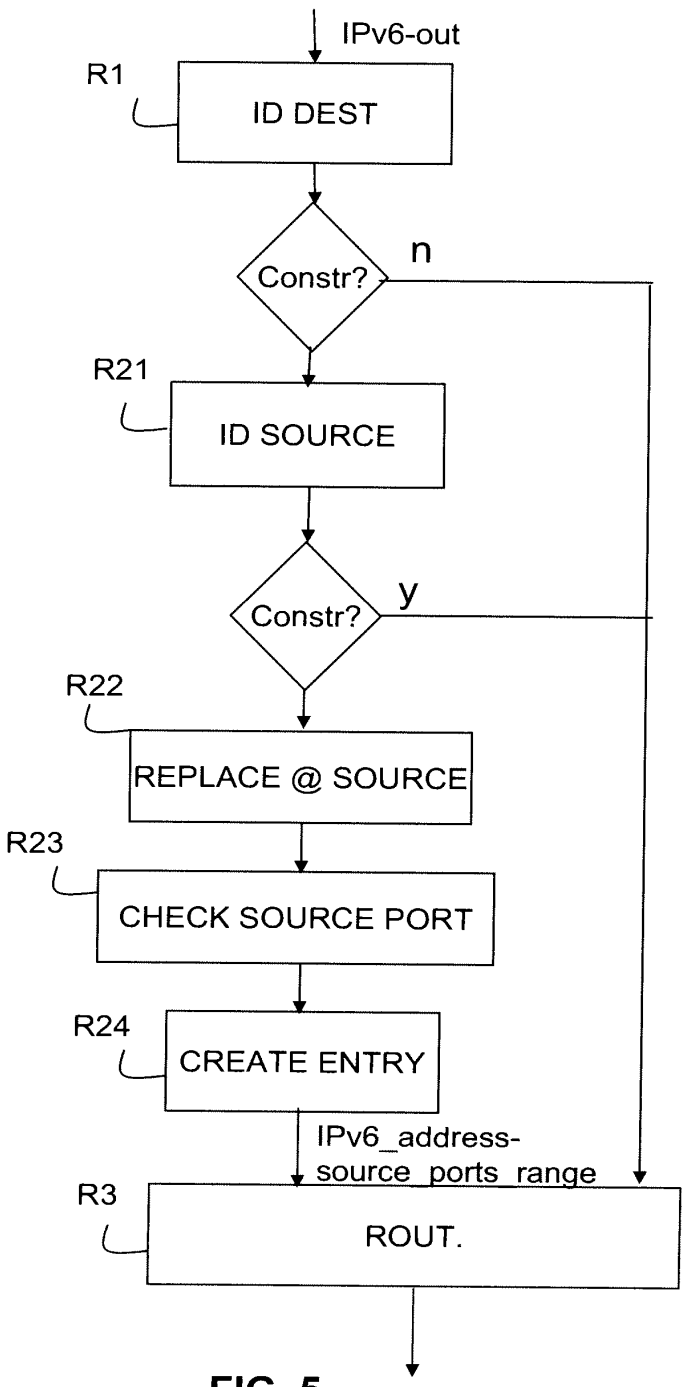

IPv6-out
R1
ID DEST
Constr?
n
R21
ID SOURCE
Constr?
y
R22
REPLACE @ SOURCE
R23
CHECK SOURCE PORT
R24
CREATE ENTRY
IPv6_address-
source_ports_range
R3
ROUT.

FIG. 5

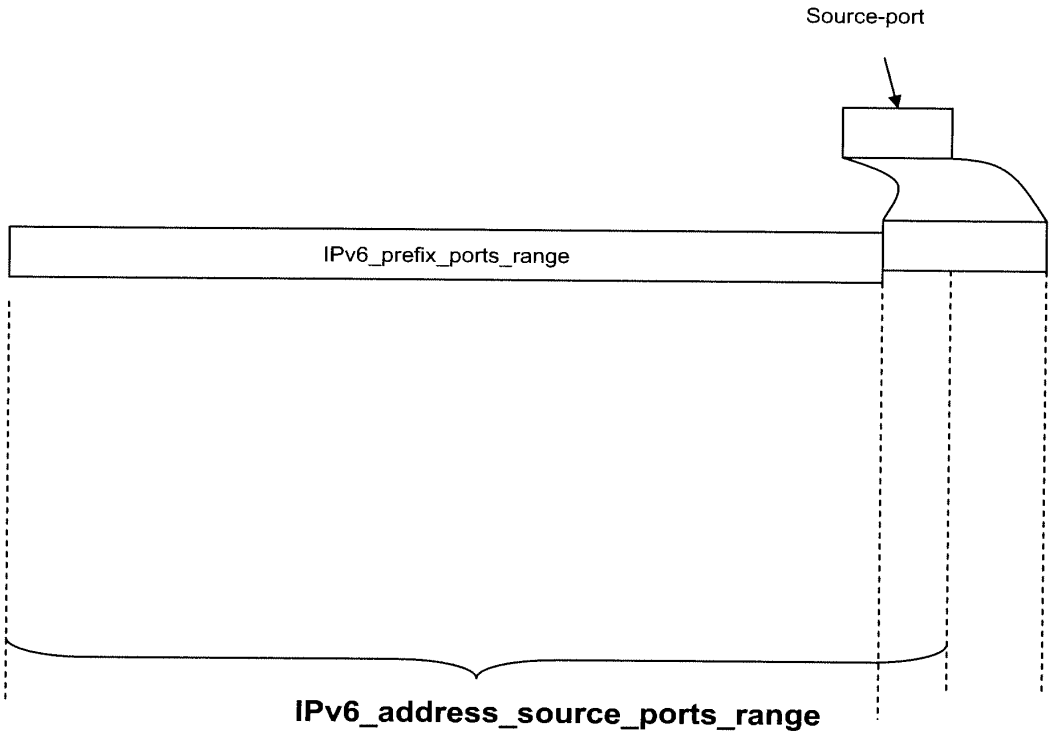

Source-port
IPv6_prefix_ports_range
IPv6_address_source_ports_range

FIG. 6

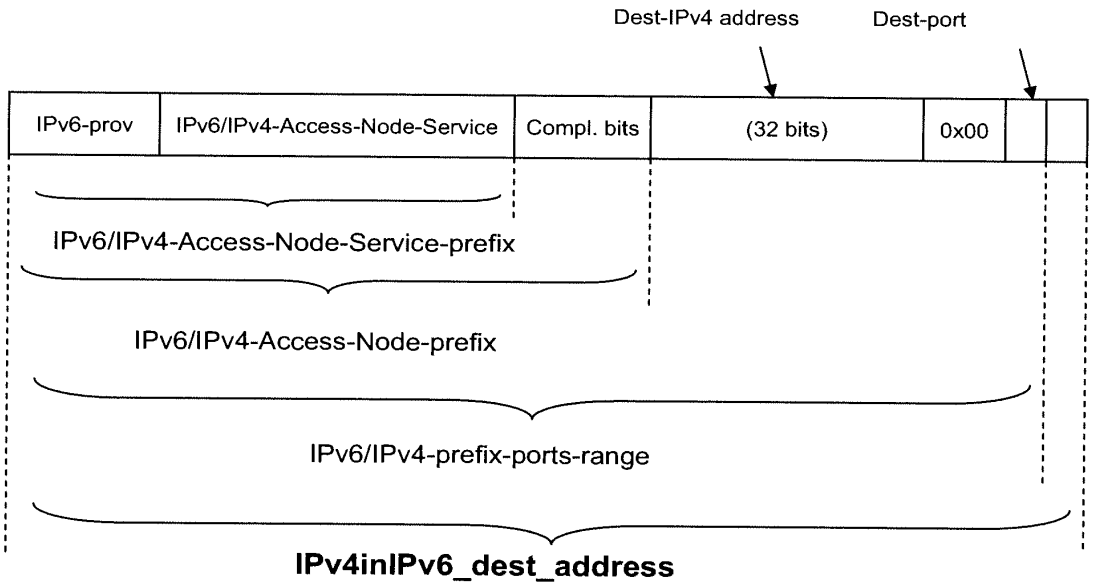

Dest-IPv4 address
Dest-port
IPv6-prov
IPv6/IPv4-Access-Node-Service
Compl. bits
(32 bits)
0x00
IPv6/IPv4-Access-Node-Service-prefix
IPv6/IPv4-Access-Node-prefix
IPv6/IPv4-prefix-ports-range
IPv4inIPv6_dest_address

FIG. 7

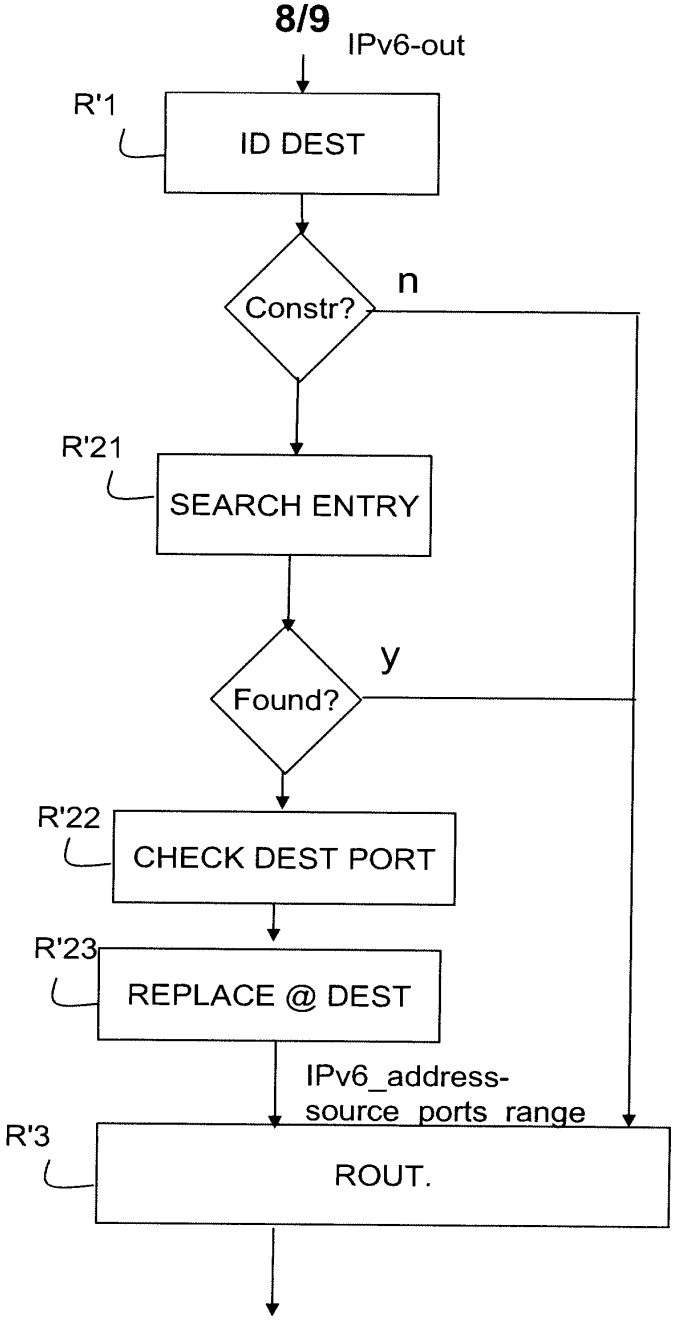

IPv6-out
R'1
ID DEST
Constr?
n
R'21
SEARCH ENTRY
Found?
y
R'22
CHECK DEST PORT
R'23
REPLACE @ DEST
IPv6_address-
source_ports_range
R'3
ROUT.

FIG. 8

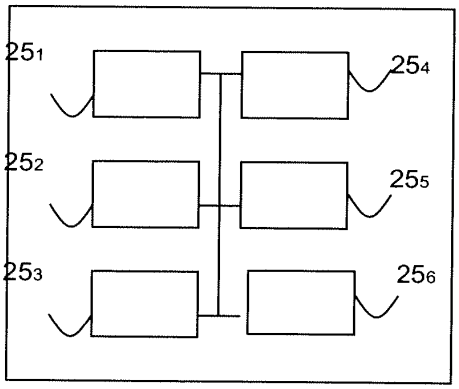


FIG. 9

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: Mohamed BOUCADAIR and Jean-Luc GRIMAULT

Serial No:

Filed:

For: A METHOD OF RECEIVING A DATA PACKET IN AN IPv6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

DECLARATION

I, Andrew Scott Marland, of 11, rue de Florence, 75008 Paris, France, declare that I am well acquainted with the English and French languages and that the attached translation of the French language PCT international application, Serial No. **PCT/FR2009/051228** is a true and faithful translation of that document as filed.

All statements made herein are to my own knowledge true, and all statements made on information and belief are believed to be true; and further, these statements are made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any document or any registration resulting therefrom.

Date: November 19, 2010

Andrew Scott Marland

TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

Expéditeur : L'ADMINISTRATION CHARGEE DE LA RECHERCHE INTERNATIONALE

Destinataire

FRANCE TELECOM
R&D/PIV/Brevets
38-40 Rue du Général Leclerc
92794 Issy-Les-Moulineaux Cedex 9
FRANCE

Le 26/11/2009

RRF: RRI PIV/Brevets

PCT

NOTIFICATION DE TRANSMISSION DU RAPPORT DE RECHERCHE INTERNATIONALE ET DE L'OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE OU DE LA DÉCLARATION
(règle 44.1 du PCT)

Référence du dossier du déposant ou du mandataire 07049-WO MI/NB	Date d'expédition *(jour/mois/année)* 20/11/2009
Demande internationale n° PCT/FR2009/051228	**POUR SUITE À DONNER** voir les paragraphes 1 et 4 ci-après
Déposant FRANCE TELECOM	Date du dépôt international *(jour/mois/année)* 26/06/2009

1. [x] Il est notifié au déposant que le rapport de recherche internationale a été établi et lui est transmis ci-joint.

Dépôt de modifications et d'une déclaration selon l'article 19 :
Le déposant peut, s'il le souhaite, modifier les revendications de la demande internationale (voir la règle 46):

Quand? Le délai dans lequel les modifications doivent être déposées est de deux mois à compter de la date de transmission du rapport de recherche internationale.

Où? Directement auprès du Bureau International de l'OMPI, 34, chemin des Colombettes 1211 Genève 20, Suisse, n° de télécopieur: +41 22 338 82 70

Pour des instructions plus détaillées, voir les notes sur la feuille d'accompagnement.

2. [ ] Il est notifié au déposant qu'il ne sera pas établi de rapport de recherche internationale et que la déclaration à cet effet, prévue à l'article 17.2)a), ainsi que l'opinion écrite de l'administration chargée de la recherche internationale sont transmises par le présent formulaire.

3. [ ] **En ce qui concerne la réserve** pouvant être formulée, conformément à la règle 40.2, à l'égard du paiement d'une ou de plusieurs taxes additionnelles, il est notifié au déposant que

[ ] la réserve ainsi que la décision y relative ont été transmises au Bureau international en même temps que la requête du déposant tendant à ce que le texte de la réserve et celui de la décision en question soient notifiés aux offices désignés.

[ ] la réserve n'a encore fait l'objet d'aucune décision; dès qu'une décision aura été prise, le déposant en sera avisé.

4. **Rappels**

Peu après l'expiration d'un délai de **18 mois** à compter de la date de priorité, la demande internationale sera publiée par le Bureau international. Si le déposant souhaite éviter ou différer la publication, il doit faire parvenir au Bureau international une déclaration de retrait de la demande internationale, ou de la revendication de priorité, conformément aux règles 90*bis*.1 et 90*bis*.3, respectivement, avant l'achèvement de la préparation technique de la publication internationale.

Le déposant a la possibilité de présenter des observations de manière informelle au Bureau international sur l'opinion écrite de l'administration chargée de la recherche internationale. Le Bureau international enverra aux offices désignés une copie de ces observations, à moins qu'un rapport d'examen préliminaire international ait été établi ou doive être établi. Ces observations seraient également mises à la disposition des tiers mais pas avant l'expiration d'un délai de 30 mois à compter de la date de priorité.

Dans un délai de **19 mois** à compter de la date de priorité, mais seulement en ce qui concerne certains offices désignés, le déposant doit présenter une demande d'examen préliminaire international s'il souhaite que l'ouverture de la phase nationale soit **reportée à 30 mois** à compter de la date de priorité (ou même au-delà dans certains offices); si tel n'est pas le cas, le déposant doit accomplir, dans un délai de **20 mois** à compter de la date de priorité, les démarches prescrites pour l'ouverture de la phase nationale auprès de ces offices désignés.

En ce qui concerne d'autres offices désignés, le délai de **30 mois** (ou plus) s'appliquera même si aucune demande d'examen préliminaire international n'est présentée dans le délai de 19 mois.

Voir l'annexe du formulaire PCT/IB/301 et, pour plus de précisions quant aux délais applicables, office par office, voir les chapitres nationaux dans le volume II du *Guide du déposant du PCT* et le site internet de l'OMPI.

Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Fonctionnaire autorisé Claude Berthon

Formulaire PCT/ISA/220 (octobre 2005) *(Voir les notes sur la feuille d'accompagnement)*

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220

Les présentes notes sont destinées à donner les instructions essentielles concernant le dépôt de modifications selon l'article 19. Les notes sont fondées sur les exigences du Traité de coopération en matière de brevets (PCT), du règlement d'exécution et des instructions administratives du PCT. En cas de divergence entre les présentes notes et ces exigences, ce sont ces dernières qui priment. Pour de plus amples renseignements, on peut aussi consulter le *Guide du déposant du PCT*, qui est une publication de l'OMPI.

Dans les présentes notes, les termes "article", "règle" et "instruction" renvoient aux dispositions du traité, de son règlement d'exécution et des instructions administratives du PCT, respectivement.

INSTRUCTIONS CONCERNANT LES MODIFICATIONS SELON L'ARTICLE 19

Après réception du rapport de recherche internationale et de l'opinion écrite de l'administration chargée de la recherche internationale, le déposant a la possibilité de modifier une fois les revendications de la demande internationale. On notera cependant que, comme toutes les parties de la demande internationale (revendications, description et dessins) peuvent être modifiées au cours de la procédure d'examen préliminaire international, il n'est généralement pas nécessaire de déposer de modifications des revendications selon l'article 19 sauf, par exemple, au cas où le déposant souhaite que ces dernières soient publiées aux fins d'une protection provisoire ou a une autre raison de modifier les revendications avant la publication internationale. En outre, il convient de rappeler que l'obtention d'une protection provisoire n'est possible que dans certains États (voir les annexes B1 et B2 du volume I du *Guide du déposant du PCT*).

L'attention du déposant est attirée sur le fait que des modifications des revendications selon l'article 19 ne sont pas permises lorsque l'administration chargée de la recherche internationale a déclaré, conformément à l'article 17.2), qu'aucun rapport de recherche internationale ne sera établi (voir le paragraphe 296 du volume I du *Guide du déposant du PCT*).

Quelles parties de la demande internationale peuvent être modifiées?

Selon l'article 19, les revendications exclusivement.

Durant la phase internationale, les revendications peuvent aussi être modifiées (ou modifiées à nouveau) selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international. La description et les dessins ne peuvent être modifiées que selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international.

Lors de l'ouverture de la phase nationale, toutes les parties de la demande internationale peuvent être modifiées selon l'article 28 ou, le cas échéant, selon l'article 41.

Quand? Dans un délai de deux mois à compter de la date de transmission du rapport de recherche internationale ou de 16 mois à compter de la date de priorité, selon l'échéance la plus tardive. Il convient cependant de noter que les modifications seront réputées avoir été reçues en temps voulu si elles parviennent au Bureau international après l'expiration du délai applicable mais avant l'achèvement de la préparation technique de la publication internationale (règle 46.1).

Où ne pas déposer les modifications?

Les modifications ne peuvent être déposées qu'auprès du Bureau international; elles ne peuvent être déposées ni auprès de l'office récepteur ni auprès de l'administration chargée de la recherche internationale (règle 46.2).

Lorsqu'une demande d'examen préliminaire international a été/est déposée, voir plus loin.

Comment? Soit en supprimant entièrement une ou plusieurs revendications, soit en ajoutant une ou plusieurs revendications nouvelles ou encore en modifiant le texte d'une ou de plusieurs des revendications telles que déposées.

Une feuille de remplacement doit être remise pour chaque feuille des revendications qui, en raison d'une ou de plusieurs modifications, diffère de la feuille initialement déposée.

Toutes les revendications figurant sur une feuille de remplacement doivent être numérotées en chiffres arabes. Si une revendication est supprimée, il n'est pas obligatoire de renuméroter les autres revendications. Chaque fois que des revendications sont renumérotées, elles doivent l'être de façon continue (instruction 205.b)).

Les modifications doivent être effectuées dans la langue dans laquelle la demande internationale est publiée.

Quels documents doivent/peuvent accompagner les modifications?

Lettre (instruction 205.b)):

Les modifications doivent être accompagnées d'une lettre.

La lettre ne sera pas publiée avec la demande internationale et les revendications modifiées. Elle ne doit pas être confondue avec la "déclaration selon l'article 19.1)" (voir plus loin sous "Déclaration selon l'article 19.1)").

La lettre doit être rédigée en anglais ou en français, au choix du déposant. Cependant, si la langue de la demande internationale est l'anglais, la lettre doit être rédigée en anglais; si la langue de la demande internationale est le français, la lettre doit être rédigée en français.

Juniper Exhibit 1002, page 57

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220 (suite)

La lettre doit indiquer les différences existant entre les revendications telles que déposées et les revendications telles que modifiées. Elle doit indiquer en particulier, pour chaque revendication figurant dans la demande internationale (étant entendu que des indications identiques concernant plusieurs revendications peuvent être groupées), si

i) la revendication n'est pas modifiée;
ii) la revendication est supprimée;
iii) la revendication est nouvelle;
iv) la revendication remplace une ou plusieurs revendications telles que déposées;
v) la revendication est le résultat de la division d'une revendication telle que déposée.

Les exemples suivants illustrent la manière dont les modifications doivent être expliquées dans la lettre d'accompagnement:

1. [Lorsque le nombre des revendications déposées initialement s'élevait à 48 et qu'à la suite d'une modification de certaines revendications il s'élève à 51]:
"Revendications 1 à 29, 31, 32, 34, 35, 37 à 48 remplacées par les revendications modifiées portant les mêmes numéros; revendications 30, 33 et 36 pas modifiées; nouvelles revendications 49 à 51 ajoutées."

2. [Lorsque le nombre des revendications déposées initialement s'élevait à 15 et qu'à la suite d'une modification de toutes les revendications il s'élève à 11]:
"Revendications 1 à 15 remplacées par les revendications modifiées 1 à 11."

3. [Lorsque le nombre des revendications déposées initialement s'élevait à 14 et que les modifications consistent à supprimer certaines revendications et à en ajouter de nouvelles]:
"Revendications 1 à 6 et 14 pas modifiées; revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées." ou
"Revendications 7 à 13 supprimées; nouvelles revendications 15, 16 et 17 ajoutées; toutes les autres revendications pas modifiées."

4. [Lorsque plusieurs sortes de modifications sont faites]:
"Revendications 1–10 pas modifiées; revendications 11 à 13, 18 et 19 supprimées; revendications 14, 15 et 16 remplacées par la revendication modifiée 14; revendication 17 divisée en revendications modifiées 15, 16 et 17; nouvelles revendications 20 et 21 ajoutées."

"Déclaration selon l'article 19.1)" (Règle 46.4)

Les modifications peuvent être accompagnées d'une déclaration expliquant les modifications et précisant l'incidence que ces dernières peuvent avoir sur la description et sur les dessins (qui ne peuvent pas être modifiés selon l'article 19.1)).

La déclaration sera publiée avec la demande internationale et les revendications modifiées.

Elle doit être rédigée dans la langue dans laquelle la demande internationale est publiée.

Elle doit être succincte (ne pas dépasser 500 mots si elle est établie ou traduite en anglais).

Elle ne doit pas être confondue avec la lettre expliquant les différences existant entre les revendications telles que déposées et les revendications telles que modifiées, et ne la remplace pas. Elle doit figurer sur une feuille distincte et doit être munie d'un titre permettant de l'identifier comme telle, constitué de préférence des mots "Déclaration selon l'article 19.1)"

Elle ne doit contenir aucun commentaire dénigrant relatif au rapport de recherche internationale ou à la pertinence des citations que ce dernier contient. Elle ne peut se référer à des citations se rapportant à une revendication donnée et contenues dans le rapport de recherche internationale qu'en relation avec une modification de cette revendication.

Conséquence du fait qu'une demande d'examen préliminaire international ait déjà été présentée

Si, au moment du dépôt de modifications et, le cas échéant, d'une déclaration, effectuées en vertu de l'article 19, une demande d'examen préliminaire international a déjà été présentée, le déposant doit de préférence, lors du dépôt des modifications (et, le cas échéant, de la déclaration) auprès du Bureau international, déposer également une copie de ces modifications (et, le cas échéant, de cette déclaration) auprès de l'administration chargée de l'examen préliminaire international et, si nécessaire, une traduction de ces modifications aux fins de la procédure auprès de cette administration (voir les règles 55.3.a) et 62.2, première phase). Pour plus de précisions, se référer aux notes du formulaire de demande d'examen préliminaire international (PCT/IPEA/401).

Si une demande d'examen préliminaire international est présentée, l'opinion écrite de l'administration chargée de la recherche internationale sera –sauf dans les cas dans lesquels l'administration chargée de l'examen préliminaire international n'a pas agi en qualité d'administration chargée de la recherche internationale et lorsqu'elle a effectué auprès du Bureau international la notification prévue à la règle 66.1 *bis*.b)– considérée comme une opinion écrite de l'administration chargée de l'examen préliminaire international. Si la demande d'examen est présentée, le déposant a la possibilité de remettre à l'administration chargée de l'examen préliminaire international une réponse à l'opinion écrite, accompagnée, le cas échéant, de modifications, et ce avant l'expiration d'un délai de 3 mois à compter de la date d'expédition du formulaire PCT/ISA/220 ou d'un délai de 22 mois à compter de la date de priorité, le délai expirant en dernier s'appliquant (règle 43*bis*.1.c)).

Conséquence au regard de la traduction de la demande internationale lors de l'ouverture de la phase nationale

L'attention du déposant est appelée sur le fait qu'il peut avoir à remettre aux offices désignés ou élus, lors de l'ouverture de la phase nationale, une traduction des revendications telles que modifiées en vertu de l'article 19 au lieu de la traduction des revendications telles que déposées ou en plus de celle–ci.

Pour plus de précisions sur les exigences de chaque office désigné ou élu, voir le volume II du *Guide du déposant du PCT*.

Juniper Exhibit 1002, page 58

TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire 07049-WO	**POUR SUITE À DONNER** voir le formulaire PCT/ISA/220 et, le cas échéant, le point 5 ci-après.	
Demande internationale n° PCT/FR2009/051228	Date du dépôt international *(jour/mois/année)* 26/06/2009	(Date de priorité (la plus ancienne) *(jour/mois/année)* 30/06/2008
Déposant FRANCE TELECOM		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 5 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**
   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base
      [X] de la demande internationale dans la langue dans laquelle elle a été déposée
      [ ] d'une traduction de la demande internationale dans la langue suivante _____, qui est la langue d'une traduction remise aux fins de la recherche internationale (règles 12.3.a) et 23.1.b))
   b. [ ] Le présent rapport de recherche internationale a été établi en prenant en considération la **rectification d'une erreur évidente** autorisée par ou notifiée à la presente administration vertu de la règle 91 (Règle 43.6*bis*(a)).
   c. [ ] En ce qui concerne **la ou les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale, (le cas échéant), voir le cadre n° I.
2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre n° II).
3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre n° III).
4. En ce qui concerne le **titre,**
   [X] le texte est approuvé tel qu'il a été remis par le déposant
   [ ] le texte a été établi par l'administration chargée de la recherche internationale et a la teneur suivante:
5. En ce qui concerne **l'abrégé,**
   [X] le texte est approuvé tel qu'il a été remis par le déposant
   [ ] le texte, reproduit dans le cadre n° IV, a été établi par l'administration chargée de la recherche internationale conformément à la règle 38.2(b). Le déposant peut présenter des observations à l'administration chargée de la recherche internationale dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale
6. En ce qui concerne les **dessins,**
   a. La figure **des dessins** à publier avec l'abrégé est la figure n° 3
      [X] proposée par le déposant
      [ ] proposée par l'administration chargée de la recherche internationale, parce que le déposant n'a pas proposé de figure
      [ ] proposée par l'administration chargée de la recherche internationale, parce que cette figure caractérise mieux l'invention
   b. [ ] Aucune des figures n'est publiée avec l'abrégé

Juniper Exhibit 1002, page 59

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/051228

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/12

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	MYUNG-KI SHIN ET AL: "Ports option support in dual stack transition mechanism (DSTM)" ADVANCED COMMUNICATION TECHNOLOGY, 2004. THE 6TH INTERNATIONAL CONFERE NCE ON PHOENIX PARK, KOREA FEB. 9-11, 2004, PISCATAWAY, NJ, USA,IEEE, vol. 1, 9 février 2004 (2004-02-09), pages 225-228, XP010701165 ISBN: 978-89-5519-119-6 abrégé * partie I* * partie III * * partie IV.B * ----- -/--	1-10

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Categories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
13 novembre 2009	20/11/2009

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Fax: (+31–70) 340–3016	Poppe, Fabrice

2

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

Juniper Exhibit 1002, page 60

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n° PCT/FR2009/051228

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 2004/039014 A (CISCO TECH IND [US]) 6 mai 2004 (2004-05-06) abrégé page 5, ligne 9 - ligne 17 page 9, ligne 6 - page 10, ligne 2; figure 4 page 10, ligne 3 - page 12, ligne 3; figure 5 page 13, ligne 5 - page 14, ligne 9	1-10
X	DANIEL PARK ET AL: "Network Address Translation - Protocol Translation (NAT-PT); draft-daniel-natpt-bis-01.txt" INTERNET ENGINEERING TASK FORCE, IETF, 22 octobre 2005 (2005-10-22), XP015042124 abrégé alinéa [0002] alinéa [0005]	1-10
A	SRISURESH P ET AL: "RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations" INTERNET CITATION, [Online] XP002204216 Extrait de l'Internet: URL:http://www.ietf.org/rfc/rfc2663.txt> [extrait le 2002-07-01] le document en entier	1-10
A	EP 1 420 559 A (THOMSON LICENSING SA [FR]) 19 mai 2004 (2004-05-19) abrégé alinéa [0002] - alinéa [0009] alinéa [0030] - alinéa [0034]; figure 4	1-10
A	AFIFI H ET AL: "Methods for IPv4-IPv6 transition" COMPUTERS AND COMMUNICATIONS, 1999. PROCEEDINGS. IEEE INTERNATIONAL SY MPOSIUM ON RED SEA, EGYPT 6-8 JULY 1999, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 6 juillet 1999 (1999-07-06), pages 478-484, XP010555073 ISBN: 978-0-7695-0250-2 abrégé alinéa [0003]	1-10
A	WO 2007/099248 A (FRANCE TELECOM [FR]; BOUCADAIR MOHAMED [FR]; NOISETTE YOANN [FR]) 7 septembre 2007 (2007-09-07) le document en entier	1-10
A	WO 2008/001007 A (FRANCE TELECOM [FR]; BOUCADAIR MOHAMED [FR]; NOISETTE YOANN [FR]) 3 janvier 2008 (2008-01-03) le document en entier	1-10

-/--

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/051228

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	KAWARASAKI Y ET AL: "IPv4/IPv6 SIP interworking methods in dual-stack network" COMMUNICATIONS, 2003. APCC 2003. THE 9TH ASIA-PACIFIC CONFERENCE ON 21-24 SEPT. 2003, PISCATAWAY, NJ, USA,IEEE, vol. 3, 21 septembre 2003 (2003-09-21), pages 1124-1128, XP010687978 ISBN: 978-0-7803-8114-8 le document en entier -----	1-10

2

Juniper Exhibit 1002, page 62

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2009/051228

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 2004039014	A	06-05-2004	AT	352148 T	15-02-2007
			AU	2003282934 A1	13-05-2004
			CA	2502945 A1	06-05-2004
			CN	1706155 A	07-12-2005
			DE	60311297 T2	15-11-2007
			EP	1554841 A1	20-07-2005
			US	2004076180 A1	22-04-2004
EP 1420559	A	19-05-2004	AU	2003289873 A1	03-06-2004
			BR	0316112 A	27-09-2005
			CN	1711739 A	21-12-2005
			WO	2004045183 A1	27-05-2004
			JP	4339259 B2	07-10-2009
			JP	2006506839 T	23-02-2006
			KR	20050074998 A	19-07-2005
			MX	PA05004998 A	02-08-2005
			US	2006259639 A1	16-11-2006
WO 2007099248	A	07-09-2007	CN	101395891 A	25-03-2009
			EP	1994724 A2	26-11-2008
			FR	2898003 A1	31-08-2007
			JP	2009528742 T	06-08-2009
			US	2009041034 A1	12-02-2009
WO 2008001007	A	03-01-2008	EP	2036301 A2	18-03-2009
			FR	2903263 A1	04-01-2008
			US	2009187664 A1	23-07-2009

TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

Expéditeur : L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

Destinataire :

voir le formulaire PCT/ISA/220

PCT

OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE

(règle 43*bis*.1 du PCT)

Date d'expédition *(jour/mois/année)* PCT/ISA/210 (deuxième feuille)	voir le formulaire
Référence du dossier du déposant ou du mandataire: voir le formulaire PCT/ISA/220	**POUR SUITE À DONNER** Voir le point 2 ci-dessous

Demande internationale No.	Date du dépôt international *(jour/mois/année)*	Date de priorité *(jour/mois/année)*
PCT/FR2009/051228	26.06.2009	30.06.2008

Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB
INV. H04L29/12

Déposant
FRANCE TELECOM

1. La présente opinion contient des indications et les pages correspondantes relatives aux points suivants :

- ☒ Cadre n° I Base de l'opinion
- ☐ Cadre n° II Priorité
- ☐ Cadre n° III Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- ☐ Cadre n° IV Absence d'unité de l'invention
- ☒ Cadre n° V Déclaration motivée selon la règle 43*bis*.1(a)(i) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- ☐ Cadre n° VI Certains documents cités
- ☐ Cadre n° VII Certaines irrégularités relevées dans la demande internationale
- ☐ Cadre n° VIII Certaines observations relatives à la demande internationale

2. **SUITE À DONNER**

Si une demande d'examen préliminaire internationale est présentée, la présente opinion sera considérée comme une opinion écrite de l'administration chargée de l'examen préliminaire international, sauf dans le cas où le déposant a choisi une administration différente de la présente administration aux fins de l'examen préliminaire international et que l'administration considérée a notifié au Bureau international, selon la règle 66.1bis.b), qu'elle n'entend pas considérer comme les siennes les opinions écrites de la présente administration chargée de la recherche internationale.

Si, comme cela est indiqué ci-dessus, la présente opinion écrite est considérée comme l'opinion écrite de l'administration chargée de l'examen préliminaire international, le déposant est invité à soumettre à l'administration chargée de l'examen préliminaire international une réponse écrite, avec le cas échéant des modifications, avant l'expiration d'un délai de 3 mois à compter de la date d'envoi du formulaire PCT/ISA/220 ou avant l'expiration d'un délai de 22 mois à compter de la date de priorité, le délai expirant le dernier devant être appliqué.

Pour plus de détails sur les possibilités offertes au déposant, se référer au formulaire PCT/ISA/220.

3. Pour de plus amples détails, se référer aux notes relatives au formulaire PCT/ISA/220.

Nom et adresse postale de l'adminstration chargée de la recherche internationale	Date à laquelle la présente opinion a été établie	Fonctionnaire autorisé
Office européen des brevets P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tél. +31 70 340 - 2040 Fax: +31 70 340 - 3016	voir le formulaire PCT/ISA/210	Poppe, Fabrice N° de téléphone +31 70 340-4378

Formulaire PCT/ISA/237 (feuille de titre) (avril 2005)

Cadre n° I Base de l'opinion

1. En ce qui concerne la **langue**, la présente opinion a été établie sur la base

   ☒ de la demande internationale dans la langue dans laquelle elle a été déposée

   ☐ d'une traduction de la demande interationale dans la langue suivante , qui est la langue d'une traduction remise aux fins de la recherche internationale (règles 12.3.a) et 23.1.b)).

2. ☐ La présente opinion a été établie en prenant en considération la **rectification d'une erreur evidente** autorisée par ou notifiée à la présente administration en vertu de la règle 91 (règle 43bis.1.a)).

3. En ce qui concerne **la ou les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale, le cas échéant, la recherche internationale a été effectuée sur la base des éléments suivants :

   a. Nature de l'élément :

   ☐ un listage de la ou des séquences

   ☐ un ou des tableaux relatifs au listage de la ou des séquences

   b. Type de support :

   ☐ sur papier

   ☐ sous forme électronique

   c. Moment du dépôt ou de la remise :

   ☐ contenu(s) dans la demande internationale telle que déposée

   ☐ déposé(s) avec la demande internationale, sous forme électronique

   ☐ remis ultérieurement à la présente administration aux fins de la recherche

4. ☐ De plus, lorsque plus d'une version ou d'une copie d'un listage des séquences ou d'un ou plusieurs tableaux y relatifs a été déposée, les déclarations requises selon lesquelles les informations fournies ultérieurement ou au titre de copies supplémentaires sont identiques à celles initialement fournies et ne vont pas au-delà de la divulgation faite dans la demande internationale telle que déposée initialement, selon le cas, ont été remises.

5. Commentaires complémentaires :

Cadre n° V Déclaration motivée selon la règle 43*bis*.1(a)(i) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-10
	Non :	Revendications	
Activité inventive	Oui :	Revendications	1-10
	Non :	Revendications	
Possibilité d'application industrielle	Oui :	Revendications	1-10
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

Concernant le point V

Déclaration motivée quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

Il est fait référence aux documents suivants:

D1: MYUNG-KI SHIN ET AL: "Ports option support in dual stack transition mechanism (DSTM)" THE 6TH INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATION TECHNOLOGY, PHOENIX PARK, KOREA FEBRUARY 9-11, 2004, pages 225-228

D2: WO 2004/039014 A (CISCO TECH IND [US]) 6 mai 2004

D3: DANIEL PARK ET AL: "Network Address Translation - Protocol Translation (NAT-PT); draft-daniel-natpt-bis-01.txt" INTERNET ENGINEERING TASK FORCE, IETF, octobre 2005

D4: SRISURESH P ET AL: "RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations" INTERNET ENGINEERING TASK FORCE, IETF, auguste 1999

D5: EP-A-1 420 559 (THOMSON LICENSING SA [FR]) 19 mai 2004

D6: AFIFI H ET AL: "Methods for Ipv4-IPv6 transition" IEEE INTERNATIONAL SYMPOSIUM ON COMPUTERS AND COMMUNICATIONS, RED SEA, EGYPT 6-8 JULY 1999, pages 478-484

Clarté (Article 6 PCT)

Les revendications 1 et 7 ne sont pas claires dans quelques aspects. Le passage correspondant dans la description, page 29, lignes 4-29, sera utilisé pour l'interprétation de ces revendications, comme indiqué ci-dessous:

1. *si nécessaire, mise en conformité*: la description, page 29, lignes 8-13, spécifie qu'une adresse de destination construite, c'est-à-dire identifiée, est toujours mise en conformité. l'Etape d'identification est donc toujours suivi par une étape de mise en conformité.

2. *au moins une adresse*: la description, page 29, lignes 14-16, spécifie que c'est toujours seulement l'adresse IPv6 de destination qui est remplacée.

3. *un remplacement d'une adresse construite par une adresse native et un remplacement d'une adresse native par une adresse construite*: la description, page 29, lignes 8-24, spécifie que cette adresse native est l'adresse native IPv6 du terminal d'utilisateur.

4. *modification du paquet de données à l'aide de l'adresse mise en conformité*: cette modification est déjà implicite dans le remplacement de l'adresse, i.e. dans l'étape de mise en conformité.

Nouveauté (Article 33(2) PCT)

Le document D1, qui est considéré comme étant l'état de la technique le plus proche de l'objet de la revendication 1, décrit (les références entre parenthèses s'appliquent à ce document) :

un procédé de réception d'un paquet de données IPv6 dans un domaine IPv6 (figure 1; partie III.A: "the packet reaches the DSTM Border Router, TEP") *interconnecté avec un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source* (partie III.A: "outer source address, outer destination address"), *comprenant les étapes suivantes:*

- *identification d'une adresse IPv6 de destination* (partie III.A: implicite dans la réception du paquet IPv6)*;*

- *si nécessaire, mise en conformité d'au moins une adresse du paquet de données et modification du paquet de données à l'aide de l'adresse mise en conformité* (partie III.D: "When a tunnelled packet arrives to the IPv6 destination, the IPv6 header is removed and the packet is processed by the IPv4 layer (...) The TEP should cache the source port number as well as the association between the IPv4 and IPv6 source addresses, in order to identify the returning path of packets with the same IPv4 address.")*; et*

- *routage du paquet de données modifié vers sa destination* (partie III.D: "The IPv4 packet will then be forwarded by the TEP using the IPv4 infrastructure").

Par conséquent, l'objet de la revendication 1 diffère de ce procédé connu en ce que:

ledit procédé est mis en oeuvre dans une passerelle résidentielle apte à connecter un terminal d'utilisateur audit domaine IPv6;

l'adresse IPv6 de destination est construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination; et en ce que

la mise en conformité d'une adresse comprend un remplacement de ladite adresse, ledit remplacement appartenant à un groupe comprenant un remplacement d'une adresse construite par une adresse native et un remplacement d'une adresse native par une adresse construite,

L'objet de la revendication 1 est donc nouveau.

Activité inventive (Article 33(3) PCT)

Le problème que la présente invention se propose de résoudre peut donc être considéré comme faciliter l'interconnexion des domaines IPv6 avec des domaines IPv4 d'une manière efficace.

La solution de ce problème proposée dans la revendication 1 de la présente demande est considérée comme impliquant une activité inventive, parce qu'elle n'est ni décrit dans les documents citées dans le rapport de recherche, ni relevée d'une démarche technique normale à partir de ces documents.

Plus en particulier, il est vrai que D1 décrit un procédé qui comprend la construction des adresses "virtuelles" (partie III.B, III.C: "contact the DSTM server to obtain a range of ports to be used as well as a temporary IPv4 address"). Mais par contre, avec le procédé de D1, c'est le terminal d'utilisateur est responsable de construire ces adresses, qui ne sont que virtuelles, dans le sens que dans le cas particulier décrit dans D1, la paire (adresse IPv4, numéro de port) peut être considérée équivalente à une adresse IPv6. Il n'en est alors pas question d'un remplacement d'une adresse native par une adresse construite.

Le même argument s'applique mutatis mutandis à l'objet des revendications indépendantes correspondantes 7, 8 et 10 qui est donc aussi inventif.

Les revendications 2-6 et 8 dépendent des revendications 1 et 7 et satisfont donc également, en tant que telles, aux conditions en ce qui concerne la nouveauté et l'activité inventive.

Etapes possibles après réception du rapport de recherche internationale (ISR) et de l'opinion écrite de l'administration chargée de la recherche internationale (WO-ISA)

Informations générales	Pour toutes les demandes internationales déposées depuis le 1er janvier 2004, l'ISA compétente établit un ISR. Cet ISR est accompagné de la WO-ISA. Contrairement à l'ancienne opinion écrite de l'IPEA (règle 66.2 PCT), la WO-ISA n'est pas censée recevoir une réponse, mais doit être prise en considération pour les étapes suivantes de la procédure. Le présent document expose les diverses possibilités.
Modification des revendications au titre de l'article 19 PCT	Dans un délai de deux mois à compter de la date de transmission de l'ISR et de la WO-ISA, le déposant peut produire des revendications modifiées au titre de l'article 19 PCT directement auprès du Bureau international de l'OMPI. La réforme du PCT de 2004 n'a pas changé cette procédure. Pour plus d'informations, cf. règle 46 PCT et formulaire PCT/ISA/220 ainsi que les notes correspondantes relatives à ce formulaire.
Dépôt d'une demande d'examen préliminaire international	En principe, la WO-ISA est considérée comme l'opinion écrite de l'IPEA. Dans de nombreux cas, cela devrait rendre superflu le dépôt d'une demande d'examen préliminaire international. Si le déposant souhaite néanmoins déposer une telle demande, il doit le faire avant l'expiration de trois mois à compter de la date de transmission de l'ISR/WO-ISA, ou de 22 mois à compter de la date de priorité, selon celui de ces deux délais qui expire le plus tard (règle 54bis PCT). Comme auparavant, le déposant peut présenter auprès de l'IPEA des modifications en vertu de l'article 34 PCT, normalement en même temps qu'il présente sa demande d'examen préliminaire international (règle 66.1 b) PCT). Si une demande d'examen préliminaire international est présentée et qu'aucune observation/modification n'a été reçue, l'IPEA transforme la WO-ISA en un IPRP (rapport préliminaire international sur la brevetabilité), qui reprendra simplement le contenu de la WO-ISA. La demande pourra toujours être retirée en vertu de l'article 37 PCT.
Dépôt d'observations informelles	Après avoir reçu l'ISR/WO-ISA, le déposant peut présenter des observations informelles relatives à la WO-ISA directement auprès du Bureau international de l'OMPI. Ces observations sont communiquées aux offices désignés en même temps que l'IPRP (rapport préliminaire international sur la brevetabilité) au plus tôt 30 mois à compter de la date de priorité. Cf. également la case suivante.
Fin de la phase internationale	A la fin de la phase internationale, le Bureau international de l'OMPI transforme la WO-ISA ou, si une demande a été présentée, l'opinion écrite de l'IPEA, en un IPRP qui sera transmis en même temps que les éventuelles observations informelles communiquées aux offices désignés. L'IPRP remplace l'ancien IPER (rapport d'examen préliminaire international).
Règles PCT pertinentes & complément d'informations	Règle 43 PCT, règle 43bis PCT, règle 44 PCT, règle 44bis PCT, PCT Newsletter 12/2003, JO 11/2003, JO 12/2003.

BNSDOCID: <XS_____200704010CL_1>

Bitte beachten Sie, dass angeführte Nichtpatentliteratur (wie z. B. wissenschaftliche oder technische Dokumente) je nach geltendem Recht dem Urheberrechtsschutz und/oder anderen Schutzarten für schriftliche Werke unterliegen könnte. Die Vervielfältigung urheberrechtlich geschützter Texte, ihre Verwendung in anderen elektronischen oder gedruckten Publikationen und ihre Weitergabe an Dritte ist ohne ausdrückliche Zustimmung des Rechtsinhabers nicht gestattet.

Veuillez noter que les ouvrages de la littérature non-brevets qui sont cités, par exemple les documents scientifiques ou techniques, etc., peuvent être protégés par des droits d'auteur et/ou toute autre protection des écrits prévue par les législations applicables. Les textes ainsi protégés ne peuvent être reproduits ni utilisés dans d'autres publications électroniques ou imprimées, ni rediffusés sans l'autorisation expresse du titulaire du droit d'auteur.

Please be aware that cited works of non-patent literature such as scientific or technical documents or the like may be subject to copyright protection and/or any other protection of written works as appropriate based on applicable laws. Copyrighted texts may not be copied or used in other electronic or printed publications or re-distributed without the express permission of the copyright holder.

XS CPRTENFRDE

3NSDOCID: <XS. __2006100103CF_I_>

VIII-4-1	**Déclaration : Qualité d'inventeur (seulement aux fins de la désignation des États-Unis d'Amérique)** Déclaration relative à la qualité d'inventeur (règles 4.17.iv) et 51bis.1.a)iv)) aux fins de la désignation des États-Unis d'Amérique :	Par la présente, je declare que je crois être le premier inventeur original et unique (si un seul inventeur est mentionné ci-dessous) ou l'un des premiers coïnventeurs (si plusieurs inventeurs sont mentionnés ci-dessous) de l'objet revendiqué pour lequel un brevet est demandé. La présente déclaration a trait à la demande internationale PCT/FR2009/051228 (si la déclaration est remise en vertu de la règle 26ter) Par la présente, je déclare que mon domicile, mon adresse postale et ma nationalité sont tels qu'indiqués près de mon nom. Par la présente, je déclare avoir passé en revue et comprendre le contenu de la demande internationale à laquelle il est fait référence ci-dessus, y compris les revendications de ladite demande. J'ai indiqué dans la requête de ladite demande, conformément à la règle 4.10 du PCT, toute revendication de priorité d'une demande étrangère et j'ai identifié ci-dessous, sous l'intitulé "Demandes antérieures", au moyen du numéro de demande, du pays ou du membre de l'Organisation mondiale du commerce, du jour, du mois et de l'année du dépôt, toute demande de brevet ou de certificat d'auteur d'invention déposée dans un pays autre que les États-Unis d'Amérique, y compris toute demande internationale selon le PCT désignant au moins un pays autre que les États-Unis d'Amérique, dont la date de dépôt est antérieure à celle de la demande étrangère dont la priorité est revendiquée.
VIII-4-1-1	Demandes antérieures :	

		Par la présente, je reconnais l'obligation qui m'est faite de divulguer les renseignements dont j'ai connaissance et qui sont pertinents quant à la brevetabilité de l'invention, tels qu'ils sont définis dans le Titre 37, § 1.56, du Code fédéral des réglementations, y compris, en ce qui concerne les demandes de continuation-in-part les renseignements pertinents qui sont devenus accessibles entre la date de dépôt de la demande antérieure et la date du dépôt international de la demande de continuation-in-part. Je déclare par la présente que toute déclaration ci-incluse est, à ma connaissance, véridique et que toute déclaration formulée à partir de renseignements ou de suppositions est tenue pour véridique; et de plus, que toutes ces déclarations ont été formulées en sachant que toute fausse déclaration volontaire ou son équivalent est passible d'une amende ou d'une incarcération, ou des deux, en vertu de la Section 1001 du Titre 18 du Code des États-Unis, et que de telles déclarations volontairement fausses risquent de compromettre la validité de la demande de brevet ou du brevet délivré à partir de celle-ci.
VIII-4-1-1-1	Nom (NOM DE FAMILLE, prénom) :	BOUCADAIR, Mohamed
VIII-4-1-1-2	Domicile : (ville et État (des États-Unis d'Amérique), le cas échéant, ou pays)	RENNES, France
VIII-4-1-1-3	Adresse postale :	1 square Louis Harel de la Nöe 35000 RENNES France
VIII-4-1-1-4	Nationalité :	FR
VIII-4-1-1-5	Signature de l'inventeur : (La signature doit être celle de l'inventeur, il ne peut s'agir de celle du mandataire)	
VIII-4-1-1-6	Date :	02-07-09

VIII-4-1-2-1	Nom (NOM DE FAMILLE, prénom) :	GRIMAULT, Jean-Luc
VIII-4-1-2-2	Domicile : (ville et État (des États-Unis d'Amérique), le cas échéant, ou pays)	MONDEVILLE, France
VIII-4-1-2-3	Adresse postale :	7 impasse de l'Europe 14120 MONDEVILLE France
VIII-4-1-2-4	Nationalité :	FR
VIII-4-1-2-5	Signature de l'inventeur : (La signature doit être celle de l'inventeur, il ne peut s'agir de celle du mandataire)	
VIII-4-1-2-6	Date	30/6/2009

PATENT
Attorney Docket No. P3714US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Boucadair et al.

Group Art Unit: Unassigned

Application No. Unassigned
(U.S. National Phase of PCT/FR2009/051228)

Examiner: Unassigned

Filed: December 29, 2010

For: A METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY (as currently amended)

PRELIMINARY AMENDMENT

Mail Stop PCT
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

Prior to the examination of the above-identified patent application, please amend the application as follows:

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Abstract begin on page 3 of this paper.

Amendments to the Claims are reflected in the listing of claims which begins on page 4 of this paper.

Remarks begin on page 7 of this paper.

Amendments to the Specification

At page 1, please replace the title of the application as published with the following title:

A METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

At page 1, please insert the following new paragraph below the title:

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is the U.S. national phase of the International Patent Application No. PCT/FR2009/051228 filed June 26, 2009, which claims the benefit of French Application No. 08 54405 filed June 30, 2008, the entire content of which is incorporated herein by reference.

At page 1, between lines 10 and 11, insert the heading:

BACKGROUND

At page 3, line 9, delete the heading:

~~DRAWBACKS OF THE PRIOR ART~~

At page 4, line 12 amend the heading as follows:

SUMMARY ~~OF THE INVENTION~~

At page 12, lines 29 and 30, amend the heading as follows:

DETAILED DESCRIPTION ~~OF ONE PARTICULAR IMPLEMENTATION OF THE INVENTION~~

Juniper Exhibit 1002, page 77

Amendments to the Abstract

Please replace the Abstract as published on the front page of the PCT publication with the following new Abstract:

A method of receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet comprising an IPv6 destination address and an IPv6 source address. The method comprises the following steps: identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address, and a destination port number; if necessary, regularizing at least one address of the data packet and modifying the data packet; and routing the modified data packet to its destination.

A replacement Abstract is attached hereto on a separate sheet in accordance with 37 CFR 1.72.

Juniper Exhibit 1002, page 78

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application.

Claim 1 (currently amended): A ~~receiving~~ method for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet ~~including~~ comprising an IPv6 destination address and an IPv6 source address, ~~characterized in that,~~ said method being executed in a home gateway adapted to connect a user terminal to said IPv6 domain, ~~it includes~~ and comprising the following steps:

[[·]] identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address and a destination port number;

[[·]] if necessary, regularizing at least one address of the data packet by replacing said address, the replacement process belonging to a group comprising replacement of a constructed address with a native address and replacement of a native address with a constructed address, and modifying the data packet using the regularized address; and

[[·]] routing the modified data packet to its destination.

Claim 2 (currently amended): ~~A receiving~~ The method according to claim 1, ~~characterized in that,~~ wherein when the data packet comes from said user terminal and goes to the IPv4 domain, the step of regularizing the source address further ~~includes~~ comprises the following steps:

[[·]] identifying an IPv6 native source address;

[[·]] creating an entry in an address translation table, said entry associating said native source address with a source address constructed by concatenating an operator prefix, an IPv4 address assigned to the gateway, and a source port number belonging to a range of port numbers authorized for said gateway; and

[[·]] replacing the native source address of the data packet with the constructed source address.

Claim 3 (currently amended): ~~A receiving~~ The method according to claim 2, ~~characterized in that~~ wherein address identification uses an identifier contained in the destination address.

Juniper Exhibit 1002, page 79

Claim 4 (currently amended): ~~A receiving~~ The method according to claim 2, ~~characterized in that~~ ~~it~~ further ~~includes~~ comprising a step of verifying that the source port number of the data packet and the source port number of the constructed source address match.

Claim 5 (currently amended): ~~A receiving~~ The method according to claim 1, ~~characterized in that,~~ wherein when the data packet comes from the IPv4 domain and goes to said user terminal, the step of regularizing the source address ~~includes~~ comprises the following steps:

[[·]] searching an address translation table of the gateway for an entry associating with said constructed destination address a native destination address;

[[·]] if an entry is found, replacing the constructed destination address of the data packet with the native destination address from that entry.

Claim 6 (currently amended): ~~A receiving~~ The method according to claim 5, ~~characterized in that it~~ further ~~includes~~ comprising a step of verifying that the destination port number of the data packet and the destination port number contained in the constructed destination address match.

Claim 7 (currently amended): A device for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet ~~including~~ comprising an IPv6 destination address and an IPv6 source address, ~~characterized in that,~~ said device ~~being intended to be used~~ for use in a home gateway adapted to connect a user terminal to said IPv6 domain, ~~it includes~~ comprising:

[[·]] means for identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address, and a destination port number;

[[·]] means for regularizing, if necessary, at least one address of the data packet by replacing said address, the replacement process belonging to a group comprising replacement of a constructed address with a native address and replacement of a native address with a constructed address, and modifying the data packet using the regularized address; and

[[·]] means for routing the modified data packet to its destination.

Claim 8 (currently amended): A home gateway adapted to connect user terminals of a home network to an IPv6 domain connected to an IPv4 domain, ~~characterized in that it includes~~ comprising:

[[·]] means for obtaining an IPv4 address, a range of port numbers authorized for said gateway, and a range of IPv6 addresses authorized for said gateway, said range of IPv6

Juniper Exhibit 1002, page 80

addresses being constructed by concatenating an operator prefix, said IPv4 address, and the range of authorized IPv4 port numbers; and

[[·]] a device according to claim 7 for receiving an IPv6 data packet in the IPv6 domain connected to the IPv4 domain.

Claim 9 (currently amended): A home gateway according to claim 8, ~~including~~ comprising an address translation table containing entries associating at least one source address for a communications session involving a user terminal of its home network, ~~characterized in that~~ wherein said gateway is adapted to store in said entry an IPv6 constructed source address and an IPv6 native source address.

Claim10 (currently amended): A non-transitory computer program product that is at least one of downloadable from a communications network ~~and/or~~ and stored on a computer-readable medium ~~and/or~~ and executable by a microprocessor, ~~characterized in that it includes~~ comprising program code instructions for executing the method according to claim 1 of receiving a data packet in an IPv6 domain.

Juniper Exhibit 1002, page 81

Remarks

The present application is a U.S. National Phase of a PCT patent application. The present Amendment revises the specification and claims to conform to United States patent practice, before examination of the present PCT application in the United States National Examination Phase.

All of the changes are editorial and applicants believe no new matter is added thereby. The amendment, addition, and/or cancellation of claims is not intended to be a surrender of any of the subject matter of those claims.

Early examination on the merits is respectfully requested. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
Mark Bergner, Reg. No. 45,877
DRINKER BIDDLE & REATH LLP
191 North Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: December 29, 2010

CH01/ 25646398.2

Juniper Exhibit 1002, page 82

ABSTRACT

A method of receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet comprising an IPv6 destination address and an IPv6 source address. The method comprises the following steps: identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address, and a destination port number; if necessary, regularizing at least one address of the data packet and modifying the data packet; and routing the modified data packet to its destination.

Juniper Exhibit 1002, page 83

Electronic Patent Application Fee Transmittal	
Application Number:	
Filing Date:	
Title of Invention:	A METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY
First Named Inventor/Applicant Name:	Mohamed Boucadair
Filer:	Brian Charles Rupp/Irina Mikitiouk
Attorney Docket Number:	P3714US
Filed as Large Entity	

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
National Stage Fee	1631	1	330	330
Natl Stage Search Fee - Report provided	1642	1	430	430
National Stage Exam - all other cases	1633	1	220	220
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**980**

Electronic Acknowledgement Receipt	
EFS ID:	9133293
Application Number:	13001907
International Application Number:	PCT/FR09/51228
Confirmation Number:	5439
Title of Invention:	A METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY
First Named Inventor/Applicant Name:	Mohamed Boucadair
Customer Number:	08968
Filer:	Brian Charles Rupp/Irina Mikitiouk
Filer Authorized By:	Brian Charles Rupp
Attorney Docket Number:	P3714US
Receipt Date:	29-DEC-2010
Filing Date:	
Time Stamp:	15:15:16
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$980
RAM confirmation Number	1500
Deposit Account	070181
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal of New Application	P3714US_National_Phase_Transmittal.pdf	82317 85d5efaec73aaa746d8a07349c447735d968885e	no	2
Warnings:					
Information:					
2	Application Data Sheet	P3714US_Application_Data_Sheet.pdf	30757 698576092e441dde0ff4d4a4f71771f7ef5a1b5a	no	3
Warnings:					
Information:					
This is not an USPTO supplied ADS fillable form					
3		P3714US_English_Translation_of_PCT_Application.pdf	118806 ba7a46ba197c54215a0d8e2b840f0cebe844faaa	yes	38

Multipart Description/PDF files in .zip description

Document Description	Start	End
Specification	1	34
Claims	35	37
Abstract	38	38

Warnings:					
Information:					
4	Drawings-only black and white line drawings	P3714US_Drawings.pdf	232390 85eae89e75f65df5759b50d2dad9b8bb7b43cf4a	no	9
Warnings:					
Information:					
5	Documents submitted with 371 Applications	P3714US_Certification_of_Translation.pdf	28547 fc3d14599f0a151bd917cb674248b83878e52b33	no	1
Warnings:					
Information:					
6	Documents submitted with 371 Applications	P3714US_Copy_of_Search_Report.pdf	543354 47d3eab33bc7f3fa0507b87e33700bf0c3671707	no	8

Warnings:					
Information:					
7	Documents submitted with 371 Applications	P3714US_Copy_of_Written_Opinion.pdf	345943 ca203c32285779bec8cb6f397d194b37b0929d55	no	9
Warnings:					
Information:					
8	Oath or Declaration filed	P3714US_Copy_of_PCT_Declaration.pdf	95150 7f817015a682ff8db8d445e4957dccb62f945f9b	no	3
Warnings:					
Information:					
9		P3714US_Preliminary_Amendment.pdf	80504 21e77684727392165b1d9ced75aac8a1f4dbb009	yes	7

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Preliminary Amendment	1	1
	Specification	2	2
	Abstract	3	3
	Claims	4	6
	Applicant Arguments/Remarks Made in an Amendment	7	7

Warnings:					
Information:					
10	Abstract	P3714US_Replacement_Abstract.pdf	29362 143a5fee386585697b85b8e8257686f3988de31e	no	1
Warnings:					
Information:					
11	Fee Worksheet (PTO-875)	fee-info.pdf	33415 99ec8b4a0900ad4cf0a3ee7e8454323a01f272e1	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1620545		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATIONEN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
14 janvier 2010 (14.01.2010)

PCT

(10) Numéro de publication internationale
WO 2010/004180 A1

(51) Classification internationale des brevets : *H04L 29/12* (2006.01)

(21) Numéro de la demande internationale : PCT/FR2009/051228

(22) Date de dépôt international : 26 juin 2009 (26.06.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0854405 30 juin 2008 (30.06.2008) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BOUCADAIR, Mohamed** [FR/FR]; 1, square Louis Harel de la Nöe, F-35000 Rennes (FR). **GRIMAULT, Jean-Luc** [FR/FR]; 7, impasse de l'Europe, F-14120 Mondeville (FR).

(74) Mandataire : **FRANCE TELECOM R&D/PIV/BREVETS**; BENETIERE Marion, 38-40, rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Suite sur la page suivante]

WO 2010/004180 A1

(54) Title : METHOD FOR RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AND ASSOCIATED DEVICE AND RESIDENTIAL GATEWAY

(54) Titre : PROCEDE DE RECEPTION D'UN PAQUET DE DONNEES DANS UN DOMAINE IPV6, DISPOSITIF ET PASSERELLE RESIDENTIELLE ASSOCIES

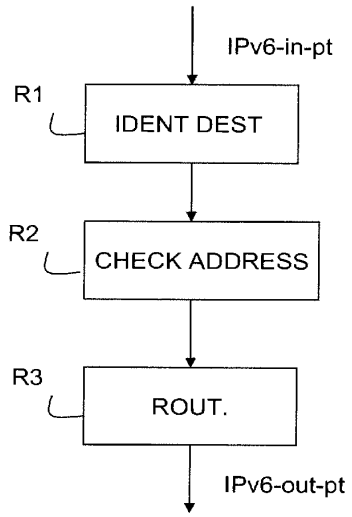


FIG. 3

(57) Abstract : The invention relates to a method for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet comprising an IPv6 destination address and an IPv6 source address. According to the invention, such a method comprises the following steps: an IPv6 destination address constructed by concatenation of an operator prefix, an IPv4 destination address and a destination port number is identified; if necessary, at least one address of the data packet is brought into compliance and the data packet is modified; and the modified data packet is routed towards its destination.

(57) Abrégé : L'invention concerne un procédé de réception d'un paquet de données IPv6 dans un domaine IPv6 interconnecté avec un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source. Selon l'invention, un tel procédé comprend les étapes suivantes : identification d'une adresse IPv6 de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination; si nécessaire, mise en conformité d'au moins une adresse du paquet de données et modification du paquet de données; et routage du paquet de données modifié vers sa destination.

ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (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, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *avec rapport de recherche internationale (Art. 21(3))*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues (règle 48.2.h))*

Procédé de réception d'un paquet de données dans un domaine IPv6, dispositif et passerelle résidentielle associés

Domaine de l'invention

Le domaine de l'invention est celui d'un réseau de télécommunications, en particulier un réseau de télécommunications IP dans lequel sont transportés des paquets de données d'un équipement source identifié par une adresse source vers un équipement de destination identifié par une adresse de destination.

Un tel réseau de télécommunications regroupe une pluralité d'équipements, de liens et de fonctions dédiés au transport des données issues d'équipements terminaux connectés à ce réseau. En particulier, les fonctions de transport peuvent être implémentées grâce à l'activation de protocoles de routage et de transmission. Un réseau de télécommunications administré par un opérateur est encore appelé un domaine.

Un fournisseur de service de connectivité IP déploie une architecture dédiée pour permettre aux utilisateurs d'équipements terminaux d'être joignables. L'accès au service de connectivité IP est géré par le fournisseur de service qui s'appuie sur le réseau de télécommunications d'un opérateur pour router les paquets de données émis par les équipements terminaux vers leurs destinations finales. Dans certains cas, ledit fournisseur de service est aussi l'opérateur de réseau de télécommunications.

Un tel fournisseur de service affecte une adresse IP, généralement cette adresse est publique à une passerelle résidentielle entre un réseau résidentiel et le réseau public ou domaine IP de l'opérateur. La passerelle résidentielle affecte généralement aux terminaux de son réseau résidentiel des adresses IP privées.

Dans la suite, on désignera par « passerelle résidentielle » tout équipement d'interconnexion entre un réseau privé et un réseau opéré par un fournisseur de service, le réseau privé pouvant aussi bien être un réseau résidentiel qu'un réseau d'entreprise.

Dans la suite, le réseau opéré par les fournisseurs de service sera aussi désigné par le terme "réseau public".

Placée en coupure des paquets de données entre un terminal de son réseau résidentiel privé et le domaine IP de l'opérateur, la passerelle résidentielle comporte, de façon connue, une table dans laquelle elle associe l'adresse IP privée et le port associé à ce terminal, avec une adresse IP publique de type IPv4 et un port de cette même passerelle sur le réseau public.

Cette table est connue de l'homme du métier sous l'appellation "table de nattage", cette expression venant de l'acronyme NAT (*Network Address Translator* en anglais). Plusieurs types de NAT peuvent être implémentés tels que le « Full Cone », « Port Restricted » ou encore « symétrique ».

Il est communément admis par la communauté des fournisseurs de service IP que l'épuisement des adresses IPv4 publiques est une fatalité. Pour éviter ce problème, la communauté s'est mobilisée dans le passé, ce qui a conduit à la définition d'un nouveau protocole : IPv6 (*Internet Protocol version 6*). Cette nouvelle version du protocole IP offre un grand nombre d'adresses IP et un mécanisme de routage hiérarchique aux performances améliorées. Ces mêmes fournisseurs ne sont toutefois pas indifférents aux alarmes récemment émises par l'IETF (*Internet Engineering Task Force*), notamment dans des rapports présentés au sein du groupe de travail GROW (*Global Routing Operations Working Group)* concernant un risque d'épuisement des adresses IPv4 de l'IANA (Internet Assigned Numbers Authority) fin 2010.

Néanmoins, cette solution, i.e. IPv6, n'est en pratique pas encore beaucoup activée par les opérateurs, pour des raisons financières, stratégiques et techniques liées à la gestion de la complexité des opération de transition et de migration.

Pour limiter le nombre d'adresses publiques IPv4 nécessaires pour la fourniture d'un service de connectivité IP à un parc de clients, une solution de double NAT, appelée aussi « NAT Opérateur », a été proposée et implémentée. Elle consiste à activer une fonction NAT au sein du réseau de télécommunications de l'opérateur, de telle sorte que les passerelles résidentielles utilisent une adresse privée dans leurs tables de Nattage vers l'extérieur (au lieu d'une adresse public). Ainsi, c'est la fonction « NAT Opérateur » qui assure la traduction des adresses privées des passerelles résidentielles vers des adresses publiques, ce qui permet à un fournisseur de service

d'économiser un nombre non négligeable d'adresses publiques IPv4 requises pour la fourniture du service de connectivité IP.

Inconvénients de la technique antérieure

La solution « NAT Opérateur » présente des inconvénients, parmi lesquels :

- une complexification du traitement des paquets de données IP : du fait de l'introduction d'un deuxième niveau de traduction d'adresses, les paquets de données doivent être modifiés deux fois ;
- la nécessité d'adapter la mise en œuvre des protocoles de signalisation applicative ou ALG (*Application Level Gateway*) conventionnels tels que DNS (*Domain Name System*), FTP (*File Transfer Protocol*) ou encore SIP (*Session Initiation Protocol*). Dans le cas de SIP par exemple, l'établissement et le maintien d'une session de voix sur IP, nécessite que, pour maintenir à jour la table de Nattage d'une passerelle résidentielle, des échanges de signalisation fréquents entre le terminal de l'abonné et le réseau public via des requêtes de réenregistrements doivent être implémentés de façon à maintenir les sessions de NAT actives. En présence d'un double NAT, un tel mécanisme doit aussi être prévu au niveau de l'équipement qui héberge la fonction « NAT Opérateur ». L'adresse et le port publics effectivement en cours d'utilisation pour le terminal doivent en outre être communiqués à l'application SIP ;
- une dégradation du service de connectivité IP offert par l'opérateur du réseau public de télécommunications doit être déplorée, notamment parce que des fonctionnalités telles que le "*port forwarding*" ou le *DynDNS* ne peuvent pas être supportées en présence du « NAT Opérateur ».

Par ailleurs, une telle solution ne pourra pas empêcher, mais seulement retarder le phénomène d'épuisement des adresses IPv4. Il faudra donc prévoir à moyen terme un passage à IPv6. Un tel passage va nécessairement engendrer une période de transition pendant laquelle des domaines IPv6 devront s'interconnecter avec des domaines IPv4. Or, rien n'est prévu dans les réseaux actuels pour faciliter une telle interconnexion d'une manière efficace, optimale et

sans instanciation d'états supplémentaires dans les nœuds réseaux mis en œuvre dans la fourniture du service de connectivité IP.

Il n'est pas prévu non plus de migration progressive d'un adressage IPv4 vers un adressage IPv6 à partir de mécanismes d'interconnexion simples entre un domaine IPv6 et un domaine IPv4, notamment qui ne nécessitent pas que les terminaux clients implémentent à la fois le protocole IPv4 et le protocole IPv6.

Exposé de l'invention

L'invention vient améliorer la situation à l'aide d'un procédé de réception d'un paquet de données IPv6 dans un domaine IPv6 interconnecté avec un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source.

Selon l'invention, ledit procédé est mis en œuvre dans une passerelle résidentielle apte à connecter un terminal d'utilisateur audit domaine IPv6 et il comprend les étapes suivantes :

- identification d'une adresse IPv6 de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données par remplacement de ladite adresse, ledit remplacement appartenant à un groupe comprenant un remplacement d'une adresse construite en une adresse native et un remplacement d'une adresse native en une adresse construite, et modification du paquet de données à l'aide de l'adresse mise en conformité; et
- routage du paquet de données modifié vers sa destination.

Dans un contexte de migration du protocole IPv4 vers le protocole IPv6, on considère un premier équipement terminal d'un domaine IPv4 qui ne peut émettre et recevoir un paquet de données que selon le protocole IPv4. Parallèlement, un deuxième équipement terminal du domaine IPv6 ne peut qu'émettre et recevoir un paquet de données IPv6. Selon l'invention, lorsqu'un de ces équipements souhaite envoyer un paquet de données à l'autre, il utilise son protocole, mais les données

acheminées dans le domaine IPv6 le sont selon le protocole IPv6.

Le paquet de données est donc émis soit en IPv4 ou IPv6, transformé si nécessaire en un paquet de données selon le protocole IPv6 pour son acheminement dans le domaine IPv6, puis re-transformé, si nécessaire en un paquet de données IPv4.

Une telle transformation s'appuie sur un mécanisme de construction d'adresse de destination IPv6 à partir d'une adresse de destination IPv4 du premier terminal par concaténation d'un préfixe opérateur, de cette adresse de destination IPv4 et du numéro de port de destination du paquet. En effet, on considère le cas où un équipement d'interconnexion du domaine IPv6 avec le domaine IPv4 construit une adresse de destination IPv6 à partir de l'adresse de destination IPv4 et du port de destination. Cette adresse de destination IPv6 construite est routable dans le domaine IPv6 et comprend les informations utiles véhiculées par le paquet de données IPv4.

Cette transformation nécessite que le deuxième terminal d'utilisateur, bien qu'il implémente le protocole IPv6, dispose d'une adresse « fictive » IPv4, qui peut être la sienne ou celle d'une passerelle résidentielle qui administre un réseau résidentiel auquel il est connecté. Cette adresse, utilisée comme adresse destination d'un paquet IPv4 en provenance du domaine IPv4, est exploitée par l'équipement d'interconnexion pour construire l'adresse de destination IPv6 précédemment évoquée.

Inversement, il est possible de retrouver l'adresse IPv4 et le numéro de port à l'origine d'une adresse IPv6 construite selon un tel mécanisme (c'est-à-dire respectant le formalisme de construction d'adresse IPv6 qui vient d'être mentionné). Il n'est donc pas nécessaire de stocker une table de traduction d'adresses IPv4 vers IPv6 ni de maintenir des états relatifs à des sessions au niveau du nœud d'accès (encore appelé nœud d'interconnexion) des deux domaines IPv4 et IPv6. L'invention permet donc, dans le sens IPv4 vers IPv6 (ainsi que d'IPv6 vers IPv4), de router le paquet de données IPv4 sous la forme d'un paquet de données IPv6 vers sa destination et de livrer les informations utiles contenues dans le paquet à son destinataire, sans avoir recours à des tables d'états lourdes à maintenir.

Ainsi, ni le terminal d'utilisateur IPv6 destinataire ou émetteur du paquet de données, ni éventuellement la passerelle résidentielle qui le gère, ni encore les

Juniper Exhibit 1002, page 96

routeurs en charge d'acheminer le paquet à sa destination n'ont besoin d'interpréter le protocole IPv4.

Toutefois, pour que l'acheminement du paquet de données IPv6 issu d'une telle transformation puisse se faire comme celui d'un paquet IPv6 natif, il est nécessaire de vérifier une conformité de ses adresses sources et destination par rapport au formalisme précédemment évoqué. Le procédé selon l'invention propose donc une solution pour identifier que la destination ou la provenance de ce paquet appartient à un domaine IPv4 et pour lui appliquer en conséquence un traitement de vérification approprié.

Selon un aspect de l'invention, lorsque le paquet est en provenance dudit terminal d'utilisateur et à destination du domaine IPv4, l'étape de mise en conformité de l'adresse source comprend en outre les étapes suivantes :

- identification d'une adresse IPv6 source native;
- création d'une entrée dans une table de traduction d'adresses, ladite entrée associant ladite adresse source native à une adresse source construite par concaténation d'un préfixe opérateur, d'une adresse IPv4 affectée à la passerelle et d'un numéro de port source appartenant à une plage de numéros de ports autorisés pour ladite passerelle; et
- remplacement de l'adresse source native du paquet de données par l'adresse source construite.

Il s'agit dans ce cas d'une communication sortante. Lorsqu'une adresse de destination construite a pu être identifiée, on peut en déduire que le paquet de données est destiné à un terminal d'utilisateur du domaine IPv4. Dans ce cas, son adresse source doit être une adresse construite afin qu'un équipement d'interconnexion du domaine IPv6 avec le domaine IPv4 puisse ensuite récupérer l'adresse IPv4 source et transformer à l'inverse le paquet de données IPv6 en un paquet de données IPv4. Si aucun traitement n'est effectué, le paquet ne pourra pas être traité par le nœud d'interconnexion; car l'adresse source native ne contient pas d'information relative à l'adresse IPv4 source, c'est-à-dire l'adresse IPv4 fictive du terminal ayant émis ledit paquet.

Si l'adresse source est native, le procédé selon l'invention permet de la remplacer par une adresse source construite appartenant à un préfixe ou plage d'adresses source IPv6 autorisées pour la passerelle.

En prévision de la réception d'une réponse à ce paquet de données, une association entre l'adresse source native d'origine et l'adresse source construite est ajoutée dans une table de traduction d'adresses de la passerelle résidentielle.

Ainsi, un paquet de données émis en réponse pourra être acheminé jusqu'au terminal d'utilisateur du réseau résidentiel qui avait émis le premier paquet de données.

Un avantage de l'invention est qu'elle permet à un terminal d'utilisateur IPv6 d'utiliser l'adresse source qu'il souhaite pour émettre des paquets de données à destination d'un domaine IPv4, puisque la passerelle selon l'invention fait le nécessaire pour qu'ils soient acheminés jusqu'à leur destination.

Selon un aspect de l'invention, l'identification d'adresse est réalisée à l'aide d'un identifiant compris dans l'adresse de destination.

Cet identifiant peut être valorisé différemment selon qu'il s'agit d'une adresse IPv6 native ou d'une adresse IPv6 construite à partir d'une adresse IPv4. Un avantage est de permettre une identification simple et rapide de la nature de l'adresse du paquet de données. Une telle solution permet aussi une mutualisation des équipements d'interconnexion IPv4 IPv6 entre plusieurs opérateurs.

Selon un autre aspect de l'invention, le procédé de réception comprend en outre une étape de vérification d'une concordance entre le numéro de port source du paquet de données et le numéro de port de source de l'adresse source construite.

En effet, le paquet de données comprend un numéro de port source au niveau de la couche transport selon le modèle OSI. Pour qu'une réponse puisse être acheminée par le réseau jusqu'au terminal émetteur du premier paquet, il est important que ce numéro de port source de niveau transport concorde avec le numéro de port source contenu dans l'adresse source construite du paquet de données. Si ce n'est pas le cas, le procédé selon l'invention permet de faire concorder les deux numéros de ports source.

On notera que l'étape de vérification et l'étape de mise en conformité de

l'adresse source peuvent être mises en œuvre simultanément. Par exemple, le choix d'une adresse source construite dans le préfixe de la passerelle peut intégrer la contrainte d'avoir un numéro de port source égal au numéro de port source de niveau transport.

Selon un aspect de l'invention, lorsque le paquet de données est en provenance du domaine IPv4 et à destination du terminal d'utilisateur connecté au domaine IPv6 par ladite passerelle résidentielle, l'étape de mise en conformité de l'adresse source comprend les étapes suivantes :

- recherche dans une table de traduction d'adresses de ladite passerelle d'une entrée associant à ladite adresse de destination une adresse de destination native.
- si une entrée a été trouvée, remplacement de l'adresse de destination construite du paquet de données par l'adresse de destination native de l'entrée.

On notera que le numéro de port destination est aussi remplacé par celui renseigné dans la table de traduction d'adresses et de ports telle que maintenue par la passerelle résidentielle.

Il s'agit ici d'une communication entrante. Le paquet de données IPv6 a été construit à partir d'un paquet IPv4 par un équipement d'interconnexion du domaine IPv6 au domaine IPv4. Il se peut qu'il constitue une réponse à un paquet de données précédemment émis par le terminal d'utilisateur connecté à la passerelle résidentielle. Celle-ci consulte donc sa table de traduction. Si elle y trouve une association entre l'adresse de destination extraite du paquet de données reçu et une adresse de destination IPv6 native, elle remplace l'adresse de destination et potentiellement le numéro de port destination construite du paquet de données par l'adresse IPv6 native de l'entrée et route le paquet modifié vers le terminal destinataire.

Selon un autre aspect de l'invention, le procédé de réception comprend en outre une étape de vérification d'une concordance entre le numéro de port de destination du paquet de données et le numéro de port de destination contenu dans l'adresse de destination construite.

Une telle vérification permet de s'assurer que le numéro de port de destination

du paquet de données au niveau transport coïncide bien avec le numéro de l'adresse de destination construite du paquet. Cette vérification présente un intérêt particulier si l'adresse IPv4 fictive affectée à la passerelle domestique est partagée avec plusieurs autres terminaux ou passerelles domestiques. En effet, dans ce cas, la discrimination entre ces équipements est faite sur la base de la plage de numéros de ports utilisée. Avec l'invention, le routage d'un paquet émis par terminal IPv4 vers ladite adresse fictive peut avoir lieu vers la passerelle concernée sans rencontrer de problème de routage.

Le procédé de réception peut être mis en œuvre dans un dispositif de réception d'un paquet de données dans un domaine IPv6 interconnecté à un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, caractérisé en ce qu'il comprend les étapes suivantes :

- identification d'une adresse de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données; et
- routage du paquet de données modifié vers sa destination.

Dans un mode particulier de réalisation, les différentes étapes des procédés de réception d'un paquet de données sont déterminées par des instructions de programmes d'ordinateurs.

En conséquence, l'invention vise aussi un programme d'ordinateur sur un support d'informations, ce programme étant susceptible d'être mis en œuvre dans un dispositif de réception ou plus généralement dans un ordinateur, ce programme comportant des instructions adaptées à la mise en œuvre des étapes d'un procédé d'acheminement, de réception ou de transmission tel que décrit ci-dessus.

Ce programme peut utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source

et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

L'invention vise aussi un support d'informations lisible par un ordinateur, et comportant des instructions d'un programme d'ordinateur tel que mentionné ci-dessus.

Le support d'informations peut être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, le support peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

L'invention concerne aussi une passerelle résidentielle apte à connecter des terminaux d'utilisateurs à un domaine IPv6 interconnecté à un domaine IPv4. Selon l'invention, une telle passerelle comprend :

- des moyens d'obtention d'une adresse IPv4, d'une plage de numéros de ports autorisés pour ladite passerelle et d'une plage d'adresses IPv6 autorisées pour ladite passerelle, ladite plage d'adresses IPv6 étant construite par concaténation d'un préfixe opérateur, de ladite adresse IPv4 et de la plage de numéros de ports IPv4 autorisés; et
- un dispositif de réception d'un paquet de données IPv6 dans le domaine IPv6 interconnecté au domaine IPv4 selon l'invention.

Selon l'invention, une telle passerelle ne traite que des paquets de données IPv6. Toutefois, une adresse IPv4 lui est affectée, de façon à ce qu'elle puisse être identifiée et être jointe par des émetteurs du domaine IPv4. La dite adresse n'est pas utilisée par la passerelle domestique pour l'envoi des paquets IP.

Juniper Exhibit 1002, page 101

La passerelle résidentielle peut comprendre une table de traduction d'adresses, comprenant des entrées, associant, pour une session de communication impliquant terminal d'utilisateur de son réseau résidentiel, au moins une adresse source. Selon l'invention, ladite passerelle est apte à enregistrer dans ladite entrée, une adresse source IPv6 construite et une adresse source IPv6 native du terminal d'utilisateur

Liste des figures

D'autres avantages et caractéristiques de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation particulier de l'invention, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 présente de façon schématique un domaine IPv6 interconnecté à un domaine IPv4 selon l'invention;
- la figure 2 illustre la structure d'un préfixe d'adresses IPv6 construit selon l'invention;
- la figure 3 présente de façon schématique les étapes du procédé de réception d'un paquet de données dans un domaine IPv6 interconnecté avec un domaine IPv4 selon l'invention;
- la figure 4 illustre la structure d'une adresse IPv6 construite à partir d'une adresse de destination IPv4 et d'un port de destination selon un premier mode de réalisation de l'invention;
- la figure 5 illustre la structure d'une adresse de destination IPv6 construite à partir d'une adresse IPv4 et d'un port de destination selon l'invention pour la mise en œuvre du procédé de réception selon le premier mode de réalisation de l'invention;
- la figure 6 illustre la structure d'une adresse source IPv6 construite à partir d'une adresse source IPv4 et d'un port source pour la mise en œuvre du procédé de réception selon le premier mode de réalisation invention;
- la figure 7 illustre la structure d'une adresse IPv6 construite à partir d'une adresse IPv4 et d'un port de destination selon un deuxième mode de réalisation

Juniper Exhibit 1002, page 102

de l'invention;

- la figure 8 présente de façon schématique les étapes du procédé de réception d'un paquet de données dans un domaine IPv6 interconnecté avec un domaine IPv4 selon le deuxième mode de réalisation de l'invention;et
- la figure 9 présente de façon schématique la structure d'un dispositif de réception d'un paquet de données dans un domaine IPv6 selon l'invention;

7. Description d'un mode de réalisation particulier de l'invention

Le principe général de l'invention repose sur la construction d'une adresse IPv6 à partir d'une adresse IPv4, d'un préfixe opérateur prédéterminé et d'un numéro de port. Une telle construction permet la transformation d'un paquet IPv4 entrant dans un domaine IPv6 et inversement celle d'un paquet IPv6 sortant d'un domaine IPv6 à destination d'un domaine IPv4, sans qu'il soit nécessaire de maintenir une table de correspondance entre les adresses IPv4 et IPv6 dans un nœud d'accès au domaine IPv6.

Pour rappel, les adresses IPv6 sont longues de 16 octets, soit 128 bits, contre 4 octets (32 bits) pour les adresses IPv4. On dispose ainsi d'un nombre potentiel d'adresses extrêmement grand par rapport au nombre d'adresses IPv4. Une adresse IPv6 comporte deux parties:

- la partie de gauche (le préfixe) identifie un sous-réseau du domaine ;
- la partie de droite identifie une machine connectée au sous-réseau.

Généralement, les préfixes les plus longs alloués à un sous-réseau sont des préfixes "/64"; c'est-à-dire qu'ils comportent 64 bits pour les identifier. Les 64 bits de droite de l'adresse sont alors utilisés pour identifier une machine particulière appartenant au sous-réseau. Des préfixes de longueurs plus courtes (exemple "/56" ou même "/48") permettent quant à eux d'identifier des sous-réseaux de plus grande ampleur, comportant souvent eux-mêmes des sous-réseaux "/64". Néanmoins, dans le standard IPv6, rien n'interdit d'utiliser des préfixes plus longs que "/64" et on peut donc imaginer, par exemple, un préfixe "/116" qui identifie un sous-réseau pouvant comporter 4096 machines.

Juniper Exhibit 1002, page 103

On notera que la seule restriction à des préfixes plus longs que "/64" consiste simplement dans le fait que les machines derrière le sous-réseau correspondant ne pourront pas mettre en œuvre le mécanisme d'auto-configuration décrit dans le document RFC2462. Ce mécanisme permet à une machine connaissant son adresse de niveau 2 (par exemple son adresse Ethernet MAC) de configurer elle-même, sous certaines conditions, les 64 bits de droite de son adresse IPv6, en dérivant son adresse de niveau 2 suivant un algorithme précis. Mais ce mécanisme d'auto-configuration n'est pas obligatoire et on peut préférer d'autres mécanismes comme par exemple celui correspondant au protocole DHCPv6 [RFC3315] qui permet, entre autres, d'obtenir une adresse IPv6 auprès d'un serveur DHCPv6.

Si on s'intéresse maintenant, non plus à une simple machine IPv6, mais à un routeur IPv6 (comme par exemple une passerelle résidentielle IPv6), on sait qu'un tel équipement doit disposer d'un (ou plusieurs) préfixes IPv6 qui représente(nt) le(s) sous-réseau(x) dont il route les paquets. Un routeur IPv6 doit donc être configuré avec un (ou plusieurs) préfixes.

Une extension de DHCPv6 permet à un routeur requérant un ou des préfixes IPv6 (comme par exemple une passerelle résidentielle) de les demander auprès d'un équipement pouvant en déléguer (typiquement un routeur en amont). Cette extension est décrite dans le RFC 3633 (*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*) et spécifie une option "Identity Association for Prefix Delegation Option" dans les messages DHCPv6 pour passer le ou les préfixes délégués. Une fois que le routeur requérant s'est vu déléguer un ou des préfixes IPv6, il route tous les paquets IPv6 destinés ou issus de machines dont les adresses s'inscrivent dans le(s) préfixe(s) qu'il gère.

On présente maintenant, en relation avec la **figure 1**, un domaine IPv6 1 comprenant un équipement d'interconnexion du domaine IPv6 1 avec un domaine IPv4 2 ou nœud d'accès IPv6/IPv4 40 à un domaine IPv4 2 et un routeur d'accès 30, apte à router des paquets de données vers ou en provenance d'une passerelle résidentielle 20 connectée au domaine IPv6 1. Une telle passerelle administre un réseau résidentiel 2 auxquels sont connectés les terminaux 21 et 22.

Dans le contexte de l'invention, on considère une passerelle résidentielle implémentant le protocole IPv6 seul. De ce fait, une telle passerelle n'est en mesure de traiter (en particulier, recevoir et émettre) que des paquets de données de type IPv6.

Les terminaux 21 et 22 sont eux aussi mono-version IPv6 (ou purement IPv6), c'est-à-dire qu'ils n'implémentent que le protocole IPv6. Nous verrons dans la suite en quoi l'invention permet une interconnexion d'un domaine IPv6 avec au moins un domaine IPv4 pour des terminaux IPv6.

On considère les cas "hybrides" suivants :

- acheminement d'un paquet de données IPv4 entrant émis par un terminal d'utilisateur du domaine IPv4 3 à destination d'un terminal d'utilisateur 21, 22 du réseau résidentiel de la passerelle 20 connectée au domaine IPv6 1; et
- acheminement d'un paquet de données IPv6 sortant émis par un terminal d'utilisateur 21, 22 du domaine IPv6 1 vers un terminal d'utilisateur du domaine IPv4 3.

Les cas d'une transmission de paquets purement IPv6 ou IPv4 étant connus de l'homme de métier, ils ne seront pas décrits plus en détails.

Pour pouvoir se connecter au domaine ou réseau IPv6, la passerelle résidentielle dispose d'éléments de connectivité IP fournis par le fournisseur de service de connectivité.

On notera toutefois que l'invention ne se limite pas à l'accès au service de connectivité IP, par exemple Internet ou Intranet, par une passerelle résidentielle, mais qu'elle s'applique aussi à des terminaux d'utilisateurs dans d'autres contextes d'accès à Internet ou d'accès à un réseau Intranet. On peut citer par exemple l'accès à ce service de connectivité IP depuis un réseau mobile, selon lequel un terminal mobile évolué pourrait servir de passerelle, en communiquant avec d'autres terminaux de son réseau LAN (via Bluetooth par exemple) ou encore le cas d'un simple terminal mobile.

Selon l'invention, la passerelle résidentielle 20 dispose des éléments de connectivité IP suivants:

Juniper Exhibit 1002, page 105

- une adresse IPv4 classique appelée dans la suite "@IPv4". Dans le cas où la passerelle héberge dans son réseau résidentiel des terminaux clients purement IPv6, cette adresse IPv4 est dite « fictive » car elle n'est pas utilisée par la passerelle pour envoyer/recevoir du trafic IP. Nous verrons dans la suite qu'elle est utilisée pour construire des adresses IPv6 selon l'invention
- une plage de numéros de ports autorisés appelée ports_pattern/length_of_unvariable;
- un préfixe d'adresses IPv6 construites appelé IPv6_prefix_ports_range; et
- un préfixe d'adresses appelé préfix IPv6 natif IPv6_prefix_native. Ce deuxième préfixe n'est toutefois pas obligatoire. Seul le préfixe IPv6 construit est suffisant.

Les éléments @IPv4, IPv6_prefix_ports_range et IPv6_prefix_native sont des éléments d'information standards dans le cadre habituel des protocoles IPv4 et IPv6.

Selon l'invention, l'élément d'information IPv6_prefix_ports_range contient intrinsèquement les éléments @IPv4 et ports_pattern/length_of_unvariable.

Dans un mode de réalisation de l'invention, l'adresse IPv4 @IPv4 est une adresse shared@IPv4 partagée par plusieurs passerelles résidentielles du domaine IPv6 1 et la plage de numéros de ports autorisés pour la passerelle résidentielle 20 est une plage de numéros de ports réservés à cette passerelle.

On comprendra que le fait de partager l'adresse publique shared@IPv4 entre plusieurs passerelles résidentielles permet d'économiser le nombre d'adresses IPv4 utilisées et de retarder le phénomène d'épuisement. En outre, son utilisation est justifiée par le besoin d'interconnecter des domaines IPv4 avec d'autres IPv6. Cette interconnexion se fait en général via des adresses de représentation. Si le parc de clients IPv6 est grand, alors les adresses de représentation IPv4 requises est conséquent.

Les différentes passerelles résidentielles qui se partagent la même adresse shared@IPv4 sont identifiées de façon unique par les numéros de ports qu'elles utilisent, puisque chacune d'entre elle bénéficie d'une plage de numéros de ports contigüe, certes restreinte, mais qui lui est réservée.

L'invention propose une interconnexion entre domaines IPv6 et IPv4 qui nécessite l'affectation d'adresses IPv4 pour fonctionner et assurer ainsi une continuité de connectivité entre terminaux hétérogènes (c'est-à-dire qui implémentent des protocoles d'adressage différents, tels que IPv4 et IPv6) d'une manière transparente.

Un avantage du mode de réalisation de l'invention, selon lequel les adresses IPv4 sont partagées, est donc de faciliter la migration vers l'adressage IPv6 tout en économisant les adresses IPv4. Dans un contexte de transition entre les deux modes d'adressage IPv4, IPv6, une telle économie peut avantageusement permettre d'éviter la pénurie tant que la migration n'est pas terminée. Un autre avantage est d'avoir un retour sur investissement immédiat pour les équipements IPv6 (car l'utilisation des capacités IPv6 ne dépend pas du comportement des clients mais de l'opérateur lui-même).

Dans la suite de la description, on considère l'exemple de réalisation selon lequel l'adresse IPv4 affectée à la passerelle 20 est une adresse partagée Shared@IPv4.

En relation avec la **figure 1**, la passerelle résidentielle 20 est connectée au réseau de l'opérateur par un routeur d'accès 30. Il s'agit du premier routeur que les paquets de données IPv6 et IPv4 rencontrent lorsqu'ils sortent de la passerelle résidentielle.

Suivant l'architecture réseau adoptée au niveau du routage IPv6, le routeur d'accès 30 peut annoncer en direction de l'amont du réseau (i.e. vers le réseau 1 du fournisseur de service de connectivité IP) les préfixes IPv6 qu'il route, c'est-à-dire les préfixes IPv6_prefix_ports_range et IPv6_prefix_native des passerelles résidentielles qu'il dessert.

Le routeur d'accès 30 obtient les préfixes IPv6 des passerelles résidentielles qu'il dessert de façon tout à fait classique dans un environnement réseau IPv6. On peut citer deux méthodes qui sont décrites ci-dessous:

1- il reçoit les annonces de routage IPv6 des passerelles résidentielles qu'il dessert (IPv6_prefix_ports_range et IPv6_prefix_native). A cet effet, chaque passerelle

Juniper Exhibit 1002, page 107

résidentielle annonce ses préfixes vers l'amont (IPv6_prefix_ports_range et IPv6_prefix_native); ou

2- Il obtient les différents IPv6_prefix_ports_range et IPv6_prefix_native par délégation de préfixes comme décrit dans le RFC 3633 (*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*).

En relation avec la **figure 2**, on présente maintenant un exemple de constitution d'un préfixe d'adresses IPv6 construites selon l'invention, tel que le préfixe IPv6_prefix_ports_range affecté à la passerelle résidentielle 20.

Ce préfixe IPv6 englobe les bits de l'adresse IPv4 publique Shared_@IPv4 et la plage de numéros de ports autorisés (ports_pattern/length_of_unvariable) pour la passerelle 20, et permet de façon univoque de router le paquet IPv6 entrant jusqu'à la passerelle résidentielle destinatrice. Il s'agit d'un préfixe IPv6 qui est routable dans un réseau IPv6. Il pourrait même être routé dans l'Internet IPv6, si l'on choisissait qu'il soit un préfixe s'inscrivant dans le préfixe de l'opérateur de réseau fournissant la passerelle résidentielle (particulièrement s'il était annoncé dans BGP (Border Gateway Protocol)).
Selon l'exemple de la figure 2, ce préfixe comprend de gauche à droite :

- le préfixe IPv6 affecté au nœud d'accès 40 : préfixe IPv6/IPv4_Access_Node_prefix ;
  De façon avantageuse, ce préfixe est choisi de telle sorte qu'il s'inscrive dans le préfixe opérateur IPv6 IPv6-prov affecté au fournisseur de service de connectivité IP par son RIR (Regional Internet Registry) et donc qu'il comporte ce préfixe opérateur dans ses premiers bits :
- les bits IPv6/IPv4_Access_Node_Service identifiant chez l'opérateur le service d'interconnexion IPv6/IPv4_Access_Node selon la présente invention. La séquence composée des bits du préfixe opérateur suivis des bits IPv6/IPv4_Access_Node_Service compose le préfixe IPv6/IPv4_Access_Node_Service_prefix qui identifie le service ;
- des bits complémentaires identifiant un nœud d'accès particulier IPv6/IPv4_Access_Node desservant la passerelle résidentielle. Pour des raisons de partage de charge (ou Load-balancing), le préfixe

IPv6/IPv4_Access_Node_prefix peut n'être pas spécifique à un seul nœud d'accès.

- Les 32 bits de l'adresse Shared_@IPv4 de la passerelle 20 ;
- De façon optionnelle, 8 bits réservés, mis à 0. Cet octet peut servir à faire la distinction entre les différents types de ports (UDP, TCP, SCTP, etc.) Il prendrait la valeur "X" pour le traitement UDP et "Y" pour le traitement "TCP", etc.
- Les 16 bits représentant la plage de numéros de ports autorisés pour la passerelle ou "ports_pattern", avec une partie invariable à gauche dans ces 16 bits (bits de poids le plus fort), de longueur length_of_unvariable, étant significative. On notera que dans le cas où l'adresse IPv4 de la passerelle 20 n'est pas partagée par plusieurs passerelles résidentielles, la plage de numéros de ports autorisés est de taille maximale et identique pour toutes les passerelles.

La longueur du préfixe IPv6_prefix_ports_range est établie comme suit :

[128 – 16 (longueur d'une adresse IPv6 – adresse du codage d'un port) = 112 bits
Plus length_of_unvariable (longueur des bits invariants représentant la plage de ports source autorisés).]

On notera que le préfixe IPv6_prefix_ports_range constitué selon l'invention est plus long que les préfixes recommandés par le standard IPv6 pour un déploiement IPv6. Néanmoins, ceci ne l'empêche pas d'être conforme aux standards IPv6.

Le domaine IPv6 1 présenté en relation avec la figure 1 comprend au moins un nœud d'accès 40 selon l'invention. On notera qu'il peut en comprendre plusieurs autres. Le nœud d'accès 40 IPv6/IPv4_Access_Node est un routeur particulier Dual-Stack (IPv4 et IPv6), c'est-à-dire qu'il implémente à la fois les protocoles IPv4 et IPv6.

Dans le réseau 1, le nœud d'accès 40 IPv6/IPv4_Access_Node est typiquement situé en amont du ou des routeurs d'accès 30 (donc vers le cœur du réseau ou dans un segment d'interconnexion avec des réseaux adjacents), comme représenté sur la **figure 1**. Ledit nœud d'accès est aussi appelé nœud d'interconnexion.

Juniper Exhibit 1002, page 109

Le procédé de réception d'un paquet de données IPv6 dans le domaine IPv6 va maintenant être décrit en relation avec la figure 3. De façon avantageuse, il est mis en œuvre par un dispositif de réception compris dans une passerelle résidentielle connectée au domaine IPv6, telle que la passerelle 20 et il est destiné à traiter aussi bien des paquets en provenance du réseau résidentiel 2 que des paquets de données en provenance du domaine IPv4 3. Un tel procédé comprend une étape R1 d'identification de l'adresse de destination IPv6 comme étant du type adresse de destination IPv6 native, soit comme étant du type adresse de destination IPv6 construite par concaténation d'un préfixe de nœud d'accès, d'une adresse IPv4 de destination et d'un numéro de port IPv4 de destination. On suppose ici que la passerelle 20 a obtenu ce préfixe au préalable, par exemple par configuration.

Il comprend ensuite une étape R2 de mise en conformité d'une adresse du paquet de données. Dans le sens réseau résidentiel vers un domaine IPv6, il s'agit de l'adresse source du paquet; dans le sens domaine IPv6 vers un réseau résidentiel, il s'agit de son adresse de destination. Une telle mise en conformité peut entraîner une modification du paquet de données. Le paquet de données modifié est ensuite routé en R3 vers sa destination.

Selon un premier mode de réalisation de l'invention, On considère l'établissement d'une communication sortante vers un destinataire IPv4 qui peut, par exemple, être un serveur Web IPv4 localisé dans le réseau Internet. Un terminal d'utilisateur du réseau résidentiel 2, par exemple le PC IPv6 22 connecté à la passerelle 20, émet un paquet de données à destination de ce correspondant du domaine IPv4 3. Dans ce cas, l'application mise en œuvre sur le PC est un browser IPv6. On rappelle que le terminal d'utilisateur source 22 est purement IPv6.

On distingue plusieurs cas :

- le terminal d'utilisateur 22 émet un paquet de données IPv6 à l'aide d'une adresse source égale à une adresse IPv6 construite qui lui a été affectée; ou
- le terminal d'utilisateur 22 émet un paquet de données IPv6 à l'aide d'une adresse source égale à une adresse IPv6 native qui lui a été affectée.

Juniper Exhibit 1002, page 110

On comprend que le paquet de données comprend une adresse de destination IPv6 correspondant au destinataire IPv4 que le terminal doit avoir récupéré au préalable.

Le browser du terminal 22 a donc besoin de connaître l'adresse IPv6 du serveur Web destinataire. Or, le serveur Web n'est accessible qu'en IPv4. Il faut donc que le terminal 22 dispose d'une adresse IPv6 qu'il considérera comme l'adresse du serveur Web (alors qu'en réalité le serveur Web ne dispose que d'une adresse IPv4).

Pour ce faire, une fonction de traduction d'une adresse IPv4 du serveur Web en une adresse IPv6 doit être implémentée par le fournisseur de service de connectivité IP ou par une partie tierce. Cette fonction de traduction doit respecter un formalisme de construction de l'adresse IPv6 de telle manière qu'elle contienne l'adresse IPv4 du correspondant (le serveur Web dans notre exemple). Cette fonction de traduction va maintenant être décrite en relation avec la **figure 4**.

Une telle fonction de traduction que nous appellerons DNS_IPv4toIPv6 peut être réalisée, par exemple, par le nœud d'accès 40 IPv6/IPv4_Access_Node du domaine IPv6 1, mais de façon plus générale, on considère qu'elle est mise en œuvre par un serveur DNS du domaine 1. La fonction DNS_IPv4toIPv6 est le point de contact par défaut pour toute demande de résolution DNS émise par un terminal demandeur. Par défaut, cette fonction examine d'abord les enregistrements IPv6 de type "AAAA", autrement dit les adresses IPv6 natives. Si un enregistrement est déjà présent, une réponse est alors émise vers le terminal demandeur. Si aucun enregistrement n'est présent, une demande de résolution de type "A" est alors effectuée par la fonction de traduction DNS_IPv4toIPv6. Sur réception de la réponse d'un serveur DNS comprenant l'adresse IPv4 du correspondant (le serveur Web dans notre exemple), la fonction DNS_IPv4toIPv6 transforme l'adresse IPv4 reçue dans la réponse en adresse IPv6, suivant le formalisme présenté en relation avec la figure 4 et garde cette information dans son cache.

On notera que l'exemple de la **figure 4** n'est qu'un mode de réalisation, l'essentiel étant que l'adresse IPv4 du correspondant (ici le serveur Web) soit inscrite dans une

adresse IPv6. Si aucune réponse n'est reçue de la part d'un serveur DNS, alors un message d'erreur est transmis au terminal demandeur.

Nous appellerons IPv6_remoteAddress_out_to_IPv4 l'adresse du destinataire (ici le serveur Web) ainsi transformée en IPv6. On notera que le terminal demandeur peut récupérer une adresse IPv6 de la machine distante à contacter par d'autres moyens, par exemple auprès d'un serveur.

Dans tous les cas, l'adresse IPv6 du correspondant (ici le serveur Web) peut être une adresse IPv6 native ou une adresse IPv6 respectant le formalisme introduit par la présente invention. Dans le cas d'une adresse IPv6_remoteAddress_out_to_IPv4 construite, elle est incluse dans le préfixe IPv6/IPv4_Access_Node_Service_prefix.

En relation avec la **figure 4**, on remarque que la séquence de 2 octets la plus à droite est marquée "réservée" et mise à 0 par défaut. Cet emplacement correspond à celui des bits de ports dans une adresse IPv6 IPv4inIPv6_dest_address pour les paquets destinés à un terminal d'utilisateur. Il est réservé de manière à pouvoir indiquer un port sur lequel le correspondant (ici le serveur Web) désire se faire appeler en particulier. Il pourrait s'agir d'un correspondant IPv4 qui lui aussi se verrait affecté une adresse IPv4 partagée entre plusieurs correspondants et qui donc ne disposerait pas de tous les ports disponibles.

Le terminal 22 émet ensuite un paquet de données IPv6 comprenant l'adresse IPv6_remoteAddress_out_to_IPv4 comme adresse de destination.

La passerelle résidentielle 20 selon l'invention comprend un dispositif de réception d'un paquet de données selon l'invention. Sur réception de ce paquet IPv6, un tel dispositif est apte à mettre en œuvre le procédé de transmission d'un paquet IPv6 à destination d'une adresse IPv6 représentant une machine connectée à un domaine IPv4 selon le premier mode de réalisation de l'invention, qui va maintenant être décrit en référence à la **figure 5**.

Un tel procédé met en œuvre l'étape R1 d'identification de l'adresse de destination IPv6 précédemment décrite.

Selon un aspect de l'invention, la passerelle résidentielle 20 connaît la longueur du préfixe IPv4_Access_Node_Service_prefix, pour aisément déterminer sa valeur en prenant les bits correspondants dans son IPv6_prefix_ports_range. Une telle identification consiste à classer comme une adresse construite une adresse IPv6 de destination qui s'inscrit dans le préfixe IPv6/IPv4_Access_Node_Service_prefix et à considérer toutes les adresses hors de ce préfixe comme des adresses natives.

Un avantage de cette identification est qu'elle est simple.

Cette méthode d'identification n'est valable toutefois que dans le contexte d'un seul opérateur. Pour un déploiement grand échelle avec mutualisation de nœuds d'interconnexion entre les domaines IPv4 et IPv6, cette méthode n'est plus appropriée.

Une telle identification peut consister à rechercher dans l'adresse de destination un identificateur ou tag, dont la valeur peut être représentative d'une adresse native ou d'une adresse construite. A titre d'exemple, comme indiqué sur la **figure 4**, un tel identificateur peut avoir une longueur d'un seul bit ADDR_TYPE_TAG, valorisé à 0 ou 1 pour indiquer qu'il s'agit d'une adresse native ou construite. L'identifiant ADDR_TYPE_TAG peut être positionné, par exemple, au début de l'adresse IPv6 construite pour faciliter les opérations de lecture, ou encore entre le IPv6/IPv4_Access_Node_Service_prefix et l'adresse IPv4.

Un avantage de l'identifiant ADDR_TYPE_TAG est qu'il permet une mutualisation des équipements d'interconnexion IPV4 IPv6 entre plusieurs opérateurs et donc un partage des coûts. Ainsi, un opérateur Oi peut assurer l'interconnexion IPv4-IPv6 pour une région Ri (avec un ensemble de préfixes IPv4 Pi). Pour les autres opérateurs Oj, seules les adresses construites par un opérateur Oi (sur la base des préfixes IPv4) sont visibles, par le biais d'annonces BGP.

On comprend bien que d'autres préfixes que le IPv6/IPv4 peuvent exister, mais ils ne sont pas utilisés pour rendre ce service de connectivité et le traitement qui leur est appliqué est celui d'un paquet IPv6 natif, c'est-à-dire qu'il est routé directement vers le routeur d'accès IPv6 30;

Juniper Exhibit 1002, page 113

Si l'adresse IPv6 de destination est classée comme construite, le procédé de transmission selon l'invention réalise une étape R2 de mise en conformité de l'adresse source du paquet à transmettre.

Dans ce premier mode de réalisation de l'invention, une telle mise en conformité consiste à identifier en R_{21} si l'adresse source est une adresse construite ou native. Une adresse est considérée comme construite s'il s'agit d'une adresse IPv6 source qui s'inscrit dans le préfixe IPv6/IPv4_Access_Node_Service_prefix, toutes les adresses hors de ce préfixe étant considérées comme des adresses sources natives. Si l'identifiant ADDR_TYPE_TAG est utilisé, alors une adresse est identifiée comme construite si l'identifiant ADDR_TYPE_TAG est positionné à « 1 ».

Si l'adresse source est construite, le paquet de données est routé vers sa destination en R3.

Si l'adresse IPv6 source est classée comme native, le procédé selon l'invention met en œuvre, préalablement à cette étape de routage, une étape R_{22} destinée à choisir une adresse IPv6 source construite dont le numéro de port source est dans la plage autorisée ports_pattern/length_of_unvariable affectée à la passerelle 20 et à modifier le paquet de données en remplaçant l'adresse source native par cette adresse construite. En R_{24}, le procédé selon l'invention crée une entrée dans la table de traduction d'adresses de la passerelle, ladite entrée comprenant une association de l'adresse source native et de l'adresse source ainsi construite.

De façon avantageuse, le procédé selon l'invention peut en outre de vérifier en R_{23} une concordance du numéro de port source contenu dans l'adresse source construite avec le numéro de port source de niveau transport du paquet de données. En relation avec la **figure 6**, on voit qu'une telle création consiste à prendre une adresse IPv6 quelconque de 128 bits comprenant comprise dans le IPv6_prefix_ports_range et à y recopier dans les 16 bits de droite les bits du port source utilisé (le port TCP ou UDP du paquet IPv6 reçu du terminal 22) dans le paquet de données à transmettre.

On comprendra que cette étape est nécessaire pour que le nœud d'accès IPv6/IPv4 40 puisse traduire le paquet de données IPv6 en un paquet de données IPv4

Juniper Exhibit 1002, page 114

avant de le router vers le domaine IPv4 destinataire. Elle présente un autre avantage dans le cas où l'adresse IPv4 affectée à la passerelle résidentielle 20 est une adresse partagée par plusieurs passerelles résidentielles du domaine IPv6 1. En effet, comme évoqué précédemment, la passerelle résidentielle 20 ne peut utiliser que les numéros de port source appartenant à une plage de numéros de port restreinte qui lui a été réservée.

On notera également que si la passerelle résidentielle 20 a bien contraint le port source à être dans la plage de numéros de ports autorisés ports_pattern/length_of_unvariable, alors l'adresse source construite:

- est inscrite dans le préfixe IPv6_prefix_ports_range; et
- ses 16 derniers bits sont identiques au numéro de port source du paquet IPv6 reçu du terminal par la passerelle;

Dans la suite, on appellera IPv6_address_source_ports_range l'adresse source IPv6 ainsi formée.

En R3, le paquet IPv6 comprenant l'adresse IPv6 source contrainte IPv6_address_source_ports_range est ensuite routé vers le routeur d'accès IPv6 30 qui dessert la passerelle.

Le routeur d'accès IPv6 30 vérifie que l'adresse source IPv6 IPv6_address_source_ports_range est bien autorisée pour la passerelle résidentielle 20. Il vérifie en d'autres termes qu'il n'y a pas de "spoofing", c'est-à-dire que la passerelle résidentielle 20 émet bien des paquets IPv6 dans son préfixe IPv6_prefix_ports_range autorisé. Pour cela le routeur d'accès IPv6 30 vérifie que l'adresse source IPv6 IPv6_address_source_ports_range du paquet IPv6 reçu de la passerelle 20 est bien inscrite dans le préfixe IPv6_prefix_ports_range affecté à cette passerelle résidentielle. Cette vérification est effectuée de façon classique selon un principe déjà utilisé pour le trafic IPv6 natif.

Si cette vérification est positive, le routeur d'accès IPv6 30 route le paquet IPv6 vers sa destination.

Puisque l'adresse IPv6 de destination s'inscrit dans le préfixe IPv6/IPv4_Access_Node_prefix caractérisant le nœud d'accès

Juniper Exhibit 1002, page 115

IPv6/IPv4_Access_Node 40 au domaine IPv6, le paquet de données est routé vers ce nœud d'accès. On suppose, par exemple, qu'un tel nœud est placé dans le domaine IPv6 1 au plus près du ou des domaines IPv4 qu'il dessert, afin d'optimiser le routage des paquets de données vers ces domaines, mais l'invention ne se limite pas à une telle situation du nœud d'accès 40, ledit nœud d'accès pouvant être situé n'importe où dans le domaine 1.

Sur réception du paquet IPv6, le nœud d'accès IPv6/IPv4_Access_Node 40 achemine le paquet de données sortant à destination d'un domaine IPv4 de la façon suivante :

- Il extrait une adresse de destination IPv4 et d'un port de destination de l'adresse de destination IPv6 et une adresse source IPv4 et d'un port source de l'adresse source IPv6 ;
- Il traduit ensuite le paquet IPv6 en un paquet IPv4 qui a les caractéristiques suivantes :
  - son adresse source IPv4 est l'adresse IPv4 Shared_@IPv4 de la passerelle résidentielle 20. C'est cette adresse Shared_@IPv4 que verra le destinataire du paquet de données IPv4 transmis (le serveur Web). Pour rappel, cette adresse IPv4 Shared_@IPv4 est incluse dans le préfixe IPv6_prefix_ports_range et donc dans l'adresse IPv6 source IPv6_address_source_ports_range. En relation avec la figure 8, l'adresse IPv4 Shared_@IPv4 peut être extraite des bits 24 à 55 ;
  - son adresse de destination IPv4 est l'adresse IPv4 du correspondant. En relation avec la figure 4, l'adresse IPv4 du destinataire peut être extraite des bits 24 à 55 de l'adresse IPv6_remoteAddress_out_to_IPv4 du paquet de données IPv6 reçu par le nœud d'accès 40 ;
  - la valeur du numéro de port source du paquet de données IPv4 traduit est le numéro du port source du paquet IPv6 reçu ;
  - le numéro de port de destination du paquet de données IPv4 traduit est le même que celui du paquet IPv6 ;

Juniper Exhibit 1002, page 116

- la partie utile du paquet IPv6 est la partie utile du paquet IPv4 traduit;

On notera que les champs de l'en-tête du paquet IPv6 sont traduits en champs IPv4 correspondant de façon classique, par exemple selon les principes du standard NAT-PT (*Network Address Translation- Protocol Translation*).

- Il route enfin le paquet IPv4 traduit vers son destinataire (le serveur Web IPv4 dans notre exemple).

On comprend que, lorsque l'adresse IPv4 affectée à la passerelle résidentielle 20 est une adresse publique partagée entre plusieurs passerelles, il est nécessaire que le numéro de port source contenu dans l'adresse IPv6 source construite du paquet de données reçu appartienne bien à la plage de numéros de ports réservés à cette passerelle. En effet, si ce n'était pas le cas, le nœud d'accès pourrait traduire le paquet IPv6 à transmettre en un paquet de données IPv4, mais les éventuels paquets de réponse émis par le destinataire ne parviendraient pas à la passerelle résidentielle.

De façon avantageuse, le nœud d'accès 40 contrôle l'appartenance du port source à la plage de numéros de ports source affectée à la passerelle 20. Une telle étape consiste à contrôler que les derniers 16 bits de l'adresse source IPv6 du paquet sont identiques aux 16 bits du port source dans le champ correspondant TCP ou UDP du paquet IPv6. Il s'agit d'un contrôle indirect, qui peut faire suite à la vérification par le routeur d'accès du fait que la passerelle résidentielle a bien envoyé un paquet dont l'adresse source est dans son préfixe. A l'issue de ces deux étapes, on peut être certain que la passerelle résidentielle 20 a bien émis un paquet de données comprenant un port source inclus dans sa plage de ports autorisés et n'a pas utilisé celle d'une autre passerelle résidentielle.

Selon un deuxième mode de réalisation de l'invention, on considère le cas d'un paquet de données IPv4-in-pt entrant dans un domaine IPv6 en provenance d'un domaine IPv4 et destiné à un terminal d'utilisateur du domaine IPv6 1, par exemple le terminal 21. Le terminal se situe derrière la passerelle résidentielle 20 qui dispose d'une adresse IPv4 @IPv4 ou Shared_@IPv4 et d'une plage de ports autorisés ports_pattern/length_of_unvariable.

Juniper Exhibit 1002, page 117

Le paquet IPv4-in-pt entrant, s'il est destiné au terminal d'utilisateur 21 du réseau résidentiel de la passerelle résidentielle 20, comprend une adresse de destination IPv4 égale à Shared_@IPv4 et un port de destination s'inscrivant dans la plage de numéros de ports autorisés ports_pattern/length_of_unvariable de la passerelle résidentielle 20.

Comme évoqué précédemment en relation avec la **figure 2**, l'adresse Shared_@IPv4 et la plage de numéros de ports ports_pattern/lenght_of_unvariable se retrouvent dans le préfixe IPv6_prefix_ports_range de la passerelle résidentielle 20.

Le paquet IPv4-in-pt est reçu par le nœud d'accès 40. En effet, dans une étape préalable, le fournisseur de connectivité IP a annoncé aux domaines IPv4 avec lesquels il a une interface, les adresses IPv4 affectées à des passerelles résidentielles du domaine 1 à destination desquelles il avait la charge d'acheminer les paquets IPv4. Il a fait cette annonce, soit par l'intermédiaire du nœud d'accès 40 lui-même ou d'un ASBR (Autonomous System Border Router) selon une technique connue de l'homme de métier.

Le paquet IPv4-in-pt comprend une adresse de destination @IPv4 ou shared@IPv4 gérée par le nœud d'accès 40 et un port de destination dest-port. Le nœud d'accès 40 est apte à construire une adresse de destination IPv6 IPv4inIPv6_dest_address par concaténation d'un préfixe IPv6/IPv4_Access_Node_prefix du nœud d'accès 40, de ladite adresse de destination IPv4 shared-@IPv4 et du numéro de port de destination dest-port, comme décrit en relation avec la **figure 7**.

Le numéro de port de destination dest-port est inséré dans la partie droite de l'adresse de destination IPv6 construite. Il insère donc à la fois les 32 bits de l'adresse IPv4 de destination du paquet IPv4 reçu et les 16 bits du port de destination dest-port pour constituer une adresse IPv6 de destination construite que nous appelons IPv4inIPv6_dest_address.

Le nœud d'accès 40 génère ensuite un paquet de données IPv6 IPv4inIPv6-pt à partir de l'adresse de destination IPv6 IPv4inIPv6_dest_address construite et du

paquet de données IPv4 reçu. Un mode de réalisation consiste à traduire le paquet IPv4 reçu dans un paquet IPv6:

- dont l'adresse source IPv6 est une des adresses IPv6 dont dispose l'IPv6/IPv4_Access_Node 40 en propre (pour une de ses interfaces);
- et dont l'adresse de destination IPv6 est l'adresse IPv4inIPv6_dest_address.

Un autre mode de réalisation consiste à traduire le paquet IPv4 IPv4-in-pt reçu en un paquet IPv6 auquel on associe l'adresse IPv6 construite après avoir préalablement extrait du paquet IPv4 reçu son adresse IPv4 de destination, son port de destination, son adresse IPv4 source et son port source.

Le paquet de données IPv6 IPv4inIPv6-pt généré à l'aide de l'adresse de destination IPv6 construite est routé dans le domaine IPv6 1. Le paquet IPv4inIPv6-pt passe donc dans le cœur de routage IPv6 du nœud d'accès 40 IPv6/IPv4_Access_Node.

Par construction, son adresse de destination IPv4inIPv6_dest_address s'inscrit dans le préfixe IPv6_prefix_ports_range de la passerelle résidentielle 20. Le paquet IPv4inIPv6-pt est routé vers l'interface du nœud d'accès IPv6/IPv4_Access_Node 40 qui dessert la route IPv6 correspondante vers de la passerelle résidentielle 20.

On notera que si l'adresse de destination IPv4inIPv6_dest_address ne s'inscrivait dans aucun préfixe IPv6_prefix_ports_range (ou aucun préfixe englobant), le paquet serait détruit à un moment à un autre sur la route, car il ne pourrait être routé vers aucun préfixe IPv6_prefix_ports_range et donc vers aucune passerelle résidentielle.

Si l'adresse de destination IPv4inIPv6_dest_address s'inscrit bien dans le préfixe IPv6_prefix_ports_range, le paquet IPv4inIPv6-pt parvient au routeur_d'acces_dual_stack 30 desservant la passerelle résidentielle 20 qui héberge le terminal d'utilisateur 21 dans son réseau résidentiel 2. Il est routé par le routeur_d'acces_dual_stack 30 vers la passerelle résidentielle, lequel connaît la route vers le préfixe IPv6_prefix_ports_range.

Selon ce deuxième mode de réalisation de l'invention, la passerelle résidentielle 20 comprend un dispositif mettant en œuvre le procédé de réception du paquet de

données IPv4inIPv6-pt selon l'invention. Un tel procédé va maintenant être décrit en relation avec la **figure 8**.

Lorsque le paquet IPv4inIPv6-pt parvient à la passerelle résidentielle 20, celle-ci met en œuvre l'étape R'1 d'identification de l'adresse de destination précédemment décrite.

Si une adresse de destination native est identifiée, le paquet de données est routé directement vers le terminal d'utilisateur destinataire, dans une étape R'3.

Si une adresse de destination construite est identifiée, par exemple à l'aide d'un identifiant compris dans l'adresse de destination, l'étape de mise en conformité du procédé de réception d'un paquet de données selon l'invention comprend une étape R'_{21} de recherche dans la table de traduction de la passerelle résidentielle d'une entrée comprenant l'adresse de destination construite. Si cette recherche est positive, une telle entrée associe à l'adresse de destination construite une adresse de destination native IPv6_address_native-UE du terminal destinataire. En R'_{23}, le procédé selon l'invention remplace l'adresse de destination construite par cette adresse native dans le paquet de données IPv6. Ce remplacement est particulièrement avantageux dans le cas où le paquet de données IPv4-in-pt fait partie d'une réponse à un paquet de données émis préalablement par le terminal destinataire 21 avec son adresse source IPv6 native, et pour lequel la passerelle avait en effet préalablement stocké cette adresse native dans sa table de NAT avant sa transmission, comme décrit dans le mode de réalisation précédent de l'invention. A ce moment-là, elle avait crée l'entrée dans sa table de traduction et remplacé cette adresse native par l'adresse construite du terminal 21, afin de permettre au nœud d'accès 40 d'en extraire une adresse source IPv4 lors de la transformation du paquet IPv6 sortant en un paquet IPv4.

De façon avantageuse, l'étape de mise en conformité comprend en outre une étape R'22 de vérification d'une concordance du port de destination de niveau transport du paquet de données avec le numéro de port de destination contenu dans l'adresse de destination du paquet. Si les deux numéros de port ne concordent pas, le paquet est rejeté. Ceci ne doit pas avoir lieu si la traduction a été effectuée par

Juniper Exhibit 1002, page 120

le nœud d'accès, mais cette étape peut être utilisée pour réaliser un contrôle de flux en provenance du nœud d'accès.

En R'3, le paquet de données est routé par la passerelle vers le terminal destinataire de son réseau résidentiel.

Dans l'exemple décrit en relation avec la **figure 1**, la passerelle résidentielle 20 selon l'invention comporte un dispositif 25 de réception d'un paquet de données dans un domaine IPv6, qui va être maintenant décrit en relation avec la **figure 10**. Il comprend les éléments matériels que l'on retrouve classiquement dans un ordinateur conventionnel ou un routeur spécialisé, à savoir un processeur 25_1, une mémoire vive de type RAM 25_2, une mémoire morte de type ROM 25_3 et des moyens 25_4 de télécommunications avec le réseau 1.

Conformément à l'invention, le dispositif 25 comporte une mémoire 25_5 comprenant une base de données dans laquelle est stockée une table de traduction d'adresses ou NAT entre le domaine 1 et son réseau résidentiel 3.
On notera que cette mémoire peut aussi bien être externe au dispositif 25 pourvu qu'il puisse y accéder.

La mémoire morte 25_5 constitue un support d'enregistrement conforme à l'invention. Ce support mémorise le programme d'ordinateur conforme à l'invention. Ce programme comporte des instructions pour l'exécution des étapes du procédé de réception d'un paquet entrant conforme à l'invention qui vient d'être décrit en référence aux figures 3, 5 et 8.

On notera également que le dispositif de réception peut aussi bien être inclus dans un terminal d'utilisateur connecté directement au réseau 1 du fournisseur de service de connectivité.

En résumé, l'invention permet une deuxième phase de migration des services de connectivité IP vers IPv6 à l'aide de mécanismes d'acheminement des paquets qui prennent en compte les faits suivants :

Juniper Exhibit 1002, page 121

- La migration finale vers IPv6 prendrait plusieurs années (une échelle de 10 ans minimum). Ceci est dû principalement au nombre important des acteurs à « convaincre » pour un passage vers IPv6, le nombre important des AS (Autonomous System) (plus de 17000) ; de la diversité des mécanismes d'interconnexion. De plus, nous tenons à préciser que le problème des adresses ne concerne à priori que les opérateurs. Les clients n'ont aucune raison pour modifier l'architecture de leurs réseaux locaux. Une entreprise "Méchu" n'a pas de motivations pour migrer ses serveurs FTP, HTTP, etc. vers IPv6. Les opérateurs doivent s'attendre à un long travail d'accompagnement pour le passage vers IPv6 ;
- Les opérateurs de services souffrent d'un problème d'épuisement d'adresses IPv4 tel que décrit dans la section plus-haut ;
- La simple migration vers IPv6 d'un domaine donné ne résout pas le problème de la connectivité globale (joindre n'importe quelle machine distante présente sur Internet). En effet, une interconnexion avec le monde IPv4 doit être mise en place ;
- Une solution à base de NAT-PT avec état n'est pas recommandée. Le service fourni en serait dégradé, vu que les services à valeur ajoutée liés au « port forwarding » configuré par les clients ne fonctionneront pas et dépendront du comportement du « boitier » d'interconnexion entre un nuage IPv4 et un autre IPv6.

Les mécanismes d'acheminement des paquets IP selon l'invention permettent de promouvoir l'utilisation du protocole IPv6 de la façon suivante :

- activation d'IPv6 et mise en place d'une solution permettant de promouvoir le trafic IPv6 basée sur une fonction d'interconnexion placée dans le réseau, qui est sans état. La solution de l'invention n'utilise que la connectivité IPv6 des passerelles résidentielles et implique l'utilisation de terminaux d'utilisateurs et passerelles résidentielles IPv6. De ce fait ces équipements ne sont en mesure de traiter (recevoir et émettre) que des paquets de données de type IPv6.

La solution de l'invention permet :

- que le réseau d'accès ne soit qu'IPv6 et ainsi que l'opérateur d'accès n'ait pas à gérer le routage IPv4 à l'accès ;
- que les passerelles résidentielles n'aient aucune notion d'IPv4 et ne gèrent que l'IPv6 ;

Juniper Exhibit 1002, page 122

- que les terminaux du réseau résidentiel de la passerelle résidentielle puissent n'utiliser qu'IPv6.

Une même adresse IPv4 peut être affectée à plusieurs passerelles résidentielles (ou autres équipements dans des contextes autres que l'accès Internet résidentiel). Il s'agit d'une affectation fictive au niveau de la passerelle résidentielle, puisque les passerelles résidentielles ne gèrent pas le routage IPv4. Les principes de bases sont les suivants :

- plage de ports source autorisés au niveau de chaque passerelle pour les communications sortantes ;
- préfixe IPv6 particulier IPv6_prefix_ports_range.

Les paquets IPv4 entrants dans le domaine IPv6 ne sont pas encapsulés par l'IPv6/IPv4_Access_Node pour être routés vers la passerelle résidentielle, mais ils sont traduits en paquets IPv6.

- Pour les communications sortantes, sur résolution DNS d'un correspondant IPv4, on retourne au terminal d'utilisateur initiateur une adresse IPv6 construite sur la base de l'adresse IPv4 du correspondant. Le terminal d'utilisateur utilise alors cette adresse de destination IPv6 pour émettre les paquets de données. Pour émettre ce paquet, il peut utiliser son adresse source IPv6 native ou construite.
- S'il a utilisé son adresse source native, la passerelle résidentielle transforme l'adresse IPv6 native source en une adresse source construite IPv6 contenant sa propre adresse IPv4 partagée entre les passerelles (Shared_@IPv4) et le port source (inscrit dans la plage source autorisée).
- Un équipement d'interconnexion du domaine IPv6 au domaine IPv4 vérifie que la passerelle résidentielle a bien utilisé sa plage de ports source autorisés en comparant la partie de l'adresse source qui contient les bits port source et le port source dans le champ port du paquet IPv6. Il traduit le paquet IPv6 en paquet IPv4 pour le transmettre au correspondant en utilisant :
    - pour l'adresse source IPv4 : les bits dans l'adresse IPv6 source qui contiennent Shared_@IPv4
    - pour l'adresse destination IPv4 : les bits dans l'adresse IPv6 qui contiennent l'adresse IPv4 du correspondant.

Juniper Exhibit 1002, page 123

REVENDICATIONS

1. Procédé de réception d'un paquet de données IPv6 dans un domaine IPv6 interconnecté avec un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, caractérisé en ce que, ledit procédé étant mis en œuvre dans une passerelle résidentielle apte à connecter un terminal d'utilisateur audit domaine IPv6, il comprend les étapes suivantes :

- identification d'une adresse IPv6 de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données par remplacement de ladite adresse, ledit remplacement appartenant à un groupe comprenant un remplacement d'une adresse construite par une adresse native et un remplacement d'une adresse native par une adresse construite, et modification du paquet de données à l'aide de l'adresse mise en conformité; et
- routage du paquet de données modifié vers sa destination.

2. Procédé de réception selon la revendication 1, caractérisé en ce que, lorsque le paquet de données est en provenance dudit terminal d'utilisateur et à destination du domaine IPv4, l'étape de mise en conformité de l'adresse source comprend en outre les étapes suivantes :

- identification d'une adresse IPv6 source native;
- création d'une entrée dans une table de traduction d'adresses, ladite entrée associant ladite adresse source native à une adresse source construite par concaténation d'un préfixe opérateur, d'une adresse IPv4 affectée à la passerelle et d'un numéro de port source appartenant à une plage de numéros de ports autorisés pour ladite passerelle; et
- remplacement de l'adresse source native du paquet de données par l'adresse source construite.

3. Procédé de réception selon la revendication 2, caractérisé en ce que

Juniper Exhibit 1002, page 124

l'identification d'adresse est réalisée à l'aide d'un identifiant compris dans l'adresse de destination.

4. Procédé de réception selon la revendication 2, caractérisé en ce qu'il comprend en outre une étape de vérification d'une correspondance entre le numéro de port source du paquet de données et le numéro de port de source de l'adresse source construite.

5. Procédé de réception selon la revendication 1, caractérisé en ce que, lorsque le paquet de données est en provenance du domaine IPv4 et à destination dudit terminal d'utilisateur, l'étape de mise en conformité de l'adresse source comprend les étapes suivantes :

- recherche dans une table de traduction d'adresses de la passerelle d'une entrée associant à ladite adresse de destination construite une adresse de destination native.
- si une entrée a été trouvée, remplacement de l'adresse de destination construite du paquet de données par l'adresse de destination native de l'entrée.

6. Procédé de réception selon la revendication **5**, caractérisé en ce qu'il comprend en outre une étape de vérification d'une correspondance entre le numéro de port de destination du paquet de données et le numéro de port de destination contenu dans l'adresse de destination construite,

7. Dispositif de réception d'un paquet de données dans un domaine IPv6 interconnecté à un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, caractérisé en ce que, ledit dispositif étant destiné à être mis en œuvre dans une passerelle résidentielle apte à connecter un terminal d'utilisateur audit domaine IPv6, il comprend les moyens suivants

- identification d'une adresse IPv6 de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données par remplacement de ladite adresse, ledit remplacement appartenant

Juniper Exhibit 1002, page 125

à un groupe comprenant un remplacement d'une adresse construite en une adresse native et un remplacement d'une adresse native en une adresse construite, et modification du paquet de données à l'aide de l'adresse mise en conformité; et

- routage du paquet de données modifié vers sa destination.

8. Passerelle résidentielle apte à connecter des terminaux d'utilisateurs d'un réseau résidentiel à un domaine IPv6 interconnecté à un domaine IPv4, caractérisée en ce qu'elle comprend :

- des moyens d'obtention d'une adresse IPv4, d'une plage de numéros de ports autorisés pour ladite passerelle et d'une plage d'adresses IPv6 autorisées pour ladite passerelle, ladite plage d'adresses IPv6 étant construite par concaténation d'un préfixe opérateur, de ladite adresse IPv4 et de la plage de numéros de ports IPv4 autorisés; et

- un dispositif de réception d'un paquet de données IPv6 dans le domaine IPv6 interconnecté au domaine IPv4 selon la revendication 7.

9. Passerelle résidentielle selon la revendication **8**, comprenant une table de traduction d'adresses, comprenant des entrées, associant, pour une session de communication impliquant terminal d'utilisateur de son réseau résidentiel, au moins une adresse source, caractérisée en ce que ladite passerelle est apte à enregistrer dans ladite entrée, une adresse source IPv6 construite et une adresse source IPv6 native.

10. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution du procédé de réception d'un paquet de données dans un domaine IPv6 selon la revendication **1**.

Juniper Exhibit 1002, page 126

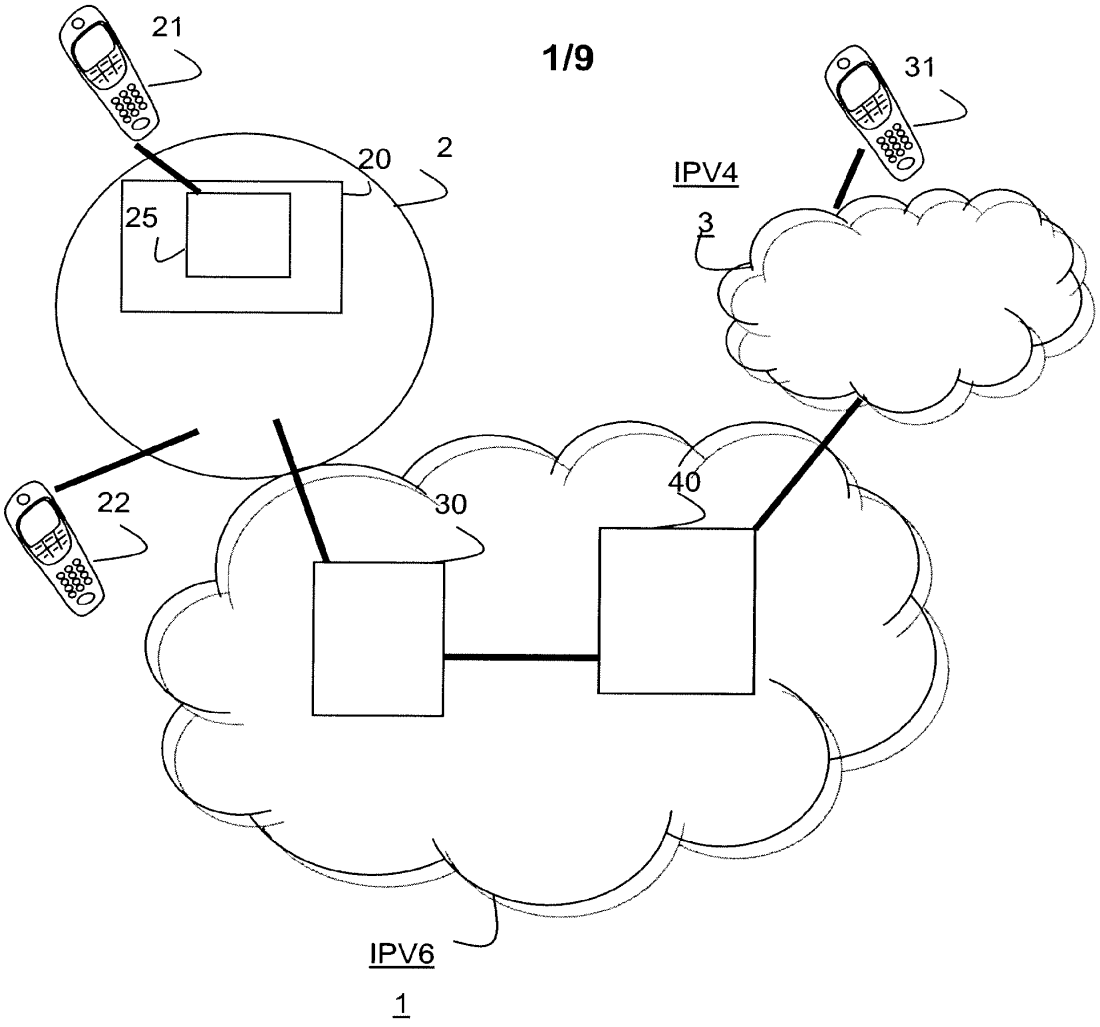


FIG. 1

Juniper Exhibit 1002, page 127

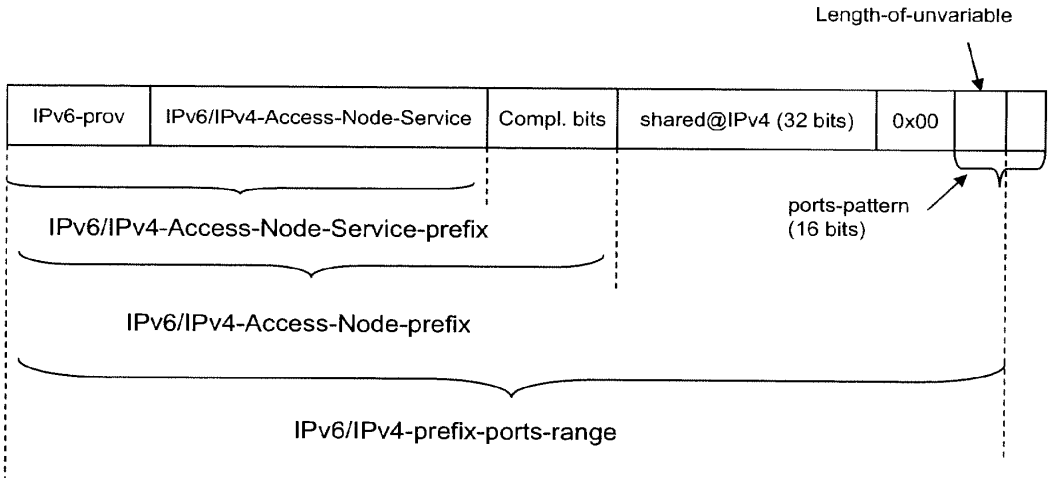

Length-of-unvariable
IPv6-prov
IPv6/IPv4-Access-Node-Service
Compl. bits
shared@IPv4 (32 bits)
0x00
ports-pattern
(16 bits)
IPv6/IPv4-Access-Node-Service-prefix
IPv6/IPv4-Access-Node-prefix
IPv6/IPv4-prefix-ports-range

FIG. 2

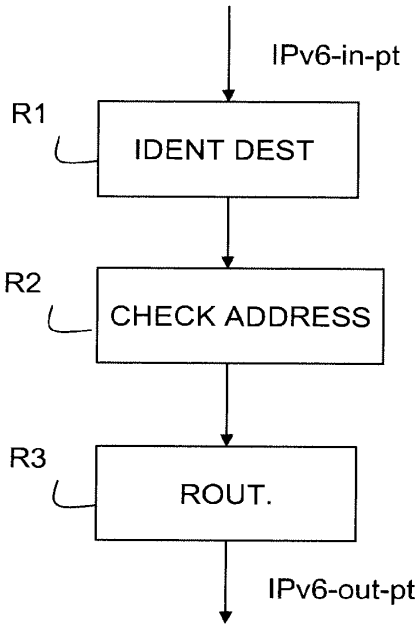


FIG. 3

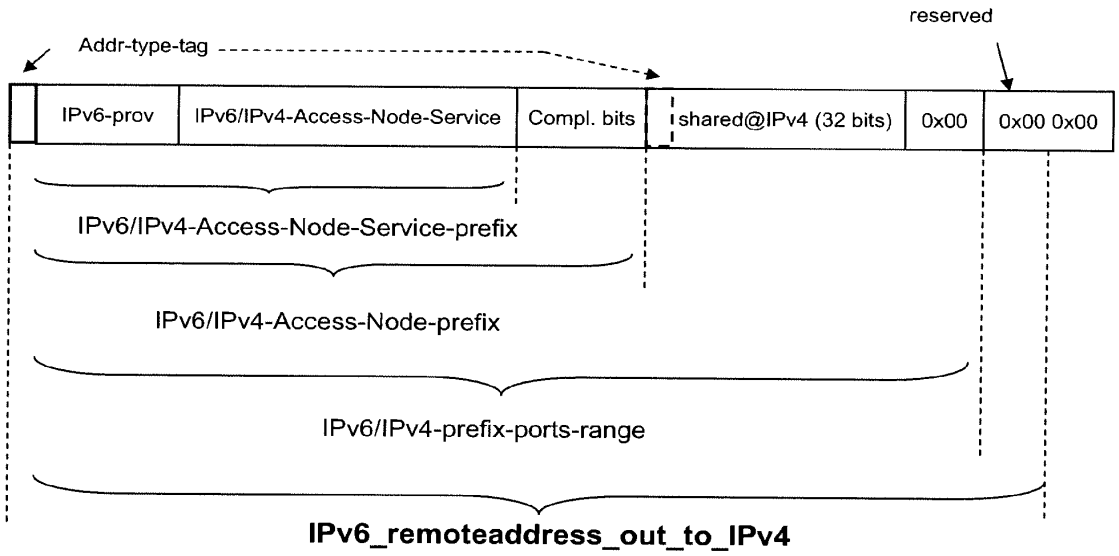


FIG. 4

Juniper Exhibit 1002, page 130

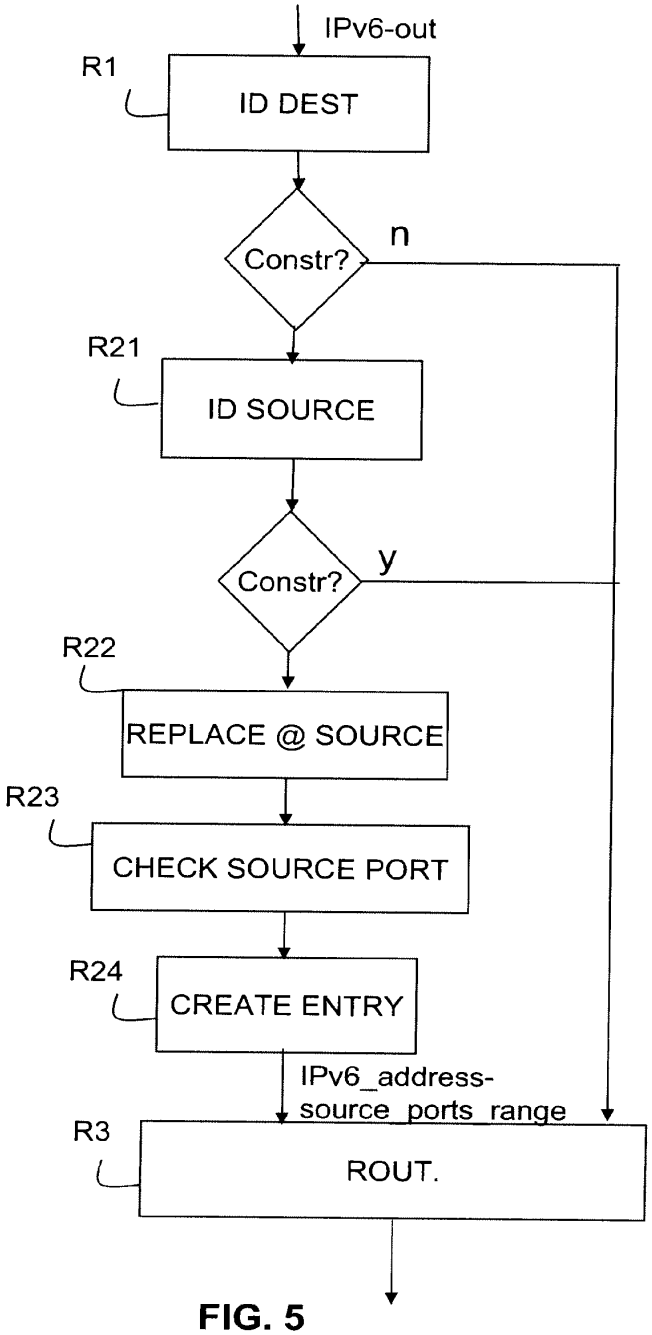

IPv6-out
R1
ID DEST
Constr?
n
R21
ID SOURCE
Constr?
y
R22
REPLACE @ SOURCE
R23
CHECK SOURCE PORT
R24
CREATE ENTRY
IPv6_address-
source_ports_range
R3
ROUT.

FIG. 5

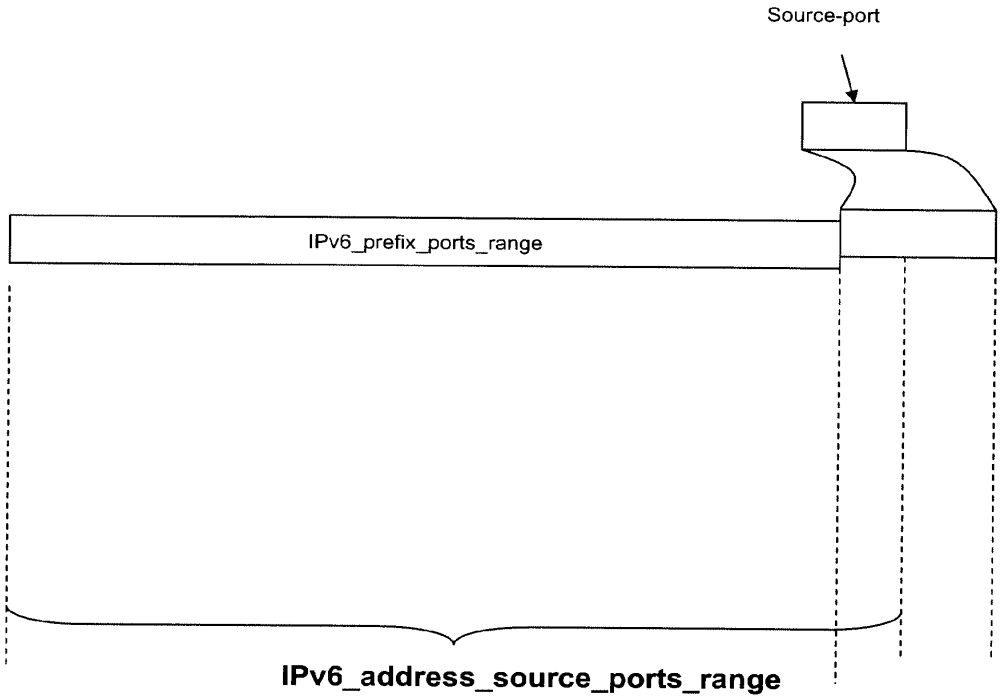

Source-port
IPv6_prefix_ports_range
IPv6_address_source_ports_range

FIG. 6

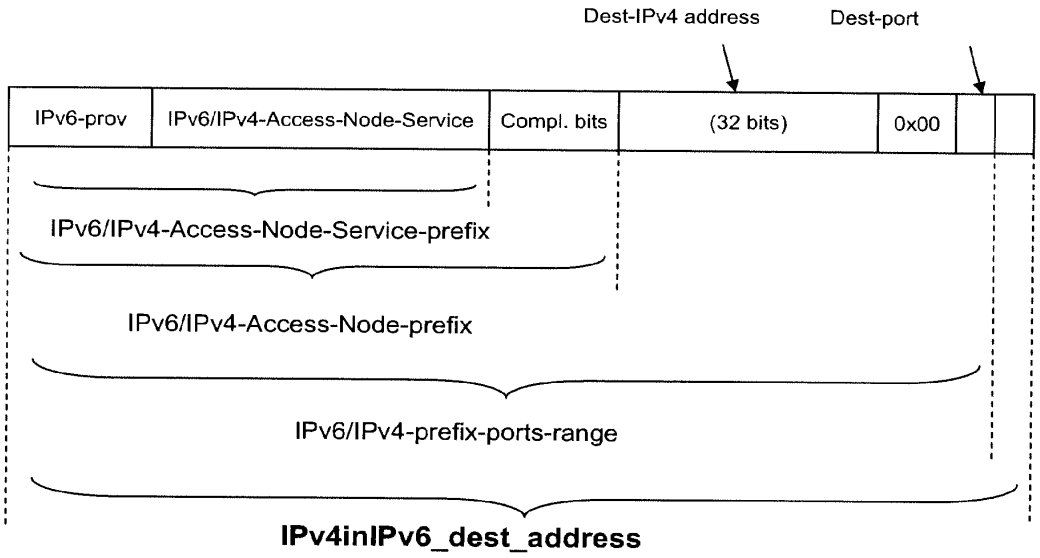

Dest-IPv4 address
Dest-port
IPv6-prov
IPv6/IPv4-Access-Node-Service
Compl. bits
(32 bits)
0x00
IPv6/IPv4-Access-Node-Service-prefix
IPv6/IPv4-Access-Node-prefix
IPv6/IPv4-prefix-ports-range
IPv4inIPv6_dest_address

FIG. 7

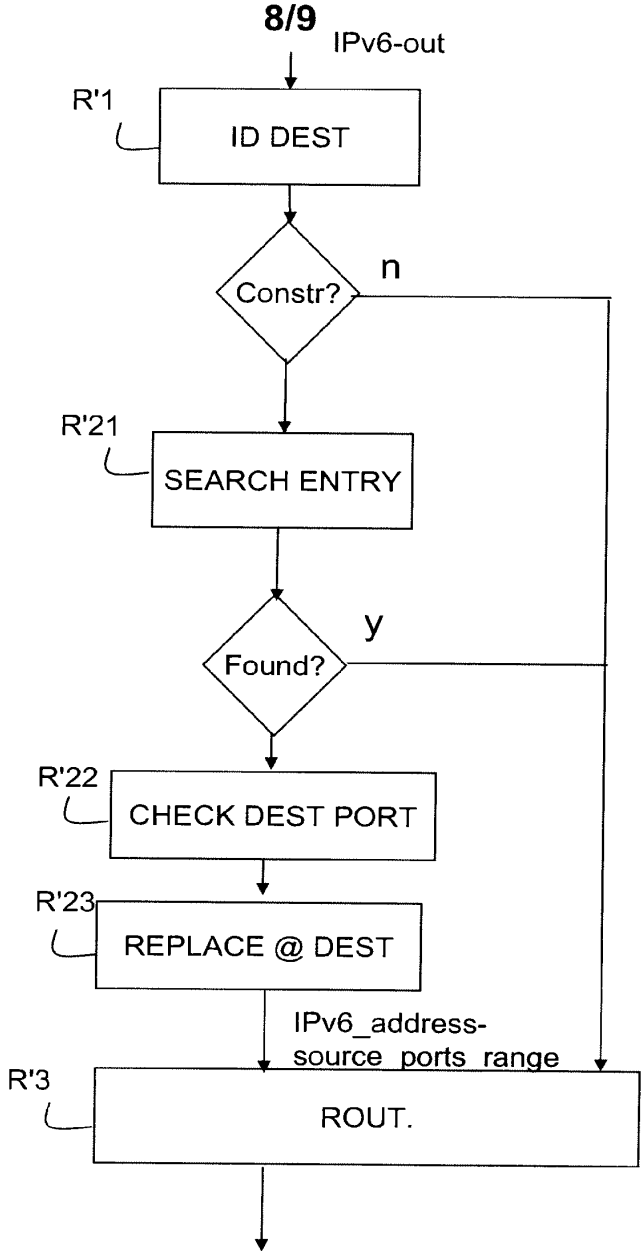

IPv6-out
R'1
ID DEST
Constr?
n
R'21
SEARCH ENTRY
Found?
y
R'22
CHECK DEST PORT
R'23
REPLACE @ DEST
IPv6_address-
source_ports_range
R'3
ROUT.

FIG. 8

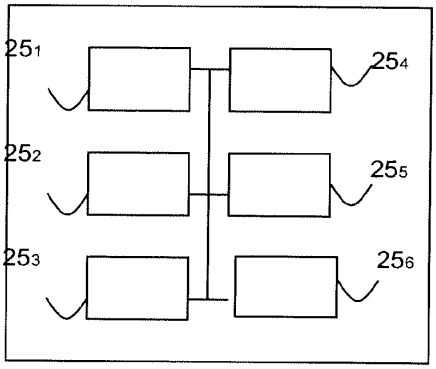


FIG. 9

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/051228

A. CLASSIFICATION OF SUBJECT MATTER
INV. 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)
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, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	MYUNG-KI SHIN ET AL: "Ports option support in dual stack transition mechanism (DSTM)" ADVANCED COMMUNICATION TECHNOLOGY, 2004. THE 6TH INTERNATIONAL CONFERE NCE ON PHOENIX PARK, KOREA FEB. 9-11, 2004, PISCATAWAY, NJ, USA,IEEE, vol. 1, 9 February 2004 (2004-02-09), pages 225-228, XP010701165 ISBN: 978-89-5519-119-6 abstract * partie I* * partie III * * partie IV.B * ----- -/--	1-10

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

[X] 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 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
13 novembre 2009	20/11/2009

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Poppe, Fabrice

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/051228

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2004/039014 A (CISCO TECH IND [US]) 6 May 2004 (2004-05-06) abstract page 5, line 9 - line 17 page 9, line 6 - page 10, line 2; figure 4 page 10, line 3 - page 12, line 3; figure 5 page 13, line 5 - page 14, line 9	1-10
X	DANIEL PARK ET AL: "Network Address Translation - Protocol Translation (NAT-PT); draft-daniel-natpt-bis-01.txt" INTERNET ENGINEERING TASK FORCE, IETF, 22 October 2005 (2005-10-22), XP015042124 abstract paragraph [0002] paragraph [0005]	1-10
A	SRISURESH P ET AL: "RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations" INTERNET CITATION, [Online] XP002204216 Retrieved from the Internet: URL:http://www.ietf.org/rfc/rfc2663.txt> [retrieved on 2002-07-01] the whole document	1-10
A	EP 1 420 559 A (THOMSON LICENSING SA [FR]) 19 May 2004 (2004-05-19) abstract paragraph [0002] - paragraph [0009] paragraph [0030] - paragraph [0034]; figure 4	1-10
A	AFIFI H ET AL: "Methods for IPv4-IPv6 transition" COMPUTERS AND COMMUNICATIONS, 1999. PROCEEDINGS. IEEE INTERNATIONAL SY MPOSIUM ON RED SEA, EGYPT 6-8 JULY 1999, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 6 July 1999 (1999-07-06), pages 478-484, XP010555073 ISBN: 978-0-7695-0250-2 abstract paragraph [0003]	1-10
A	WO 2007/099248 A (FRANCE TELECOM [FR]; BOUCADAIR MOHAMED [FR]; NOISETTE YOANN [FR]) 7 September 2007 (2007-09-07) the whole document	1-10
A	WO 2008/001007 A (FRANCE TELECOM [FR]; BOUCADAIR MOHAMED [FR]; NOISETTE YOANN [FR]) 3 January 2008 (2008-01-03) the whole document	1-10

-/--

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2009/051228

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KAWARASAKI Y ET AL: "IPv4/IPv6 SIP interworking methods in dual-stack network" COMMUNICATIONS, 2003. APCC 2003. THE 9TH ASIA-PACIFIC CONFERENCE ON 21-24 SEPT. 2003, PISCATAWAY, NJ, USA,IEEE, vol. 3, 21 September 2003 (2003-09-21), pages 1124-1128, XP010687978 ISBN: 978-0-7803-8114-8 the whole document	1-10

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2009/051228

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2004039014 A	06-05-2004	AT 352148 T	15-02-2007
		AU 2003282934 A1	13-05-2004
		CA 2502945 A1	06-05-2004
		CN 1706155 A	07-12-2005
		DE 60311297 T2	15-11-2007
		EP 1554841 A1	20-07-2005
		US 2004076180 A1	22-04-2004
EP 1420559 A	19-05-2004	AU 2003289873 A1	03-06-2004
		BR 0316112 A	27-09-2005
		CN 1711739 A	21-12-2005
		WO 2004045183 A1	27-05-2004
		JP 4339259 B2	07-10-2009
		JP 2006506839 T	23-02-2006
		KR 20050074998 A	19-07-2005
		MX PA05004998 A	02-08-2005
		US 2006259639 A1	16-11-2006
WO 2007099248 A	07-09-2007	CN 101395891 A	25-03-2009
		EP 1994724 A2	26-11-2008
		FR 2898003 A1	31-08-2007
		JP 2009528742 T	06-08-2009
		US 2009041034 A1	12-02-2009
WO 2008001007 A	03-01-2008	EP 2036301 A2	18-03-2009
		FR 2903263 A1	04-01-2008
		US 2009187664 A1	23-07-2009

Form PCT/ISA/210 (patent family annex) (April 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/051228

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/12

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ, IBM-TDB

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	MYUNG-KI SHIN ET AL: "Ports option support in dual stack transition mechanism (DSTM)" ADVANCED COMMUNICATION TECHNOLOGY, 2004. THE 6TH INTERNATIONAL CONFERE NCE ON PHOENIX PARK, KOREA FEB. 9-11, 2004, PISCATAWAY, NJ, USA,IEEE, vol. 1, 9 février 2004 (2004-02-09), pages 225-228, XP010701165 ISBN: 978-89-5519-119-6 abrégé * partie I* * partie III * * partie IV.B *	1-10

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
13 novembre 2009	20/11/2009

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Poppe, Fabrice

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

CI

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/051228

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	WO 2004/039014 A (CISCO TECH IND [US]) 6 mai 2004 (2004-05-06) abrégé page 5, ligne 9 - ligne 17 page 9, ligne 6 - page 10, ligne 2; figure 4 page 10, ligne 3 - page 12, ligne 3; figure 5 page 13, ligne 5 - page 14, ligne 9	1-10
X	DANIEL PARK ET AL: "Network Address Translation - Protocol Translation (NAT-PT); draft-daniel-natpt-bis-01.txt" INTERNET ENGINEERING TASK FORCE, IETF, 22 octobre 2005 (2005-10-22), XP015042124 abrégé alinéa [0002] alinéa [0005]	1-10
A	SRISURESH P ET AL: "RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations" INTERNET CITATION, [Online] XP002204216 Extrait de l'Internet: URL:http://www.ietf.org/rfc/rfc2663.txt> [extrait le 2002-07-01] le document en entier	1-10
A	EP 1 420 559 A (THOMSON LICENSING SA [FR]) 19 mai 2004 (2004-05-19) abrégé alinéa [0002] - alinéa [0009] alinéa [0030] - alinéa [0034]; figure 4	1-10
A	AFIFI H ET AL: "Methods for IPv4-IPv6 transition" COMPUTERS AND COMMUNICATIONS, 1999. PROCEEDINGS. IEEE INTERNATIONAL SY MPOSIUM ON RED SEA, EGYPT 6-8 JULY 1999, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 6 juillet 1999 (1999-07-06), pages 478-484, XP010555073 ISBN: 978-0-7695-0250-2 abrégé alinéa [0003]	1-10
A	WO 2007/099248 A (FRANCE TELECOM [FR]; BOUCADAIR MOHAMED [FR]; NOISETTE YOANN [FR]) 7 septembre 2007 (2007-09-07) le document en entier	1-10
A	WO 2008/001007 A (FRANCE TELECOM [FR]; BOUCADAIR MOHAMED [FR]; NOISETTE YOANN [FR]) 3 janvier 2008 (2008-01-03) le document en entier	1-10

-/--

CI

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2009/051228

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	KAWARASAKI Y ET AL: "IPv4/IPv6 SIP interworking methods in dual-stack network" COMMUNICATIONS, 2003. APCC 2003. THE 9TH ASIA-PACIFIC CONFERENCE ON 21-24 SEPT. 2003, PISCATAWAY, NJ, USA,IEEE, vol. 3, 21 septembre 2003 (2003-09-21), pages 1124-1128, XP010687978 ISBN: 978-0-7803-8114-8 le document en entier	1-10

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2009/051228

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 2004039014	A	06-05-2004	AT	352148 T	15-02-2007
			AU	2003282934 A1	13-05-2004
			CA	2502945 A1	06-05-2004
			CN	1706155 A	07-12-2005
			DE	60311297 T2	15-11-2007
			EP	1554841 A1	20-07-2005
			US	2004076180 A1	22-04-2004
EP 1420559	A	19-05-2004	AU	2003289873 A1	03-06-2004
			BR	0316112 A	27-09-2005
			CN	1711739 A	21-12-2005
			WO	2004045183 A1	27-05-2004
			JP	4339259 B2	07-10-2009
			JP	2006506839 T	23-02-2006
			KR	20050074998 A	19-07-2005
			MX	PA05004998 A	02-08-2005
			US	2006259639 A1	16-11-2006
WO 2007099248	A	07-09-2007	CN	101395891 A	25-03-2009
			EP	1994724 A2	26-11-2008
			FR	2898003 A1	31-08-2007
			JP	2009528742 T	06-08-2009
			US	2009041034 A1	12-02-2009
WO 2008001007	A	03-01-2008	EP	2036301 A2	18-03-2009
			FR	2903263 A1	04-01-2008
			US	2009187664 A1	23-07-2009

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/FR2009/051228

International filing date: 26 June 2009 (26.06.2009)

Document type: Certified copy of priority document

Document details: Country/Office: FR
Number: 0854405
Filing date: 30 June 2008 (30.06.2008)

Date of receipt at the International Bureau: 23 October 2009 (23.10.2009)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

RÉPUBLIQUE FRANÇAISE

PCT/FR 2009 / 051228

INSTITUT NATIONAL
DE LA PROPRIÉTÉ
INDUSTRIELLE

d'invention

Certificat d'utilité

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 06 OCT. 2009

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DB 267/02/07



INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITE

cerfa N°12236*01

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Téléphone: 0820 213 213 Télécopie: 01.53.04.52.65

Code de la propriété intellectuelle-livreVI

REQUÊTE EN DÉLIVRANCE

DATE DE REMISE DES PIÈCES: **30/06/2008** N° D'ENREGISTREMENT NATIONAL: **0854405** DÉPARTEMENT DE DÉPÔT: DATE DE DÉPÔT:	FRANCE TELECOM BENETIERE Marion FRANCE TELECOM/R&D/PIV/BREVETS 38-40, rue du Général Leclerc 92794 ISSY MOULINEAUX CEDEX 9 France
Vos références pour ce dossier: 07049	

1 NATURE DE LA DEMANDE	
Demande de brevet	
2 TITRE DE L'INVENTION	
	PROCEDE DE RECEPTION D'UN PAQUET DE DONNEES DANS UN DOMAINE IPv6, DISPOSITIF ET PASSERELLE RESIDENTIELLE ASSOCIES
3 DECLARATION DE PRIORITE OU REQUETE DU BENEFICE DE LA DATE DE DEPOT D'UNE DEMANDE ANTERIEURE FRANCAISE	Pays ou organisation Date N°
4-1 DEMANDEUR	
Nom	FRANCE TELECOM
Suivi par	BENETIERE Marion
Rue	6, place d'Alleray
Code postal et ville	75015 PARIS
Pays	France
Nationalité	France
Forme juridique	Société anonyme
N° SIREN	380 129 866
Code APE-NAF	642A
N° de téléphone	02 99 12 47 27
N° de télécopie	01 45 29 65 60
Courrier électronique	marion.benetiere@orange-ftgroup.com
5C ADRESSE DE CORRESPONDANCE	
Nom	FRANCE TELECOM
Rue	FRANCE TELECOM/R&D/PIV/BREVETS 38-40, rue du Général Leclerc
Code postal et ville	92794 ISSY MOULINEAUX CEDEX 9
Pays	France

CI

6 DOCUMENTS ET FICHIERS JOINTS	Fichier électronique	Pages	Détails
Texte du brevet	textebrevet.pdf	36	D 32, R 3, AB 1
Dessins	dessins.pdf	9	page 9, figures 09, Abrégé: page 3, Fig.3
Désignation d'inventeurs	Design.PDF		
COPIE DU POUVOIR GENERAL	other1.pdf		
7 MODE DE PAIEMENT			
Mode de paiement	Prélèvement du compte courant		
Numéro du compte client	432		
8 RAPPORT DE RECHERCHE			
Etablissement immédiat			

9 REDEVANCES JOINTES	Devise	Taux	Quantité	Montant à payer
062 Dépôt d'une demande électronique	EURO	26.00	1.00	26.00
063 Rapport de recherche	EURO	500.00	1.00	500.00
Total à acquitter	EURO			526.00

La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Signé par
Signataire: FR, FRANCE TELECOM RD, Myriam PLAT
Emetteur du certificat: FR, INPI, INPI-EN-LIGNE 1.0
Fonction
(Demandeur)

1er dépôt

R E P U B L I Q U E F R A N C A I S E

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITE

Réception électronique de la soumission

Il est certifié par la présente qu'une demande de brevet (ou d'un certificat d'utilité) a été reçue par le biais du dépôt électronique sécurisé de l'INPI. Après réception, un numéro d'enregistrement et une date de réception ont été automatiquement attribués.

Numéro de demande	0854405	
Numéro de soumission	1000032979	
Date de réception	30 juin 2008	
Vos références	07049	
Demandeur	FRANCE TELECOM	
Pays	FR	
Titre de l'invention	PROCEDE DE RECEPTION D'UN PAQUET DE DONNEES DANS UN DOMAINE IPv6, DISPOSITIF ET PASSERELLE RESIDENTIELLE ASSOCIES	
Documents envoyés	package-data.xml	FR-office-specific-info.xml
	request.xml	fee-sheet.xml
	application-body.xml	indication-bio-deposit.xml
	textebrevet.pdf (36 p.)	dessins.pdf (9 p.)
	Design.PDF (1 p.)	other1.pdf (1 p.)
	Requetefr.PDF (2 p.)	ValidLog.PDF (1 p.)
Déposé par	CN=Myriam PLAT,O=FRANCE TELECOM RD,C=FR	
Méthode de dépôt	Dépôt électronique	
Date et heure de réception électronique	30 juin 2008, 17:18:22 (CEST)	
Empreinte officielle du dépôt	56:F8:D8:0C:E6:41:F5:7C:D9:E2:3B:D5:1E:2F:2A:75:F9:C4:1C:D6	

/INPI, section dépôt/

Procédé de réception d'un paquet de données dans un domaine IPv6, dispositif et passerelle résidentielle associés

Domaine de l'invention

Le domaine de l'invention est celui d'un réseau de télécommunications, en particulier un réseau de télécommunications IP dans lequel sont transportés des paquets de données d'un équipement source identifié par une adresse source vers un équipement de destination identifié par une adresse de destination.

Un tel réseau de télécommunications regroupe une pluralité d'équipements, de liens et de fonctions dédiés au transport des données issues d'équipements terminaux connectés à ce réseau. En particulier, les fonctions de transport peuvent être implémentées grâce à l'activation de protocoles de routage et de transmission. Un réseau de télécommunications administré par un opérateur est encore appelé un domaine.

Un fournisseur de service de connectivité IP déploie une architecture dédiée pour permettre aux utilisateurs d'équipements terminaux d'être joignables. L'accès au service de connectivité IP est géré par le fournisseur de service qui s'appuie sur le réseau de télécommunications d'un opérateur pour router les paquets de données émis par les équipements terminaux vers leurs destinations finales. Dans certains cas, ledit fournisseur de service est aussi l'opérateur de réseau de télécommunications.

Un tel fournisseur de service affecte une adresse IP, généralement cette adresse est publique, à une passerelle résidentielle entre un réseau résidentiel et le réseau public ou domaine IP de l'opérateur. La passerelle résidentielle affecte généralement aux terminaux de son réseau résidentiel des adresses IP privées.

Dans la suite, on désignera par « passerelle résidentielle » tout équipement d'interconnexion entre un réseau privé et un réseau opéré par un fournisseur de service, le réseau privé pouvant aussi bien être un réseau résidentiel qu'un réseau d'entreprise.

Dans la suite, le réseau opéré par les fournisseurs de service sera aussi désigné par le terme "réseau public".

Procédé de réception d'un paquet de données dans un domaine IPv6, dispositif et passerelle résidentielle associés

Domaine de l'invention

Le domaine de l'invention est celui d'un réseau de télécommunications, en particulier un réseau de télécommunications IP dans lequel sont transportés des paquets de données d'un équipement source identifié par une adresse source vers un équipement de destination identifié par une adresse de destination.

Un tel réseau de télécommunications regroupe une pluralité d'équipements, de liens et de fonctions dédiés au transport des données issues d'équipements terminaux connectés à ce réseau. En particulier, les fonctions de transport peuvent être implémentées grâce à l'activation de protocoles de routage et de transmission. Un réseau de télécommunications administré par un opérateur est encore appelé un domaine.

Un fournisseur de service de connectivité IP déploie une architecture dédiée

Procédé de réception d'un paquet de données dans un domaine IPv6, dispositif et passerelle résidentielle associés

Domaine de l'invention

Le domaine de l'invention est celui d'un réseau de télécommunications, en particulier un réseau de télécommunications IP dans lequel sont transportés des paquets de données d'un équipement source identifié par une adresse source vers un équipement de destination identifié par une adresse de destination.

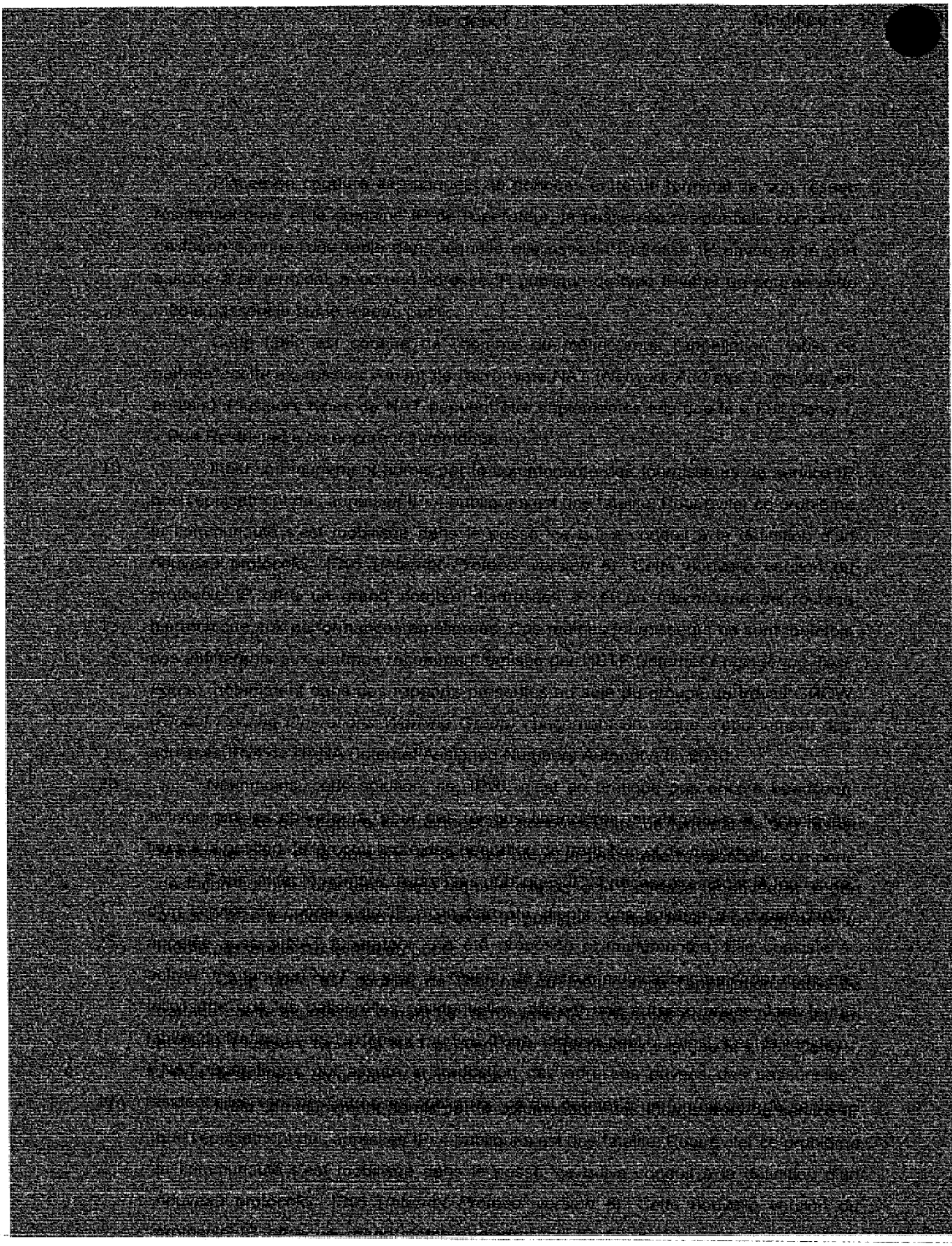
Un tel réseau de télécommunications regroupe une pluralité d'équipements, de liens et de fonctions dédiés au transport des données issues d'équipements terminaux connectés à ce réseau. En particulier, les fonctions de transport peuvent être implémentées grâce à l'activation de protocoles de routage et de transmission. Un réseau de télécommunications administré par un opérateur est encore appelé un domaine.

Un fournisseur de service de connectivité IP déploie une architecture dédiée pour permettre aux utilisateurs d'équipements terminaux d'être joignables. L'accès au service de connectivité IP est géré par le fournisseur de service qui s'appuie sur le réseau de télécommunications d'un opérateur pour router les paquets de données émis par les équipements terminaux vers leurs destinations finales. Dans certains cas, ledit fournisseur de service est aussi l'opérateur de réseau de télécommunications.

Un tel fournisseur de service affecte une adresse IP, généralement cette adresse est publique à une passerelle résidentielle entre un réseau résidentiel et le réseau public ou domaine IP de l'opérateur. La passerelle résidentielle affecte généralement aux terminaux de son réseau résidentiel des adresses IP privées.

Dans la suite, on désignera par « passerelle résidentielle » tout équipement d'interconnexion entre un réseau privé et un réseau opéré par un fournisseur de service, le réseau privé pouvant aussi bien être un réseau résidentiel qu'un réseau d'entreprise.

Dans la suite, le réseau opéré par les fournisseurs de service sera aussi désigné par le terme "réseau public".



CI

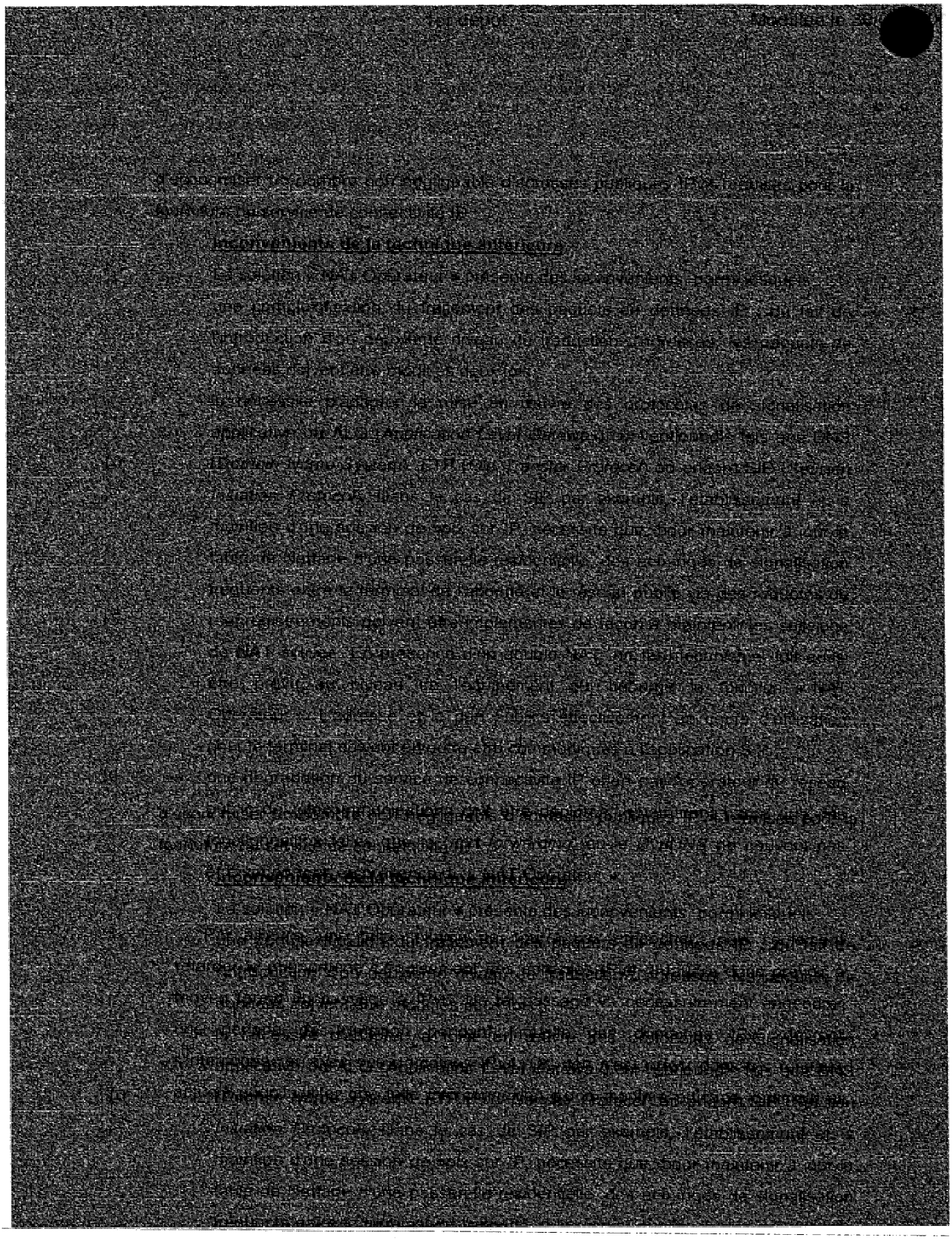
Placée en coupure des paquets de données entre un terminal de son réseau résidentiel privé et le domaine IP de l'opérateur, la passerelle résidentielle comporte, de façon connue, une table dans laquelle elle associe l'adresse IP privée et le port associé à ce terminal, avec une adresse IP publique de type IPv4 et un port de cette même passerelle sur le réseau public.

Cette table est connue de l'homme du métier sous l'appellation "table de nattage", cette expression venant de l'acronyme NAT (*Network Address Translator* en anglais). Plusieurs types de NAT peuvent être implémentés tels que le « Full Cone », « Port Restricted » ou encore « symétrique ».

Il est communément admis par la communauté des fournisseurs de service IP que l'épuisement des adresses IPv4 publiques est une fatalité. Pour éviter ce problème, la communauté s'est mobilisée dans le passé, ce qui a conduit à la définition d'un nouveau protocole : IPv6 (*Internet Protocol version 6*). Cette nouvelle version du protocole IP offre un grand nombre d'adresses IP et un mécanisme de routage hiérarchique aux performances améliorées. Ces mêmes fournisseurs ne sont toutefois pas indifférents aux alarmes récemment émises par l'IETF (*Internet Engineering Task Force*), notamment dans des rapports présentés au sein du groupe de travail GROW (*Global Routing Operations Working Group)* concernant un risque d'épuisement des adresses IPv4 de l'IANA (Internet Assigned Numbers Authority) fin 2010.

Néanmoins, cette solution, i.e. IPv6, n'est en pratique pas encore beaucoup activée par les opérateurs, pour des raisons financières, stratégiques et techniques liées à la gestion de la complexité des opération de transition et de migration.

Pour limiter le nombre d'adresses publiques IPv4 nécessaires pour la fourniture d'un service de connectivité IP à un parc de clients, une solution de double NAT, appelée aussi « NAT Opérateur », a été proposée et implémentée. Elle consiste à activer une fonction NAT au sein du réseau de télécommunications de l'opérateur, de telle sorte que les passerelles résidentielles utilisent une adresse privée dans leurs tables de Nattage vers l'extérieur (au lieu d'une adresse public). Ainsi, c'est la fonction « NAT Opérateur » qui assure la traduction des adresses privées des passerelles résidentielles vers des adresses publiques, ce qui permet à un fournisseur de service



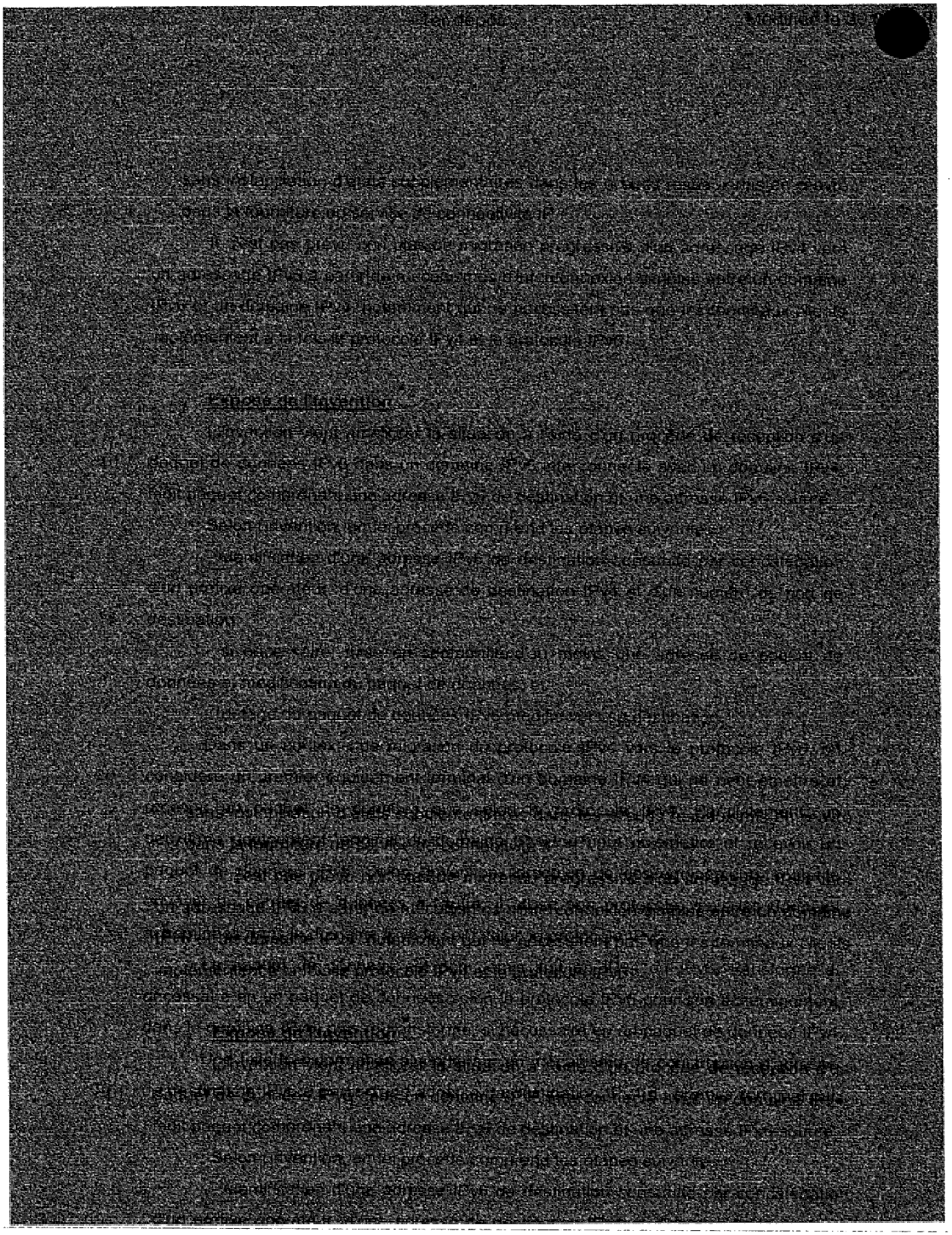
d'économiser un nombre non négligeable d'adresses publiques IPv4 requises pour la fourniture du service de connectivité IP.

Inconvénients de la technique antérieure

La solution « NAT Opérateur » présente des inconvénients, parmi lesquels :

- une complexification du traitement des paquets de données IP : du fait de l'introduction d'un deuxième niveau de traduction d'adresses, les paquets de données doivent être modifiés deux fois ;
- la nécessité d'adapter la mise en œuvre des protocoles de signalisation applicative ou ALG (*Application Level Gateway*) conventionnels tels que DNS (*Domain Name System*), FTP (*File Transfer Protocol*) ou encore SIP (*Session Initiation Protocol*). Dans le cas de SIP par exemple, l'établissement et le maintien d'une session de voix sur IP, nécessite que, pour maintenir à jour la table de Nattage d'une passerelle résidentielle, des échanges de signalisation fréquents entre le terminal de l'abonné et le réseau public via des requêtes de réenregistrements doivent être implémentés de façon à maintenir les sessions de NAT actives. En présence d'un double NAT, un tel mécanisme doit aussi être prévu au niveau de l'équipement qui héberge la fonction « NAT Opérateur ». L'adresse et le port publics effectivement en cours d'utilisation pour le terminal doivent en outre être communiqués à l'application SIP ;
- une dégradation du service de connectivité IP offert par l'opérateur du réseau public de télécommunications doit être déplorée, notamment parce que des fonctionnalités telles que le "*port forwarding*" ou le *DynDNS* ne peuvent pas être supportées en présence du « NAT Opérateur ».

Par ailleurs, une telle solution ne pourra pas empêcher, mais seulement retarder le phénomène d'épuisement des adresses IPv4. Il faudra donc prévoir à moyen terme un passage à IPv6. Un tel passage va nécessairement engendrer une période de transition pendant laquelle des domaines IPv6 devront s'interconnecter avec des domaines IPv4. Or, rien n'est prévu dans les réseaux actuels pour faciliter une telle interconnexion d'une manière efficace, optimale et



sans instanciation d'états supplémentaires dans les nœuds réseaux mis en œuvre dans la fourniture du service de connectivité IP.

Il n'est pas prévu non plus de migration progressive d'un adressage IPv4 vers un adressage IPv6 à partir de mécanismes d'interconnexion simples entre un domaine IPv6 et un domaine IPv4, notamment qui ne nécessitent pas que les terminaux clients implémentent à la fois le protocole IPv4 et le protocole IPv6.

Exposé de l'invention

L'invention vient améliorer la situation à l'aide d'un procédé de réception d'un paquet de données IPv6 dans un domaine IPv6 interconnecté avec un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source.

Selon l'invention, un tel procédé comprend les étapes suivantes :

- identification d'une adresse IPv6 de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;

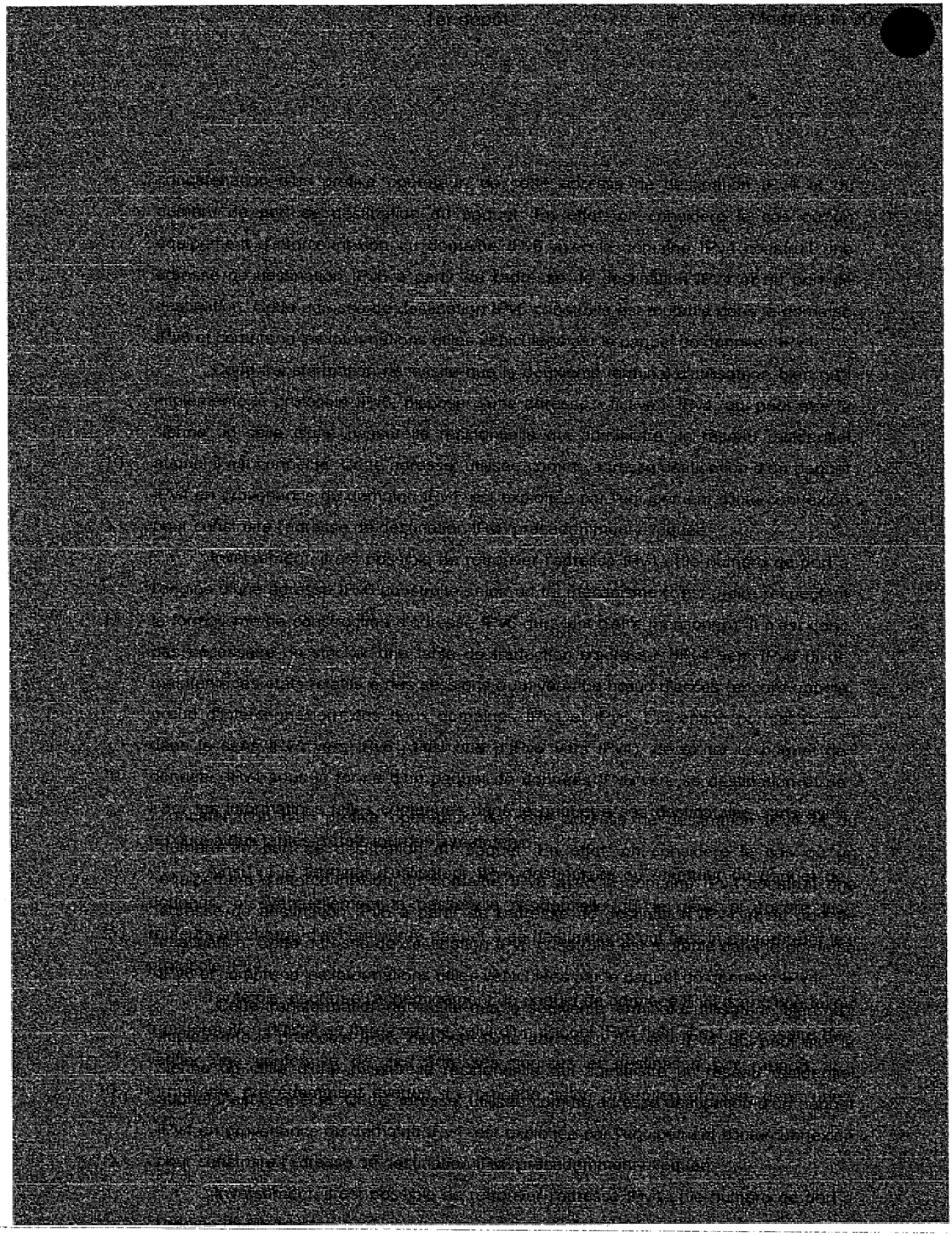
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données et modification du paquet de données; et

- routage du paquet de données IPv6 modifié vers sa destination.

Dans un contexte de migration du protocole IPv4 vers le protocole IPv6, on considère un premier équipement terminal d'un domaine IPv4 qui ne peut émettre et recevoir un paquet de données que selon le protocole IPv4. Parallèlement, un deuxième équipement terminal du domaine IPv6 ne peut qu'émettre et recevoir un paquet de données IPv6. Selon l'invention, lorsqu'un de ces équipements souhaite envoyer un paquet de données à l'autre, il utilise son protocole, mais les données acheminées dans le domaine IPv6 le sont selon le protocole IPv6.

Le paquet de données est donc émis soit en IPv4 ou IPv6, transformé si nécessaire en un paquet de données selon le protocole IPv6 pour son acheminement dans le domaine IPv6, puis re-transformé, si nécessaire en un paquet de données IPv4.

Une telle transformation s'appuie sur un mécanisme de construction d'adresse de destination IPv6 à partir d'une adresse de destination IPv4 du premier terminal par



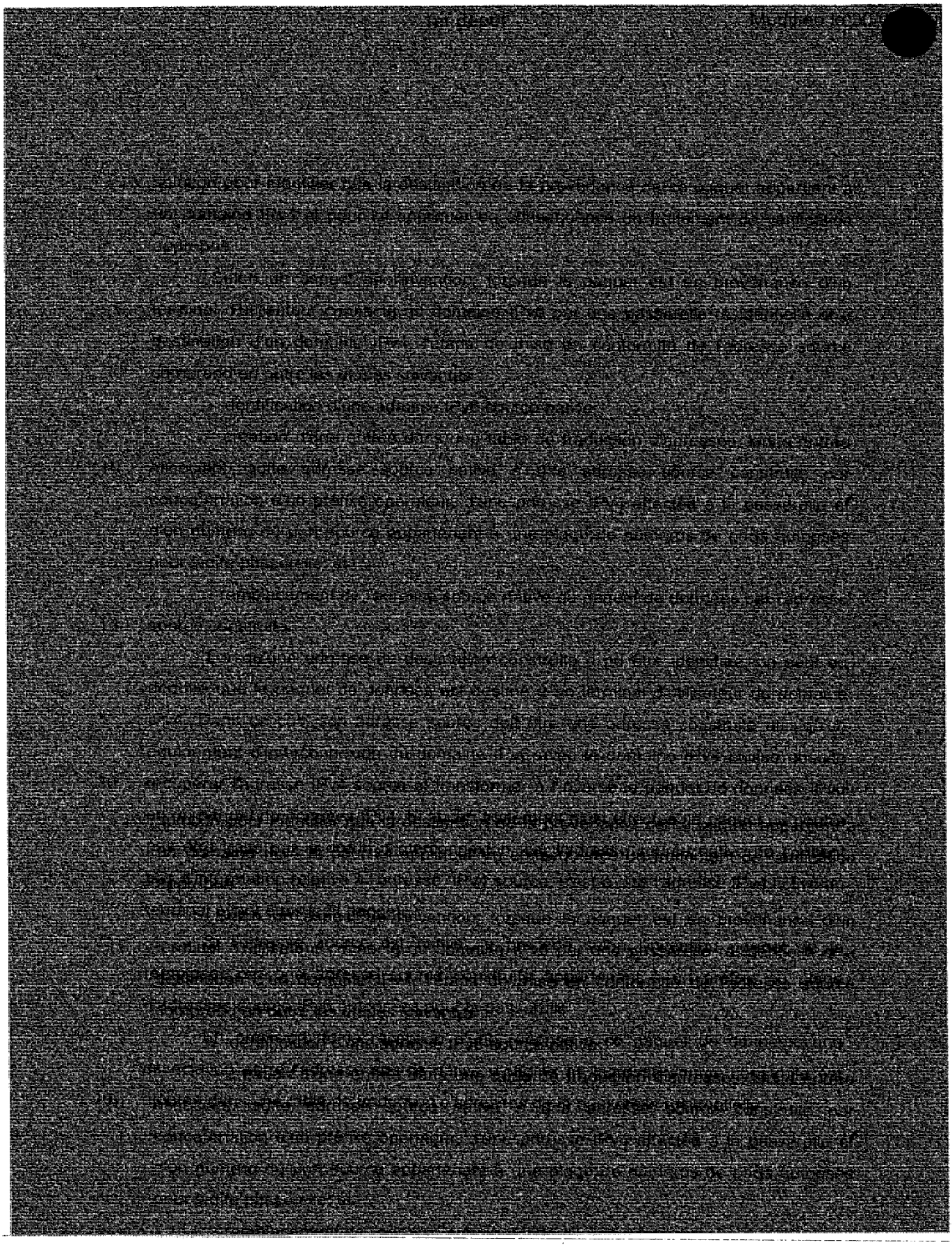
concaténation d'un préfixe opérateur, de cette adresse de destination IPv4 et du numéro de port de destination du paquet. En effet, on considère le cas où un équipement d'interconnexion du domaine IPv6 avec le domaine IPv4 construit une adresse de destination IPv6 à partir de l'adresse de destination IPv4 et du port de destination. Cette adresse de destination IPv6 construite est routable dans le domaine IPv6 et comprend les informations utiles véhiculées par le paquet de données IPv4.

Cette transformation nécessite que le deuxième terminal d'utilisateur, bien qu'il implémente le protocole IPv6, dispose d'une adresse « fictive » IPv4, qui peut être la sienne ou celle d'une passerelle résidentielle qui administre un réseau résidentiel auquel il est connecté. Cette adresse, utilisée comme adresse destination d'un paquet IPv4 en provenance du domaine IPv4, est exploitée par l'équipement d'interconnexion pour construire l'adresse de destination IPv6 précédemment évoquée.

Inversement, il est possible de retrouver l'adresse IPv4 et le numéro de port à l'origine d'une adresse IPv6 construite selon un tel mécanisme (c'est-à-dire respectant le formalisme de construction d'adresse IPv6 qui vient d'être mentionné). Il n'est donc pas nécessaire de stocker une table de traduction d'adresses IPv4 vers IPv6 ni de maintenir des états relatifs à des sessions au niveau du nœud d'accès (encore appelé nœud d'interconnexion) des deux domaines IPv4 et IPv6. L'invention permet donc, dans le sens IPv4 vers IPv6 (ainsi que d'IPv6 vers IPv4), de router le paquet de données IPv4 sous la forme d'un paquet de données IPv6 vers sa destination et de livrer les informations utiles contenues dans le paquet à son destinataire, sans avoir recours à des tables d'états lourdes à maintenir.

Ainsi, ni le terminal d'utilisateur IPv6 destinataire ou émetteur du paquet de données, ni éventuellement la passerelle résidentielle qui le gère, ni encore les routeurs en charge d'acheminer le paquet à sa destination n'ont besoin d'interpréter le protocole IPv4.

Toutefois, pour que l'acheminement du paquet de données IPv6 issu d'une telle transformation puisse se faire comme celui d'un paquet IPv6 natif, il est nécessaire de vérifier une conformité de ses adresses sources et destination par rapport au formalisme précédemment évoqué. Le procédé selon l'invention propose donc une



solution pour identifier que la destination ou la provenance de ce paquet appartient à un domaine IPv4 et pour lui appliquer en conséquence un traitement de vérification approprié.

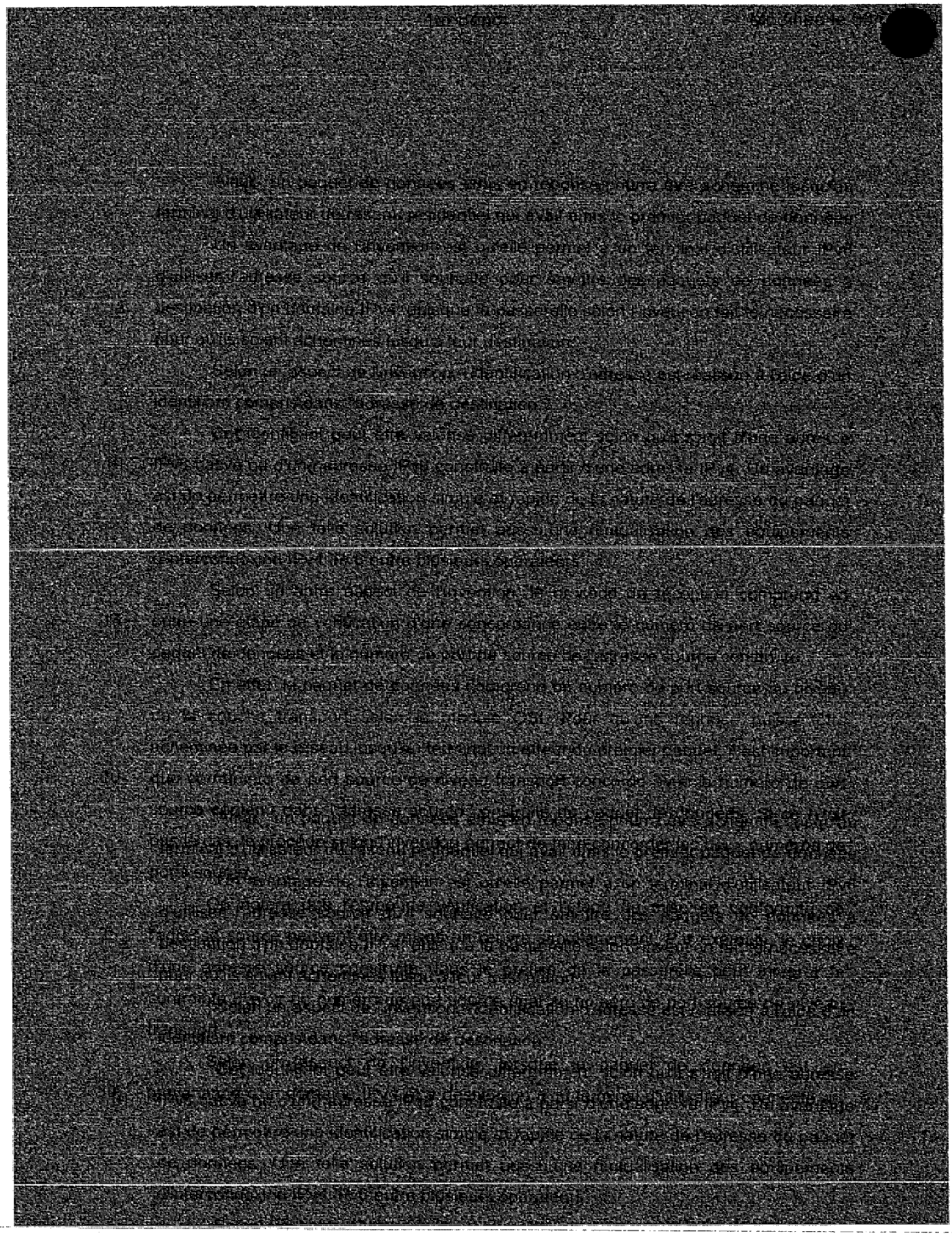
Selon un aspect de l'invention, lorsque le paquet est en provenance d'un terminal d'utilisateur connecté au domaine IPv6 par une passerelle résidentielle et à destination d'un domaine IPv4, l'étape de mise en conformité de l'adresse source comprend en outre les étapes suivantes :

- identification d'une adresse IPv6 source native;
- création d'une entrée dans une table de traduction d'adresses, ladite entrée associant ladite adresse source native à une adresse source construite par concaténation d'un préfixe opérateur, d'une adresse IPv4 affectée à la passerelle et d'un numéro de port source appartenant à une plage de numéros de ports autorisés pour ladite passerelle; et
- remplacement de l'adresse source native du paquet de données par l'adresse source construite.

Lorsqu'une adresse de destination construite a pu être identifiée, on peut en déduire que le paquet de données est destiné à un terminal d'utilisateur du domaine IPv4. Dans ce cas, son adresse source doit être une adresse construite afin qu'un équipement d'interconnexion du domaine IPv6 avec le domaine IPv4 puisse ensuite récupérer l'adresse IPv4 source et transformer à l'inverse le paquet de données IPv6 en un paquet de données IPv4. Si aucun traitement n'est effectué, le paquet ne pourra pas être traité par le nœud d'interconnexion; car l'adresse source native ne contient pas d'information relative à l'adresse IPv4 source, c'est-à-dire l'adresse IPv4 fictive du terminal ayant émis ledit paquet.

Si l'adresse source est native, le procédé selon l'invention permet de la remplacer par une adresse source construite appartenant à un préfixe ou plage d'adresses source IPv6 autorisées pour la passerelle.

En prévision de la réception d'une réponse à ce paquet de données, une association entre l'adresse source native d'origine et l'adresse source construite est ajoutée dans une table de traduction d'adresses de la passerelle résidentielle.



Ainsi, un paquet de données émis en réponse pourra être acheminé jusqu'au terminal d'utilisateur du réseau résidentiel qui avait émis le premier paquet de données.

Un avantage de l'invention est qu'elle permet à un terminal d'utilisateur IPv6 d'utiliser l'adresse source qu'il souhaite pour émettre des paquets de données à destination d'un domaine IPv4, puisque la passerelle selon l'invention fait le nécessaire pour qu'ils soient acheminés jusqu'à leur destination.

Selon un aspect de l'invention, l'identification d'adresse est réalisée à l'aide d'un identifiant compris dans l'adresse de destination.

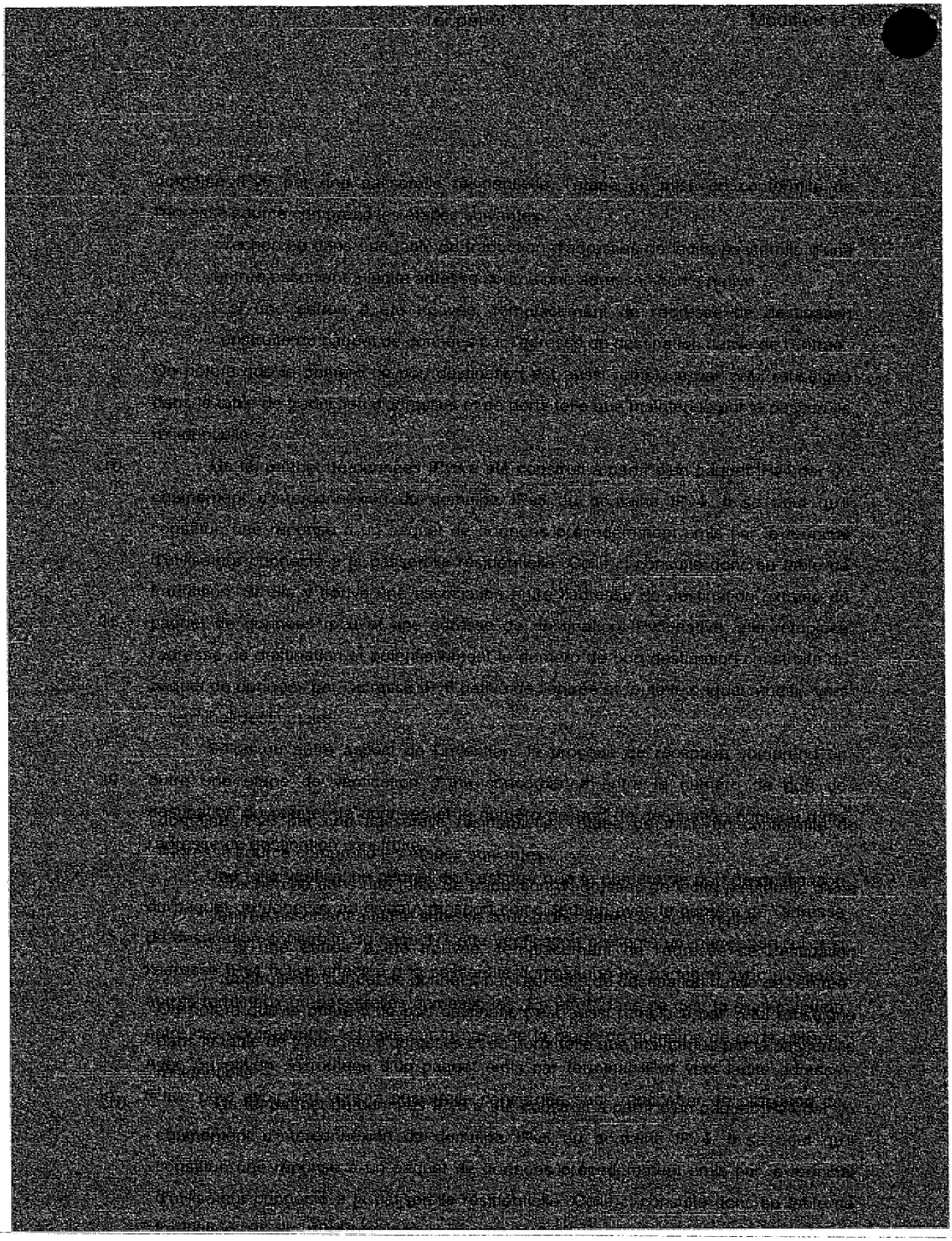
Cet identifiant peut être valorisé différemment selon qu'il s'agit d'une adresse IPv6 native ou d'une adresse IPv6 construite à partir d'une adresse IPv4. Un avantage est de permettre une identification simple et rapide de la nature de l'adresse du paquet de données. Une telle solution permet aussi une mutualisation des équipements d'interconnexion IPv4 IPv6 entre plusieurs opérateurs.

Selon un autre aspect de l'invention, le procédé de réception comprend en outre une étape de vérification d'une concordance entre le numéro de port source du paquet de données et le numéro de port de source de l'adresse source construite.

En effet, le paquet de données comprend un numéro de port source au niveau de la couche transport selon le modèle OSI. Pour qu'une réponse puisse être acheminée par le réseau jusqu'au terminal émetteur du premier paquet, il est important que ce numéro de port source de niveau transport concorde avec le numéro de port source contenu dans l'adresse source construite du paquet de données. Si ce n'est pas le cas, le procédé selon l'invention permet de faire concorder les deux numéros de ports source.

On notera que l'étape de vérification et l'étape de mise en conformité de l'adresse source peuvent être mises en œuvre simultanément. Par exemple, le choix d'une adresse source construite dans le préfixe de la passerelle peut intégrer la contrainte d'avoir un numéro de port source égal au numéro de port source de niveau transport.

Selon un aspect de l'invention, lorsque le paquet de données est en provenance d'un domaine IPv4 et à destination d'un terminal d'utilisateur connecté au



domaine IPv6 par une passerelle résidentielle, l'étape de mise en conformité de l'adresse source comprend les étapes suivantes :

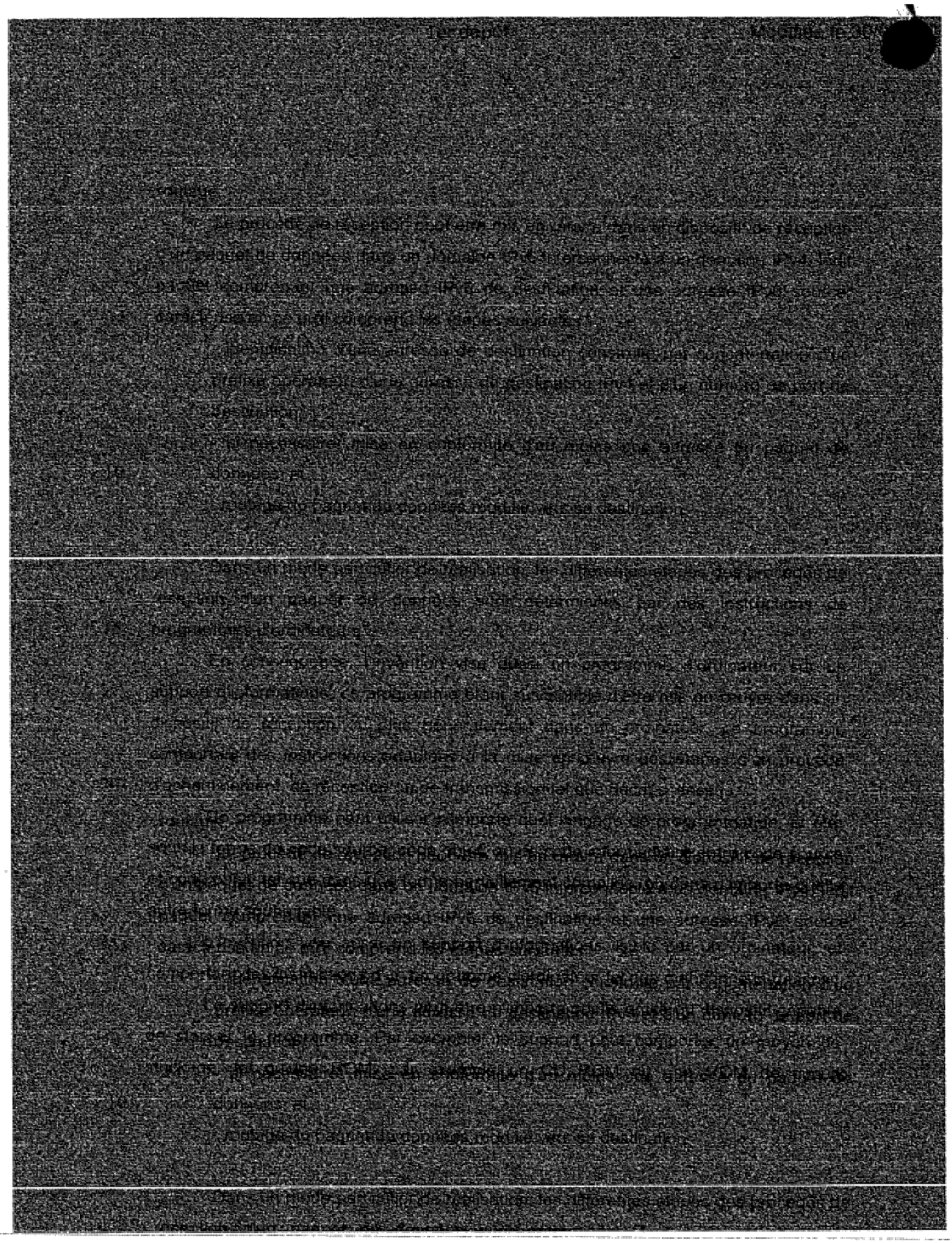
- recherche dans une table de traduction d'adresses de ladite passerelle d'une entrée associant à ladite adresse source une adresse source native.
- si une entrée a été trouvée, remplacement de l'adresse de destination construite du paquet de données par l'adresse de destination native de l'entrée.

On notera que le numéro de port destination est aussi remplacé par celui renseigné dans la table de traduction d'adresses et de ports telle que maintenue par la passerelle résidentielle.

Un tel paquet de données IPv6 a été construit à partir d'un paquet IPv4 par un équipement d'interconnexion du domaine IPv6 au domaine IPv4. Il se peut qu'il constitue une réponse à un paquet de données précédemment émis par le terminal d'utilisateur connecté à la passerelle résidentielle. Celle-ci consulte donc sa table de traduction. Si elle y trouve une association entre l'adresse de destination extraite du paquet de données reçu et une adresse de destination IPv6 native, elle remplace l'adresse de destination et potentiellement le numéro de port destination construite du paquet de données par l'adresse IPv6 native de l'entrée et route le paquet modifié vers le terminal destinataire.

Selon un autre aspect de l'invention, le procédé de réception comprend en outre une étape de vérification d'une concordance entre le numéro de port de destination du paquet de données et le numéro de port de destination contenu dans l'adresse de destination construite.

Une telle vérification permet de s'assurer que le numéro de port de destination du paquet de données au niveau transport coïncide bien avec le numéro de l'adresse de destination construite du paquet. Cette vérification présente un intérêt particulier si l'adresse IPv4 fictive affectée à la passerelle domestique est partagée avec plusieurs autres terminaux ou passerelles domestiques. En effet, dans ce cas, la discrimination entre ces équipements est faite sur la base de la plage de numéros de ports utilisée. Avec l'invention, le routage d'un paquet émis par terminal IPv4 vers ladite adresse fictive peut avoir lieu vers la passerelle concernée sans rencontrer de problème de



microélectronique, ou encore un moyen d'enregistrement magnétique, par exemple une disquette (floppy disc) ou un disque dur.

D'autre part, le support d'informations peut être un support transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Le programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, le support d'informations peut être un circuit intégré dans lequel le programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution du procédé en question.

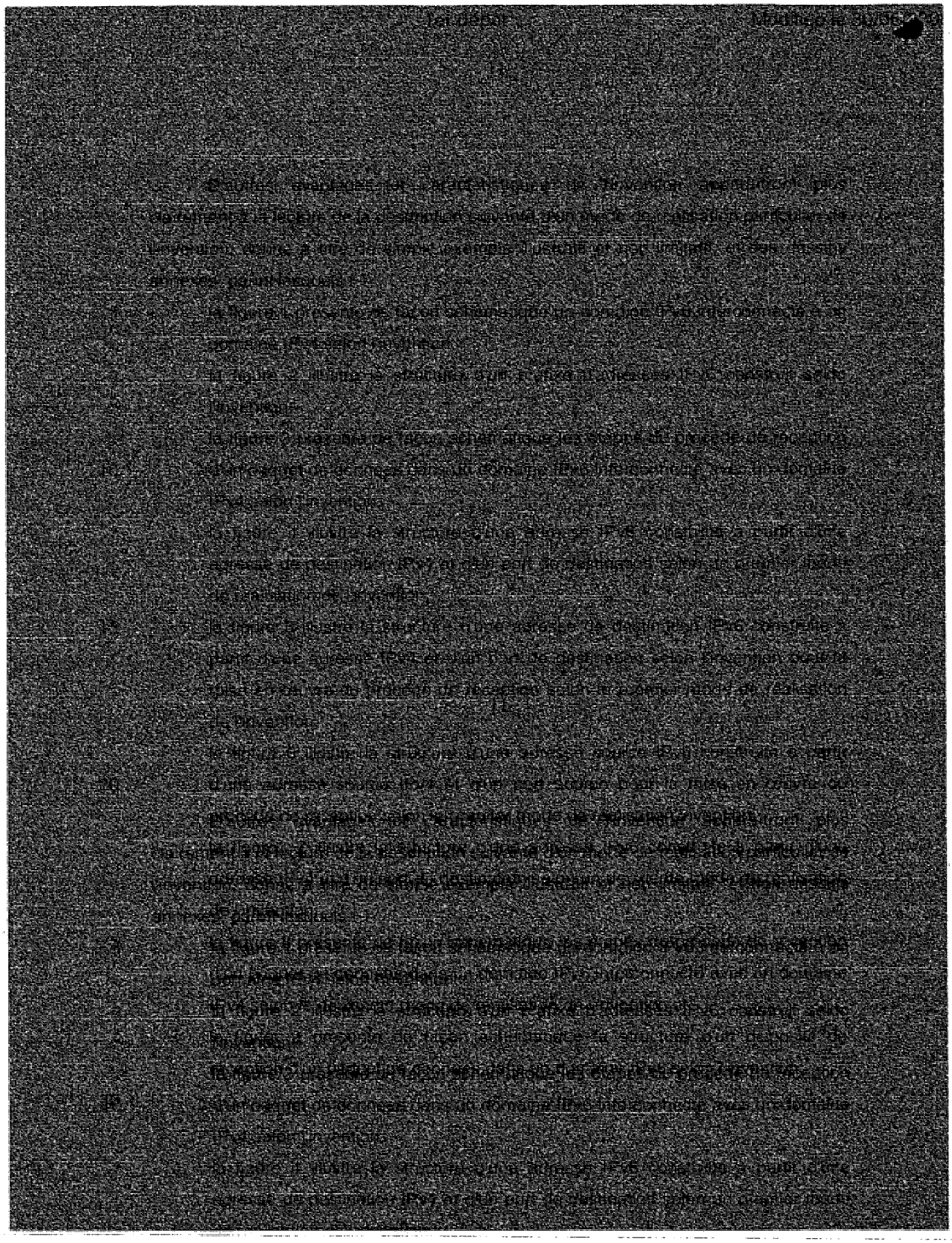
L'invention concerne aussi une passerelle résidentielle apte à connecter des terminaux d'utilisateurs à un domaine IPv6 interconnecté à un domaine IPv4. Selon l'invention, une telle passerelle comprend :

- des moyens d'obtention d'une adresse IPv4, d'une plage de numéros de ports autorisés pour ladite passerelle et d'une plage d'adresses IPv6 autorisées pour ladite passerelle, ladite plage d'adresses IPv6 étant construite par concaténation d'un préfixe opérateur, de ladite adresse IPv4 et de la plage de numéros de ports IPv4 autorisés; et
- un dispositif de réception d'un paquet de données IPv6 dans le domaine IPv6 interconnecté au domaine IPv4 selon l'invention.

Selon l'invention, une telle passerelle ne traite que des paquets de données IPv6. Toutefois, une adresse IPv4 lui est affectée, de façon à ce qu'elle puisse être identifiée et être jointe par des émetteurs du domaine IPv4. La dite adresse n'est pas utilisée par la passerelle domestique pour l'envoi des paquets IP.

La passerelle résidentielle peut comprendre une table de traduction d'adresses, comprenant des entrées, associant, pour une session de communication impliquant terminal d'utilisateur de son réseau résidentiel, au moins une adresse source. Selon l'invention, ladite passerelle est apte à enregistrer dans ladite entrée, une adresse source IPv6 construite et une adresse source IPv6 native du terminal d'utilisateur

Liste des figures



D'autres avantages et caractéristiques de l'invention apparaîtront plus clairement à la lecture de la description suivante d'un mode de réalisation particulier de l'invention, donné à titre de simple exemple illustratif et non limitatif, et des dessins annexés, parmi lesquels :

- la figure 1 présente de façon schématique un domaine IPv6 interconnecté à un domaine IPv4 selon l'invention;
- la figure 2 illustre la structure d'un préfixe d'adresses IPv6 construit selon l'invention;
- la figure 3 présente de façon schématique les étapes du procédé de réception d'un paquet de données dans un domaine IPv6 interconnecté avec un domaine IPv4 selon l'invention;
- la figure 4 illustre la structure d'une adresse IPv6 construite à partir d'une adresse de destination IPv4 et d'un port de destination selon un premier mode de réalisation de l'invention;
- la figure 5 illustre la structure d'une adresse de destination IPv6 construite à partir d'une adresse IPv4 et d'un port de destination selon l'invention pour la mise en œuvre du procédé de réception selon le premier mode de réalisation de l'invention;
- la figure 6 illustre la structure d'une adresse source IPv6 construite à partir d'une adresse source IPv4 et d'un port source pour la mise en œuvre du procédé de réception selon le premier mode de réalisation invention;
- la figure 7 illustre la structure d'une adresse IPv6 construite à partir d'une adresse IPv4 et d'un port de destination selon un deuxième mode de réalisation de l'invention;
- la figure 8 présente de façon schématique les étapes du procédé de réception d'un paquet de données dans un domaine IPv6 interconnecté avec un domaine IPv4 selon le deuxième mode de réalisation de l'invention;et
- la figure 9 présente de façon schématique la structure d'un dispositif de réception d'un paquet de données dans un domaine IPv6 selon l'invention;

7. Description d'un mode de réalisation particulier de l'invention

Le principe général de l'invention repose sur la construction d'une adresse IPv6 à partir d'une adresse IPv4, d'un préfixe opérateur prédéterminé et d'un numéro de port. Une telle construction permet la transformation d'un paquet IPv4 entrant dans un domaine IPv6 et inversement celle d'un paquet IPv6 sortant d'un domaine IPv6 à destination d'un domaine IPv4, sans qu'il soit nécessaire de maintenir une table de correspondance entre les adresses IPv4 et IPv6 dans un nœud d'accès au domaine IPv6.

Pour rappel, les adresses IPv6 sont longues de 16 octets, soit 128 bits, contre 4 octets (32 bits) pour les adresses IPv4. On dispose ainsi d'un nombre potentiel d'adresses extrêmement grand par rapport au nombre d'adresses IPv4. Une adresse IPv6 comporte deux parties:

- la partie de gauche (le préfixe) identifie un sous-réseau du domaine ;
- la partie de droite identifie une machine connectée au sous-réseau.

Généralement, les préfixes les plus longs alloués à un sous-réseau sont des préfixes "/64"; c'est-à-dire qu'ils comportent 64 bits pour les identifier. Les 64 bits de droite de l'adresse sont alors utilisés pour identifier une machine particulière appartenant au sous-réseau. Des préfixes de longueurs plus courtes (exemple "/56" ou même "/48") permettent quant à eux d'identifier des sous-réseaux de plus grande ampleur, comportant souvent eux-mêmes des sous-réseaux "/64". Néanmoins, dans le standard IPv6, rien n'interdit d'utiliser des préfixes plus longs que "/64", et on peut donc imaginer, par exemple, un préfixe "/116" qui identifie un sous-réseau pouvant comporter 4096 machines.

On notera que la seule restriction à des préfixes plus longs que "/64" consiste simplement dans le fait que les machines derrière le sous-réseau correspondant ne pourront pas mettre en œuvre le mécanisme d'auto-configuration décrit dans le document RFC2462. Ce mécanisme permet à une machine connaissant son adresse de niveau 2 (par exemple son adresse Ethernet MAC) de configurer elle-même, sous certaines conditions, les 64 bits de droite de son adresse IPv6, en dérivant son adresse de niveau 2 suivant un algorithme précis. Mais ce mécanisme d'auto-

7. Description d'un mode de réalisation particulier de l'invention

Le principe général de l'invention repose sur la construction d'une adresse IPv6 à partir d'une adresse IPv4, d'un préfixe opérateur prédéterminé et d'un numéro de port. Une telle construction permet la transformation d'un paquet IPv4 entrant dans un domaine IPv6 et inversement celle d'un paquet IPv6 sortant d'un domaine IPv6 à destination d'un domaine IPv4, sans qu'il soit nécessaire de maintenir une table de correspondance entre les adresses IPv4 et IPv6 dans un nœud d'accès au domaine IPv6.

Pour rappel, les adresses IPv6 sont longues de 16 octets, soit 128 bits, contre 4 octets (32 bits) pour les adresses IPv4. On dispose ainsi d'un nombre potentiel d'adresses extrêmement grand par rapport au nombre d'adresses IPv4. Une adresse IPv6 comporte deux parties:

- la partie de gauche (le préfixe) identifie un sous-réseau du domaine ;
- la partie de droite identifie une machine connectée au sous-réseau.

7. Description d'un mode de réalisation particulier de l'invention

Le principe général de l'invention repose sur la construction d'une adresse IPv6 à partir d'une adresse IPv4, d'un préfixe opérateur prédéterminé et d'un numéro de port. Une telle construction permet la transformation d'un paquet IPv4 entrant dans un domaine IPv6 et inversement celle d'un paquet IPv6 sortant d'un domaine IPv6 à destination d'un domaine IPv4, sans qu'il soit nécessaire de maintenir une table de correspondance entre les adresses IPv4 et IPv6 dans un nœud d'accès au domaine IPv6.

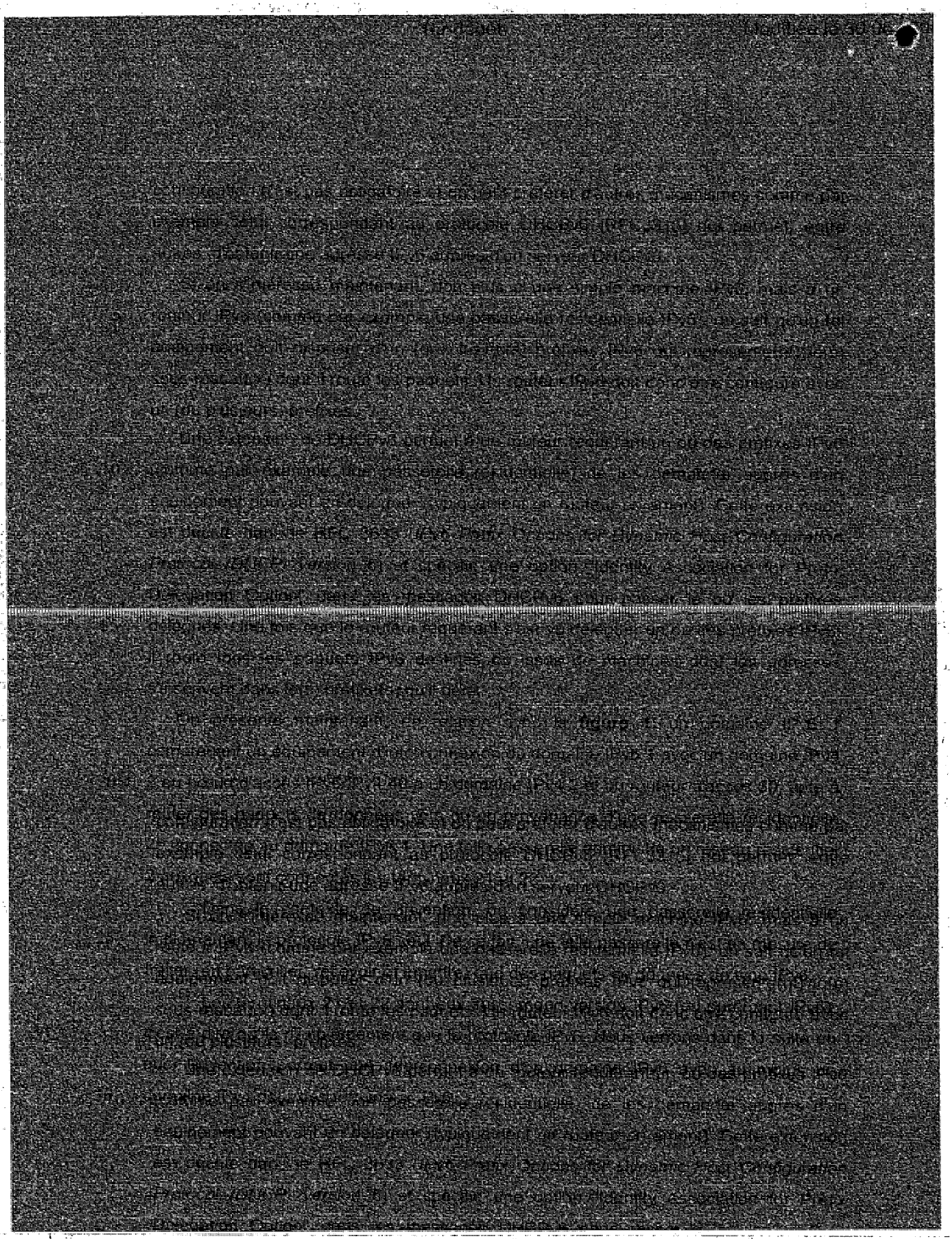
Pour rappel, les adresses IPv6 sont longues de 16 octets, soit 128 bits, contre 4 octets (32 bits) pour les adresses IPv4. On dispose ainsi d'un nombre potentiel d'adresses extrêmement grand par rapport au nombre d'adresses IPv4. Une adresse IPv6 comporte deux parties:

- la partie de gauche (le préfixe) identifie un sous-réseau du domaine ;
- la partie de droite identifie une machine connectée au sous-réseau.

Généralement, les préfixes les plus longs alloués à un sous-réseau sont des préfixes "/64"; c'est-à-dire qu'ils comportent 64 bits pour les identifier. Les 64 bits de droite de l'adresse sont alors utilisés pour identifier une machine particulière appartenant au sous-réseau. Des préfixes de longueurs plus courtes (exemple "/56" ou même "/48") permettent quant à eux d'identifier des sous-réseaux de plus grande ampleur, comportant souvent eux-mêmes des sous-réseaux "/64". Néanmoins, dans le standard IPv6, rien n'interdit d'utiliser des préfixes plus longs que "/64" et on peut donc imaginer, par exemple, un préfixe "/116" qui identifie un sous-réseau pouvant comporter 4096 machines.

On notera que la seule restriction à des préfixes plus longs que "/64" consiste simplement dans le fait que les machines derrière le sous-réseau correspondant ne pourront pas mettre en œuvre le mécanisme d'auto-configuration décrit dans le document RFC2462. Ce mécanisme permet à une machine connaissant son adresse de niveau 2 (par exemple son adresse Ethernet MAC) de configurer elle-même, sous certaines conditions, les 64 bits de droite de son adresse IPv6, en dérivant son adresse de niveau 2 suivant un algorithme précis. Mais ce mécanisme d'auto-

Juniper Exhibit 1002, page 171



CI

configuration n'est pas obligatoire et on peut préférer d'autres mécanismes comme par exemple celui correspondant au protocole DHCPv6 [RFC3315] qui permet, entre autres, d'obtenir une adresse IPv6 auprès d'un serveur DHCPv6.

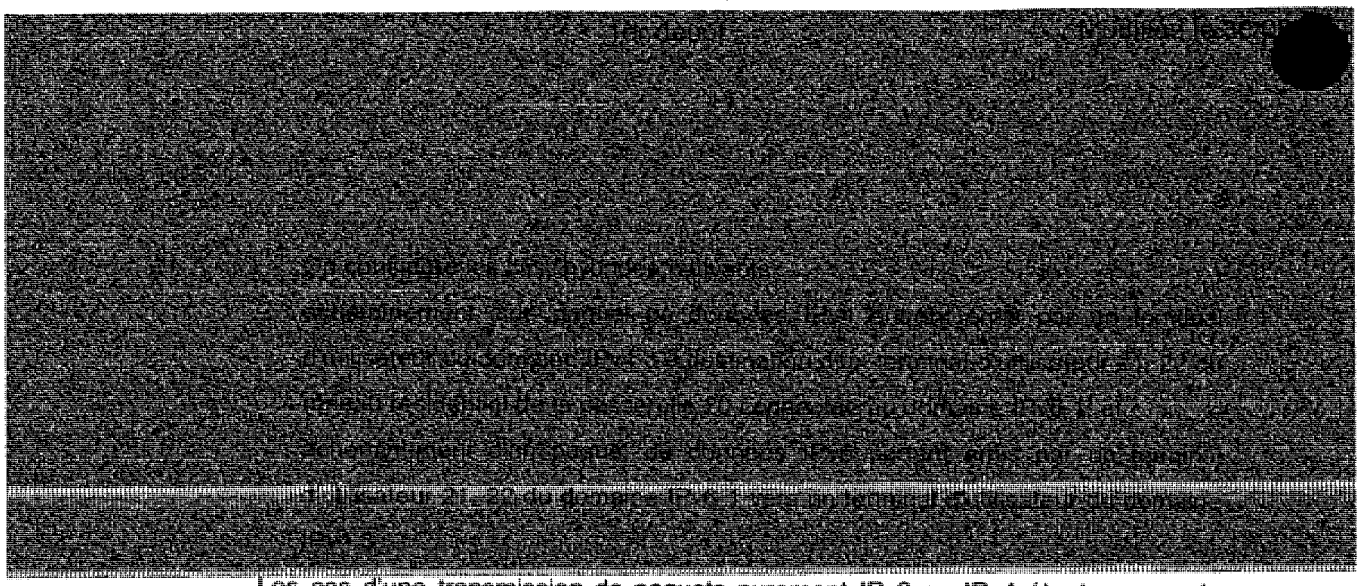
Si on s'intéresse maintenant, non plus à une simple machine IPv6, mais à un routeur IPv6 (comme par exemple une passerelle résidentielle IPv6), on sait qu'un tel équipement doit disposer d'un (ou plusieurs) préfixes IPv6 qui représente(nt) le(s) sous-réseau(x) dont il route les paquets. Un routeur IPv6 doit donc être configuré avec un (ou plusieurs) préfixes.

Une extension de DHCPv6 permet à un routeur requérant un ou des préfixes IPv6 (comme par exemple une passerelle résidentielle) de les demander auprès d'un équipement pouvant en déléguer (typiquement un routeur en amont). Cette extension est décrite dans le RFC 3633 (*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*) et spécifie une option "Identity Association for Prefix Delegation Option" dans les messages DHCPv6 pour passer le ou les préfixes délégués. Une fois que le routeur requérant s'est vu déléguer un ou des préfixes IPv6, il route tous les paquets IPv6 destinés ou issus de machines dont les adresses s'inscrivent dans le(s) préfixe(s) qu'il gère.

On présente maintenant, en relation avec la **figure 1**, un domaine IPv6 1 comprenant un équipement d'interconnexion du domaine IPv6 1 avec un domaine IPv4 2 ou nœud d'accès IPv6/IPv4 40 à un domaine IPv4 2 et un routeur d'accès 30, apte à router des paquets de données vers ou en provenance d'une passerelle résidentielle 20 connectée au domaine IPv6 1. Une telle passerelle administre un réseau résidentiel 2 auxquels sont connectés les terminaux 21 et 22.

Dans le contexte de l'invention, on considère une passerelle résidentielle implémentant le protocole IPv6 seul. De ce fait, une telle passerelle n'est en mesure de traiter (en particulier, recevoir et émettre) que des paquets de données de type IPv6.

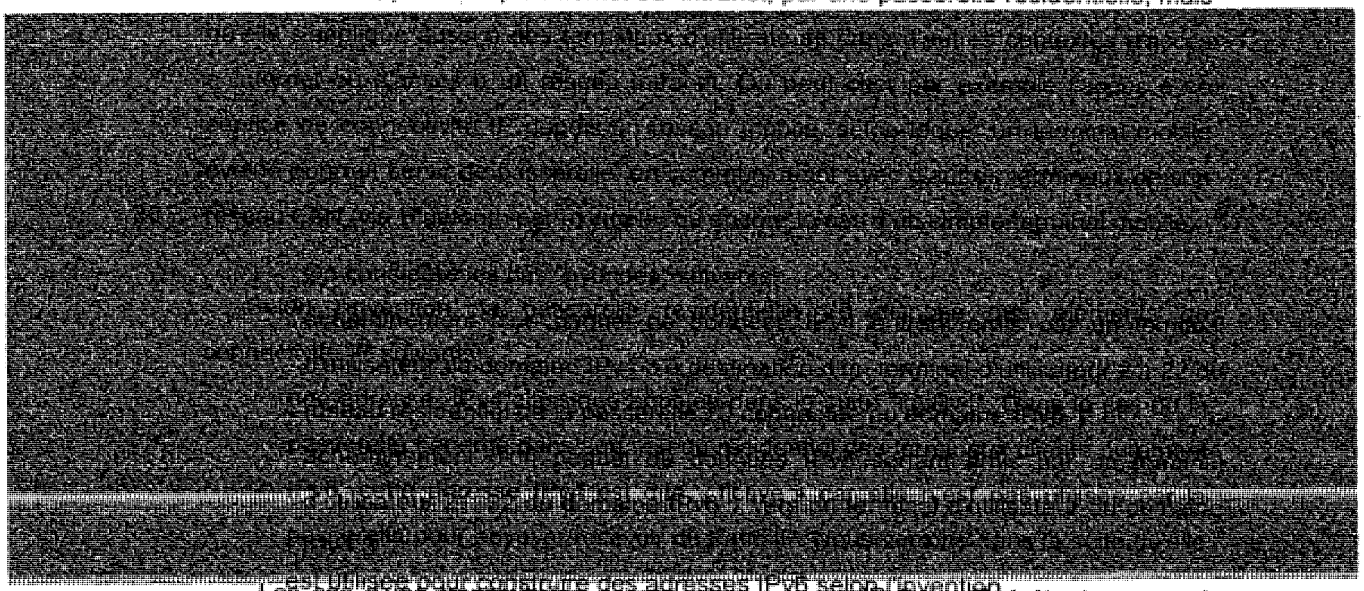
Les terminaux 21 et 22 sont eux aussi mono-version IPv6 (ou purement IPv6), c'est-à-dire qu'ils n'implémentent que le protocole IPv6. Nous verrons dans la suite en quoi l'invention permet une interconnexion d'un domaine IPv6 avec au moins un domaine IPv4 pour des terminaux IPv6.



Les cas d'une transmission de paquets purement IPv6 ou IPv4 étant connus de l'homme de métier, ils ne seront pas décrits plus en détails.

Pour pouvoir se connecter au domaine ou réseau IPv6, la passerelle résidentielle dispose d'éléments de connectivité IP fournis par le fournisseur de service de connectivité.

On notera toutefois que l'invention ne se limite pas à l'accès au service de connectivité IP, par exemple Internet ou Intranet, par une passerelle résidentielle, mais



Les cas d'une transmission de paquets purement IPv6 ou IPv4 étant connus de l'homme de métier, ils ne seront pas décrits plus en détails.

Pour pouvoir se connecter au domaine ou réseau IPv6, la passerelle résidentielle dispose d'éléments de connectivité IP fournis par le fournisseur de service de connectivité.

On considère les cas "hybrides" suivants :

- acheminement d'un paquet de données IPv4 entrant émis par un terminal d'utilisateur du domaine IPv4 3 à destination d'un terminal d'utilisateur 21, 22 du réseau résidentiel de la passerelle 20 connectée au domaine IPv6 1; et
- acheminement d'un paquet de données IPv6 sortant émis par un terminal d'utilisateur 21, 22 du domaine IPv6 1 vers un terminal d'utilisateur du domaine IPv4 3.

Les cas d'une transmission de paquets purement IPv6 ou IPv4 étant connus de l'homme de métier, ils ne seront pas décrits plus en détails.

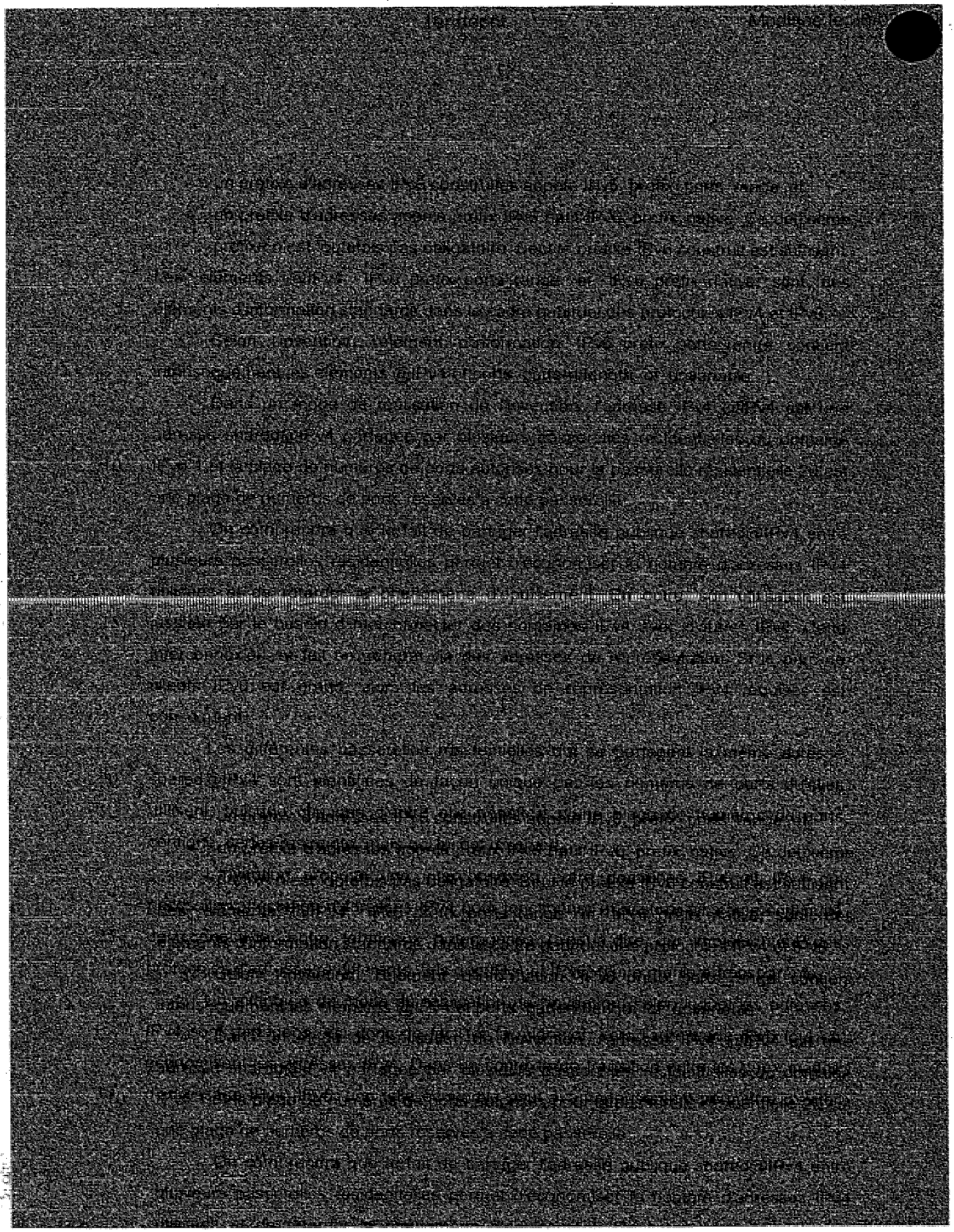
Pour pouvoir se connecter au domaine ou réseau IPv6, la passerelle résidentielle dispose d'éléments de connectivité IP fournis par le fournisseur de service de connectivité.

On notera toutefois que l'invention ne se limite pas à l'accès au service de connectivité IP, par exemple Internet ou Intranet, par une passerelle résidentielle, mais qu'elle s'applique aussi à des terminaux d'utilisateurs dans d'autres contextes d'accès à Internet ou d'accès à un réseau Intranet. On peut citer par exemple l'accès à ce service de connectivité IP depuis un réseau mobile, selon lequel un terminal mobile évolué pourrait servir de passerelle, en communiquant avec d'autres terminaux de son réseau LAN (via Bluetooth par exemple) ou encore le cas d'un simple terminal mobile.

Selon l'invention, la passerelle résidentielle 20 dispose des éléments de connectivité IP suivants:

- une adresse IPv4 classique appelée dans la suite "@IPv4". Dans le cas où la passerelle héberge dans son réseau résidentiel des terminaux clients purement IPv6, cette adresse IPv4 est dite « fictive » car elle n'est pas utilisée par la passerelle pour envoyer/recevoir du trafic IP. Nous verrons dans la suite qu'elle est utilisée pour construire des adresses IPv6 selon l'invention
- une plage de numéros de ports autorisés appelée ports_pattern/length_of_unvariable;

Juniper Exhibit 1002, page 175



- un préfixe d'adresses IPv6 construites appelé IPv6_prefix_ports_range; et
- un préfixe d'adresses appelé préfix IPv6 natif IPv6_prefix_native. Ce deuxième préfixe n'est toutefois pas obligatoire. Seul le préfixe IPv6 construit est suffisant.

Les éléments @IPv4, IPv6_prefix_ports_range et IPv6_prefix_native sont des éléments d'information standards dans le cadre habituel des protocoles IPv4 et IPv6.

Selon l'invention, l'élément d'information IPv6_prefix_ports_range contient intrinsèquement les éléments @IPv4 et ports_pattern/length_of_unvariable.

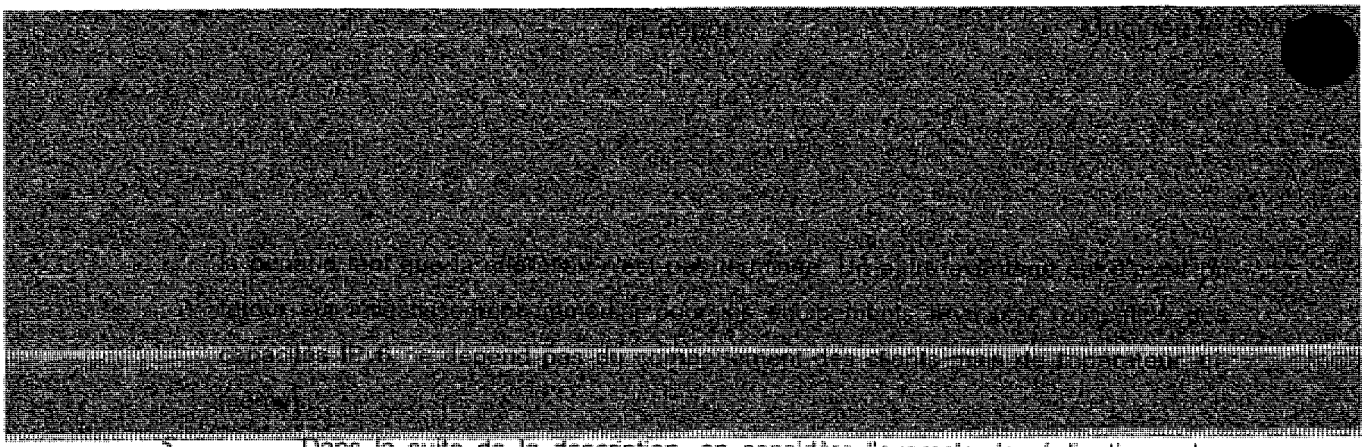
Dans un mode de réalisation de l'invention, l'adresse IPv4 @IPv4 est une adresse shared@IPv4 partagée par plusieurs passerelles résidentielles du domaine IPv6 1 et la plage de numéros de ports autorisés pour la passerelle résidentielle 20 est une plage de numéros de ports réservés à cette passerelle.

On comprendra que le fait de partager l'adresse publique shared@IPv4 entre plusieurs passerelles résidentielles permet d'économiser le nombre d'adresses IPv4 utilisées et de retarder le phénomène d'épuisement. En outre, son utilisation est justifiée par le besoin d'interconnecter des domaines IPv4 avec d'autres IPv6. Cette interconnexion se fait en général via des adresses de représentation. Si le parc de clients IPv6 est grand, alors les adresses de représentation IPv4 requises est conséquent.

Les différentes passerelles résidentielles qui se partagent la même adresse shared@IPv4 sont identifiées de façon unique par les numéros de ports qu'elles utilisent, puisque chacune d'entre elle bénéficie d'une plage de numéros de ports contigüe, certes restreinte, mais qui lui est réservée.

L'invention propose une interconnexion entre domaines IPv6 et IPv4 qui nécessite l'affectation d'adresses IPv4 pour fonctionner et assurer ainsi une continuité de connectivité entre terminaux hétérogènes (c'est-à-dire qui implémentent des protocoles d'adressage différents, tels que IPv4 et IPv6) d'une manière transparente.

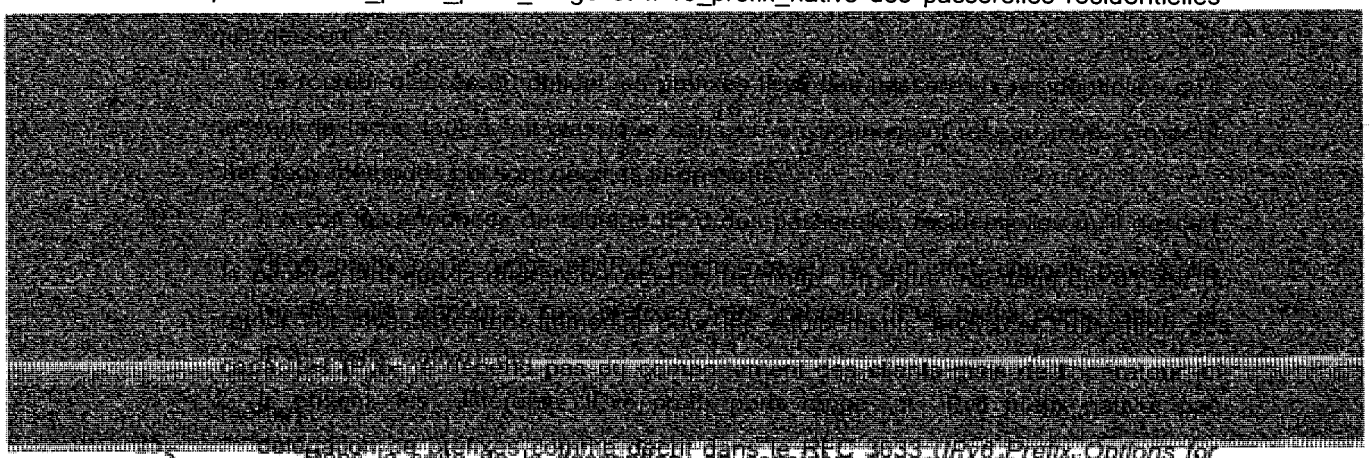
Un avantage du mode de réalisation de l'invention, selon lequel les adresses IPv4 sont partagées, est donc de faciliter la migration vers l'adressage IPv6 tout en économisant les adresses IPv4. Dans un contexte de transition entre les deux modes d'adressage IPv4, IPv6, une telle économie peut avantageusement permettre d'éviter



Dans la suite de la description, on considère l'exemple de réalisation selon lequel l'adresse IPv4 affectée à la passerelle 20 est une adresse partagée Shared@IPv4.

En relation avec la **figure 1**, la passerelle résidentielle 20 est connectée au réseau de l'opérateur par un routeur d'accès 30. Il s'agit du premier routeur que les paquets de données IPv6 et IPv4 rencontrent lorsqu'ils sortent de la passerelle résidentielle.

Suivant l'architecture réseau adoptée au niveau du routage IPv6, le routeur d'accès 30 peut annoncer en direction de l'amont du réseau (i.e. vers le réseau 1 du fournisseur de service de connectivité IP) les préfixes IPv6 qu'il route, c'est-à-dire les préfixes IPv6_prefix_ports_range et IPv6_prefix_native des passerelles résidentielles



Dans la suite de la description, on considère l'exemple de réalisation selon lequel l'adresse IPv4 affectée à la passerelle 20 est une adresse partagée Shared@IPv4.

En relation avec la **figure 2**, on présente maintenant un exemple de constitution d'un préfixe d'adresses IPv6 construites selon l'invention, tel que le préfixe IPv6_prefix_ports_range affecté à la passerelle résidentielle 20.

En relation avec la **figure 1**, la passerelle résidentielle 20 est connectée au réseau de l'opérateur par un routeur d'accès 30. Il s'agit du premier routeur que les paquets de données IPv6 et IPv4 rencontrent lorsqu'ils sortent de la passerelle résidentielle.

Suivant l'architecture réseau adoptée au niveau du routage IPv6, le routeur d'accès 30 peut annoncer en direction de l'amont du réseau (i.e. vers le réseau 1 du

la pénurie tant que la migration n'est pas terminée. Un autre avantage est d'avoir un retour sur investissement immédiat pour les équipements IPv6 (car l'utilisation des capacités IPv6 ne dépend pas du comportement des clients mais de l'opérateur lui-même).

Dans la suite de la description, on considère l'exemple de réalisation selon lequel l'adresse IPv4 affectée à la passerelle 20 est une adresse partagée Shared@IPv4.

En relation avec la **figure 1**, la passerelle résidentielle 20 est connectée au réseau de l'opérateur par un routeur d'accès 30. Il s'agit du premier routeur que les paquets de données IPv6 et IPv4 rencontrent lorsqu'ils sortent de la passerelle résidentielle.

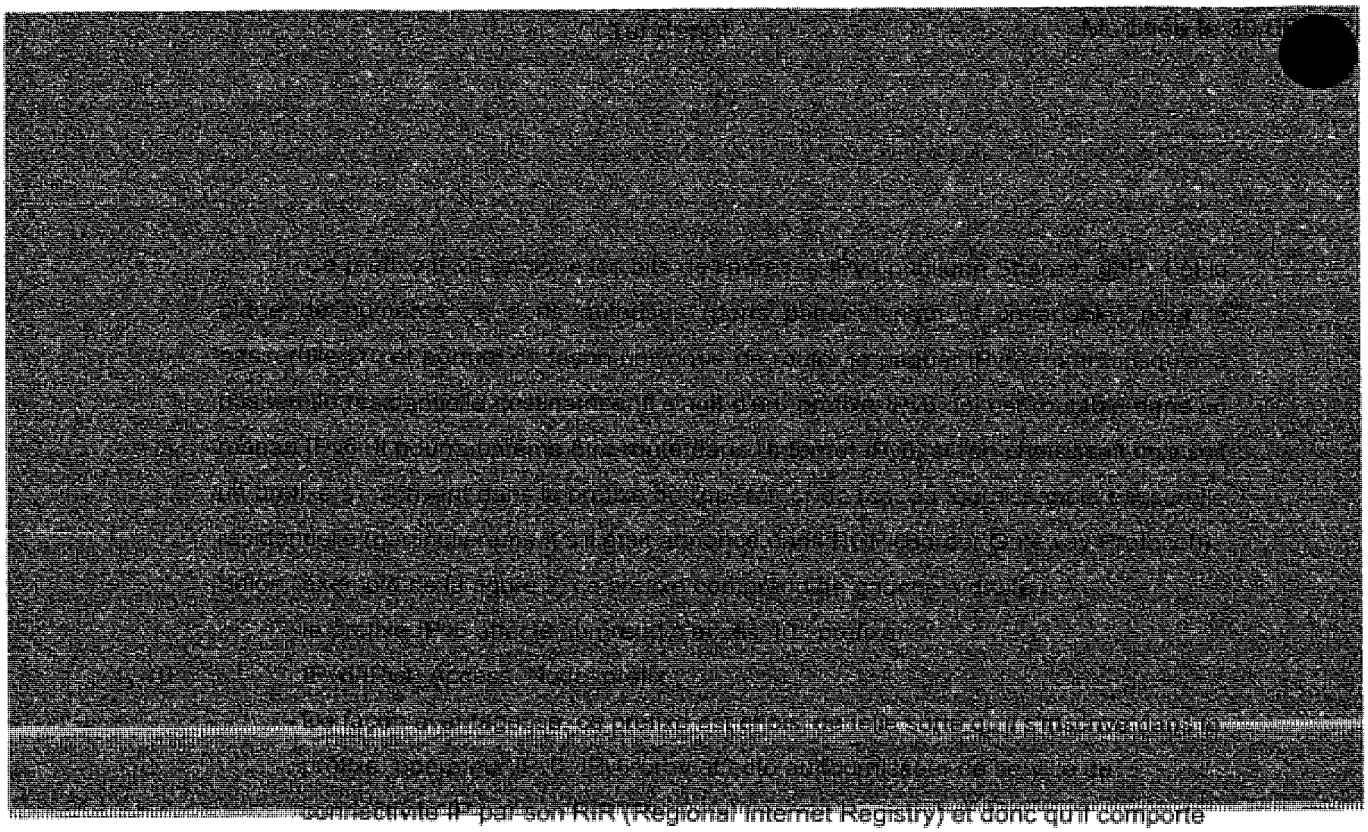
Suivant l'architecture réseau adoptée au niveau du routage IPv6, le routeur d'accès 30 peut annoncer en direction de l'amont du réseau (i.e. vers le réseau 1 du fournisseur de service de connectivité IP) les préfixes IPv6 qu'il route, c'est-à-dire les préfixes IPv6_prefix_ports_range et IPv6_prefix_native des passerelles résidentielles qu'il dessert.

Le routeur d'accès 30 obtient les préfixes IPv6 des passerelles résidentielles qu'il dessert de façon tout à fait classique dans un environnement réseau IPv6. On peut citer deux méthodes qui sont décrites ci-dessous:

1- il reçoit les annonces de routage IPv6 des passerelles résidentielles qu'il dessert (IPv6_prefix_ports_range et IPv6_prefix_native). A cet effet, chaque passerelle résidentielle annonce ses préfixes vers l'amont (IPv6_prefix_ports_range et IPv6_prefix_native); ou

2- Il obtient les différents IPv6_prefix_ports_range et IPv6_prefix_native par délégation de préfixes comme décrit dans le RFC 3633 (*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*).

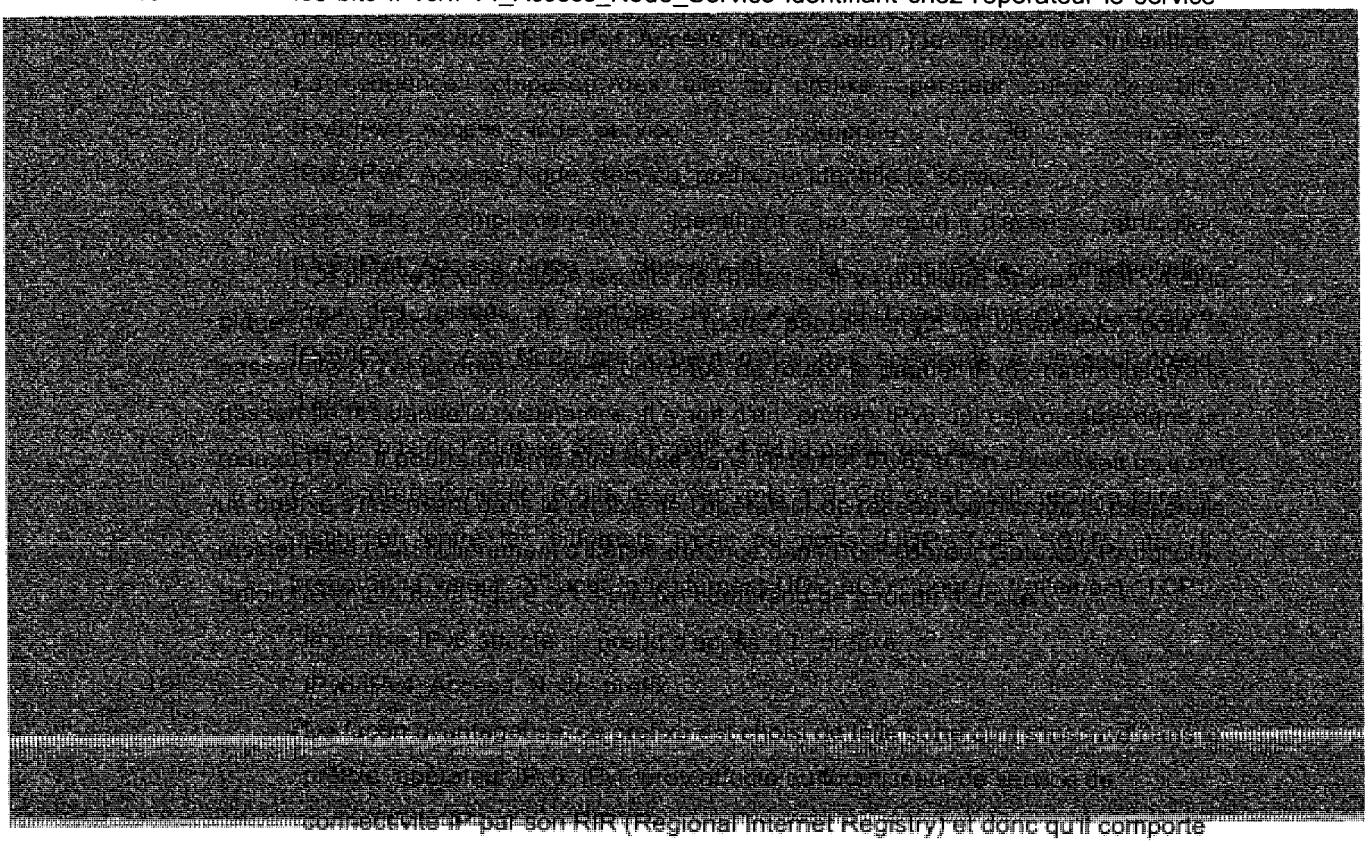
En relation avec la **figure 2**, on présente maintenant un exemple de constitution d'un préfixe d'adresses IPv6 construites selon l'invention, tel que le préfixe IPv6_prefix_ports_range affecté à la passerelle résidentielle 20.



connectivité IP par son RIR (Regional Internet Registry) et donc qu'il comporte

ce préfixe opérateur dans ses premiers bits :

- les bits IPv6/IPv4_Access_Node_Service identifiant chez l'opérateur le service



connectivité IP par son RIR (Regional Internet Registry) et donc qu'il comporte

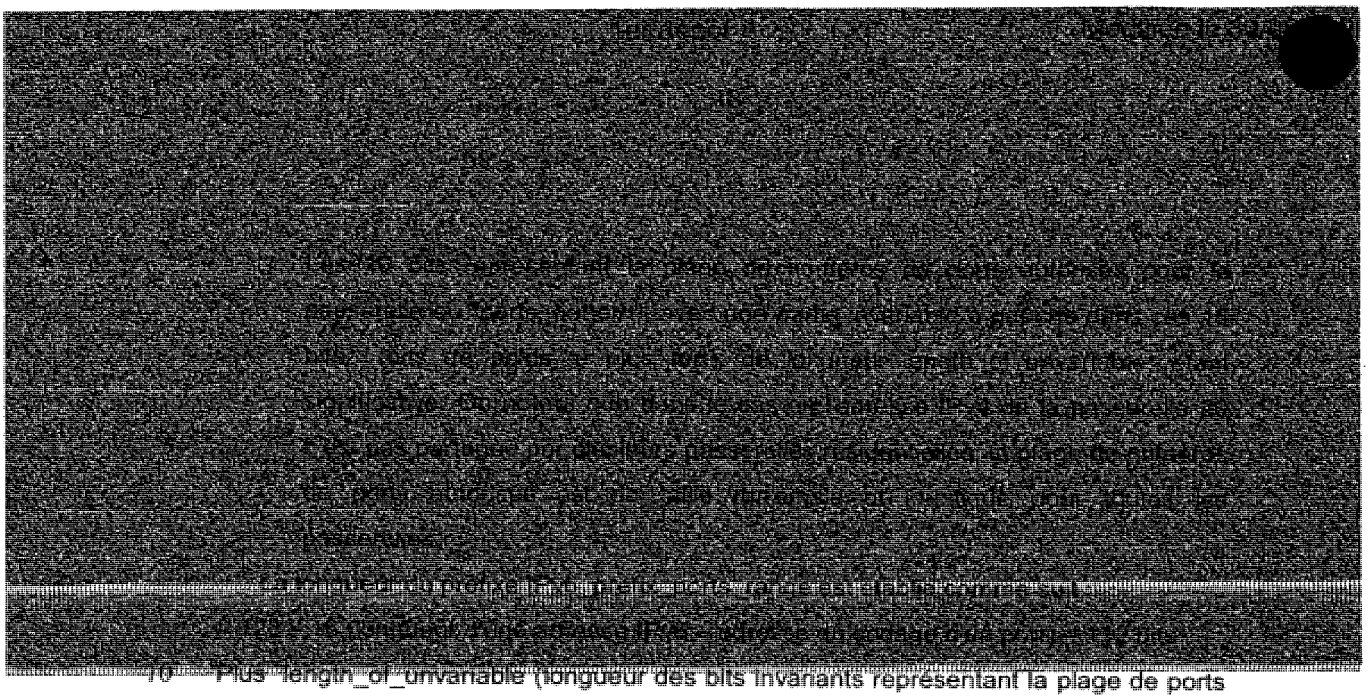
ce préfixe opérateur dans ses premiers bits :

- les bits IPv6/IPv4_Access_Node_Service identifiant chez l'opérateur le service

CI

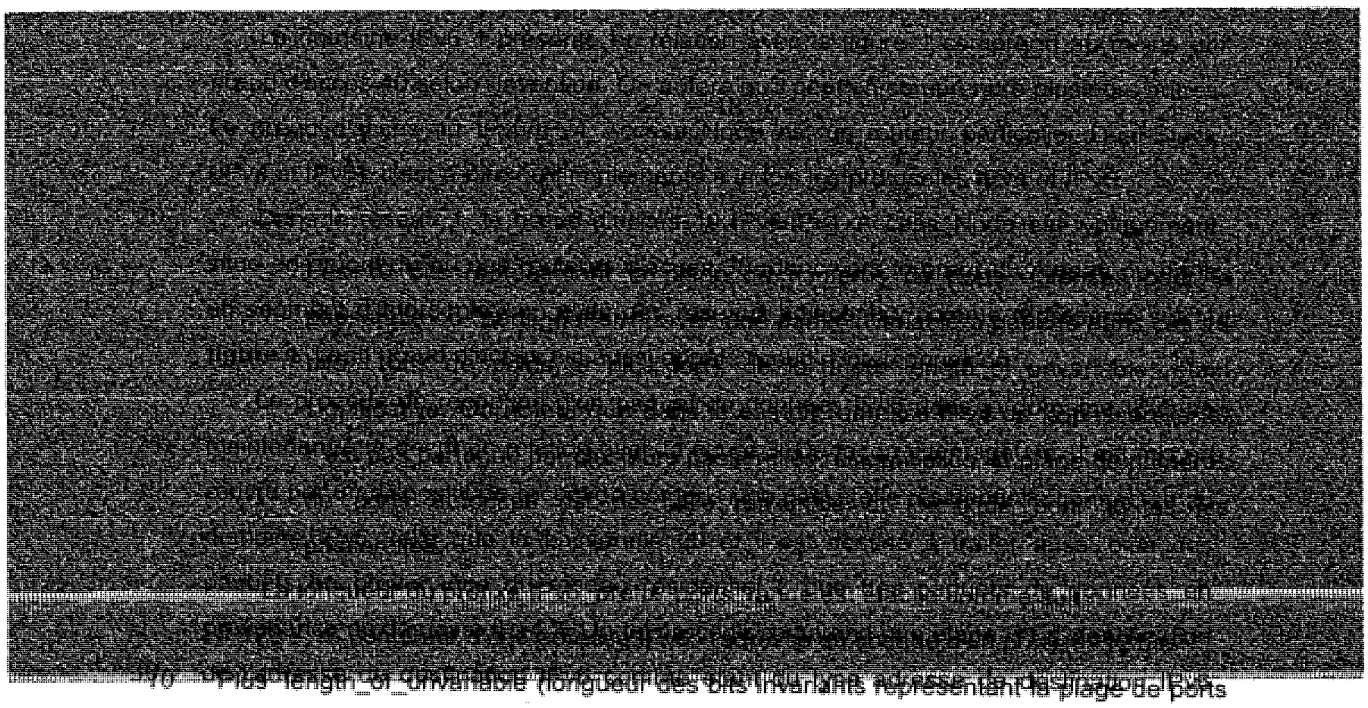
Ce préfixe IPv6 englobe les bits de l'adresse IPv4 publique Shared_@IPv4 et la plage de numéros de ports autorisés (ports_pattern/length_of_unvariable) pour la passerelle 20, et permet de façon univoque de router le paquet IPv6 entrant jusqu'à la passerelle résidentielle destinatrice. Il s'agit d'un préfixe IPv6 qui est routable dans un réseau IPv6. Il pourrait même être routé dans l'Internet IPv6, si l'on choisissait qu'il soit un préfixe s'inscrivant dans le préfixe de l'opérateur de réseau fournissant la passerelle résidentielle (particulièrement s'il était annoncé dans BGP (Border Gateway Protocol)). Selon l'exemple de la figure 2, ce préfixe comprend de gauche à droite :

- le préfixe IPv6 affecté au nœud d'accès 40 : préfixe IPv6/IPv4_Access_Node_prefix ;
  De façon avantageuse, ce préfixe est choisi de telle sorte qu'il s'inscrive dans le préfixe opérateur IPv6 IPv6-prov affecté au fournisseur de service de connectivité IP par son RIR (Regional Internet Registry) et donc qu'il comporte ce préfixe opérateur dans ses premiers bits :
- les bits IPv6/IPv4_Access_Node_Service identifiant chez l'opérateur le service d'interconnexion IPv6/IPv4_Access_Node selon la présente invention. La séquence composée des bits du préfixe opérateur suivis des bits IPv6/IPv4_Access_Node_Service compose le préfixe IPv6/IPv4_Access_Node_Service_prefix qui identifie le service ;
- des bits complémentaires identifiant un nœud d'accès particulier IPv6/IPv4_Access_Node desservant la passerelle résidentielle. Pour des raisons de partage de charge (ou Load-balancing), le préfixe IPv6/IPv4_Access_Node_prefix peut n'être pas spécifique à un seul nœud d'accès.
- Les 32 bits de l'adresse Shared_@IPv4 de la passerelle 20 ;
- De façon optionnelle, 8 bits réservés, mis à 0. Cet octet peut servir à faire la distinction entre les différents types de ports (UDP, TCP, SCTP, etc.) Il prendrait la valeur "X" pour le traitement UDP et "Y" pour le traitement "TCP", etc.



- Plus "length_of_unvariable (longueur des bits invariants représentant la plage de ports source autorisés).]

On notera que le préfixe IPv6_prefix_ports_range constitué selon l'invention est plus long que les préfixes recommandés par le standard IPv6 pour un déploiement IPv6. Néanmoins, ceci ne l'empêche pas d'être conforme aux standards IPv6.



- Plus "length_of_unvariable (longueur des bits invariants représentant la plage de ports source autorisés).]

On notera que le préfixe IPv6_prefix_ports_range constitué selon l'invention est plus long que les préfixes recommandés par le standard IPv6 pour un déploiement IPv6. Néanmoins, ceci ne l'empêche pas d'être conforme aux standards IPv6.

- Les 16 bits représentant la plage de numéros de ports autorisés pour la passerelle ou "ports_pattern", avec une partie invariable à gauche dans ces 16 bits (bits de poids le plus fort), de longueur length_of_unvariable, étant significative. On notera que dans le cas où l'adresse IPv4 de la passerelle 20 n'est pas partagée par plusieurs passerelles résidentielles, la plage de numéros de ports autorisés est de taille maximale et identique pour toutes les passerelles.

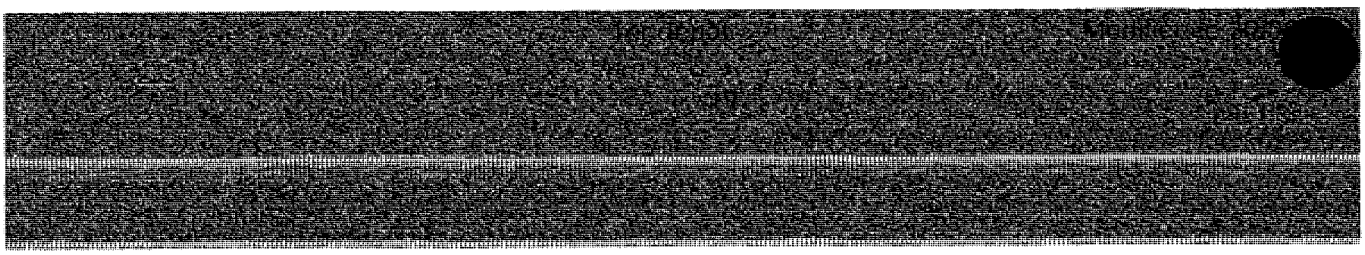
La longueur du préfixe IPv6_prefix_ports_range est établie comme suit :
[128 – 16 (longueur d'une adresse IPv6 – adresse du codage d'un port) = 112 bits
Plus length_of_unvariable (longueur des bits invariants représentant la plage de ports source autorisés).]

On notera que le préfixe IPv6_prefix_ports_range constitué selon l'invention est plus long que les préfixes recommandés par le standard IPv6 pour un déploiement IPv6. Néanmoins, ceci ne l'empêche pas d'être conforme aux standards IPv6.

Le domaine IPv6 1 présenté en relation avec la figure 1 comprend au moins un nœud d'accès 40 selon l'invention. On notera qu'il peut en comprendre plusieurs autres. Le nœud d'accès 40 IPv6/IPv4_Access_Node est un routeur particulier Dual-Stack (IPv4 et IPv6), c'est-à-dire qu'il implémente à la fois les protocoles IPv4 et IPv6.

Dans le réseau 1, le nœud d'accès 40 IPv6/IPv4_Access_Node est typiquement situé en amont du ou des routeurs d'accès 30 (donc vers le cœur du réseau ou dans un segment d'interconnexion avec des réseaux adjacents), comme représenté sur la **figure 1**. Ledit nœud d'accès est aussi appelé nœud d'interconnexion.

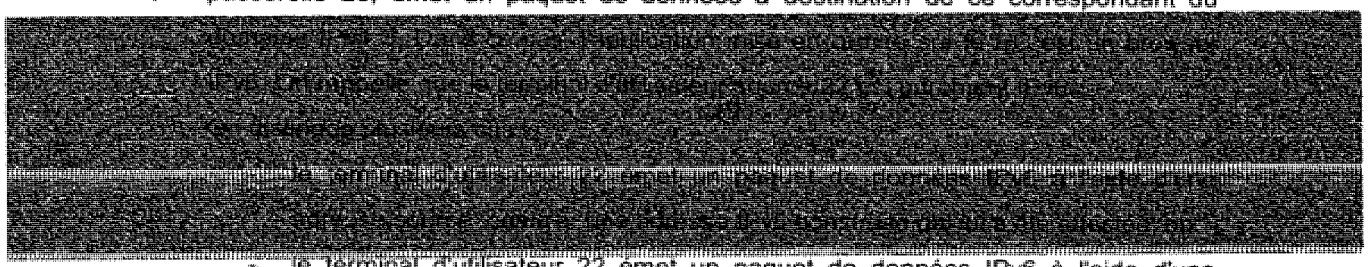
Le procédé de réception d'un paquet de données IPv6 dans le domaine IPv6 va maintenant être décrit en relation avec la figure 3. De façon avantageuse, il est mis en œuvre par un dispositif de réception compris une passerelle résidentielle connectée au domaine IPv6, telle que la passerelle 20 et il est destiné à traiter aussi bien des paquets en provenance du réseau résidentiel 2 que des paquets de données en provenance du domaine IPv4 3. Un tel procédé comprend une étape R1 d'identification de l'adresse de destination IPv6 comme étant du type adresse de destination IPv6



native, soit comme étant du type adresse de destination IPv6 construite par concaténation d'un préfixe de nœud d'accès, d'une adresse IPv4 de destination et d'un numéro de port IPv4 de destination. On suppose ici que la passerelle 20 a obtenu ce préfixe au préalable, par exemple par configuration.

Il comprend ensuite une étape R2 de mise en conformité d'une adresse du paquet de données. Dans le sens réseau résidentiel vers un domaine IPv6, il s'agit de l'adresse source du paquet; dans le sens domaine IPv6 vers un réseau résidentiel, il s'agit de son adresse de destination. Une telle mise en conformité peut entraîner une modification du paquet de données. Le paquet de données modifié est ensuite routé en R3 vers sa destination.

Selon un premier mode de réalisation de l'invention, On considère l'établissement d'une communication sortante vers un destinataire IPv4 qui peut, par exemple, être un serveur Web IPv4 localisé dans le réseau Internet. Un terminal d'utilisateur du réseau résidentiel 2, par exemple le PC IPv6 22 connecté à la passerelle 20, émet un paquet de données à destination de ce correspondant du



native, soit comme étant du type adresse de destination IPv6 construite par concaténation d'un préfixe de nœud d'accès, d'une adresse IPv4 de destination et d'un numéro de port IPv4 de destination. On suppose ici que la passerelle 20 a obtenu ce préfixe au préalable, par exemple par configuration.

Il comprend ensuite une étape R2 de mise en conformité d'une adresse du paquet de données. Dans le sens réseau résidentiel vers un domaine IPv6, il s'agit de l'adresse source du paquet; dans le sens domaine IPv6 vers un réseau résidentiel, il s'agit de son adresse de destination. Une telle mise en conformité peut entraîner une modification du paquet de données. Le paquet de données modifié est ensuite routé en R3 vers sa destination.

Selon un premier mode de réalisation de l'invention, On considère l'établissement d'une communication sortante vers un destinataire IPv4 qui peut, par exemple, être un serveur Web IPv4 localisé dans le réseau Internet. Un terminal d'utilisateur du réseau résidentiel 2, par exemple le PC IPv6 22 connecté à la passerelle 20, émet un paquet de données à destination de ce correspondant du réseau Internet. Le terminal d'utilisateur 22 émet un paquet de données IPv6 à l'aide d'une adresse source égale à une adresse IPv6 native qui lui a été affectée.

On comprend que le paquet de données comprend une adresse de destination IPv6 correspondant au destinataire IPv4 que le terminal doit avoir récupéré au préalable.

Le browser du terminal 22 a donc besoin de connaître l'adresse IPv6 du serveur Web destinataire. Or, le serveur Web n'est accessible qu'en IPv4. Il faut donc que le terminal 22 dispose d'une adresse IPv6 qu'il considérera comme l'adresse du serveur Web (alors qu'en réalité le serveur Web ne dispose que d'une adresse IPv4).

native, soit comme étant du type adresse de destination IPv6 construite par concaténation d'un préfixe de nœud d'accès, d'une adresse IPv4 de destination et d'un numéro de port IPv4 de destination. On suppose ici que la passerelle 20 a obtenu ce préfixe au préalable, par exemple par configuration.

Il comprend ensuite une étape R2 de mise en conformité d'une adresse du paquet de données. Dans le sens réseau résidentiel vers un domaine IPv6, il s'agit de l'adresse source du paquet; dans le sens domaine IPv6 vers un réseau résidentiel, il s'agit de son adresse de destination. Une telle mise en conformité peut entraîner une modification du paquet de données. Le paquet de données modifié est ensuite routé en R3 vers sa destination.

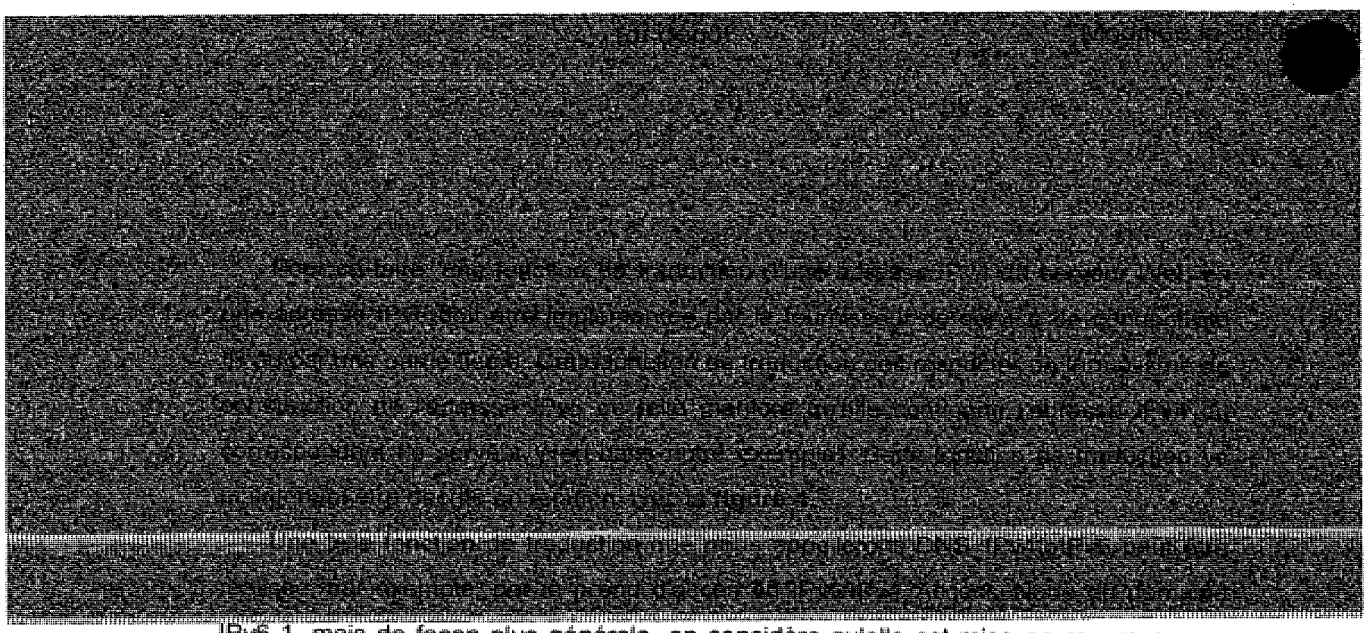
Selon un premier mode de réalisation de l'invention, On considère l'établissement d'une communication sortante vers un destinataire IPv4 qui peut, par exemple, être un serveur Web IPv4 localisé dans le réseau Internet. Un terminal d'utilisateur du réseau résidentiel 2, par exemple le PC IPv6 22 connecté à la passerelle 20, émet un paquet de données à destination de ce correspondant du domaine IPv4 3. Dans ce cas, l'application mise en œuvre sur le PC est un browser IPv6. On rappelle que le terminal d'utilisateur source 22 est purement IPv6.

On distingue plusieurs cas :

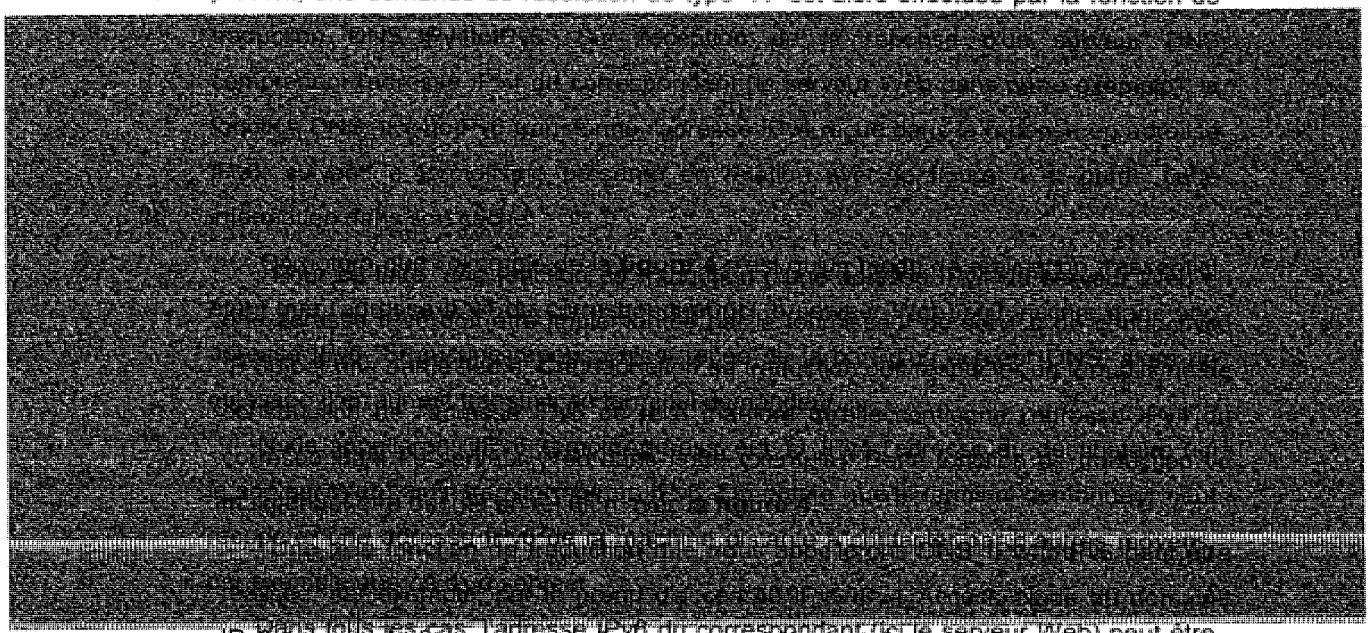
- le terminal d'utilisateur 22 émet un paquet de données IPv6 à l'aide d'une adresse source égale à une adresse IPv6 construite qui lui a été affectée; ou
- le terminal d'utilisateur 22 émet un paquet de données IPv6 à l'aide d'une adresse source égale à une adresse IPv6 native qui lui a été affectée.

On comprend que le paquet de données comprend une adresse de destination IPv6 correspondant au destinataire IPv4 que le terminal doit avoir récupéré au préalable.

Le browser du terminal 22 a donc besoin de connaître l'adresse IPv6 du serveur Web destinataire. Or, le serveur Web n'est accessible qu'en IPv4. Il faut donc que le terminal 22 dispose d'une adresse IPv6 qu'il considérera comme l'adresse du serveur Web (alors qu'en réalité le serveur Web ne dispose que d'une adresse IPv4).



IPv6 1, mais de façon plus générale, on considère qu'elle est mise en œuvre par un serveur DNS du domaine 1. La fonction DNS_IPv4toIPv6 est le point de contact par défaut pour toute demande de résolution DNS émise par un terminal demandeur. Par défaut, cette fonction examine d'abord les enregistrements IPv6 de type "AAAA", autrement dit les adresses IPv6 natives. Si un enregistrement est déjà présent, une réponse est alors émise vers le terminal demandeur. Si aucun enregistrement n'est présent, une demande de résolution de type "A" est alors effectuée par la fonction de



IPv6 1, mais de façon plus générale, on considère qu'elle est mise en œuvre par un serveur DNS du domaine 1. La fonction DNS_IPv4toIPv6 est le point de contact par défaut pour toute demande de résolution DNS émise par un terminal demandeur. Par défaut, cette fonction examine d'abord les enregistrements IPv6 de type "AAAA", autrement dit les adresses IPv6 natives. Si un enregistrement est déjà présent, une

Pour ce faire, une fonction de traduction d'une adresse IPv4 du serveur Web en une adresse IPv6 doit être implémentée par le fournisseur de service de connectivité IP ou par une partie tierce. Cette fonction de traduction doit respecter un formalisme de construction de l'adresse IPv6 de telle manière qu'elle contienne l'adresse IPv4 du correspondant (le serveur Web dans notre exemple). Cette fonction de traduction va maintenant être décrite en relation avec la **figure 4**.

Une telle fonction de traduction que nous appellerons DNS_IPv4toIPv6 peut être réalisée, par exemple, par le nœud d'accès 40 IPv6/IPv4_Access_Node du domaine IPv6 1, mais de façon plus générale, on considère qu'elle est mise en œuvre par un serveur DNS du domaine 1. La fonction DNS_IPv4toIPv6 est le point de contact par défaut pour toute demande de résolution DNS émise par un terminal demandeur. Par défaut, cette fonction examine d'abord les enregistrements IPv6 de type "AAAA", autrement dit les adresses IPv6 natives. Si un enregistrement est déjà présent, une réponse est alors émise vers le terminal demandeur. Si aucun enregistrement n'est présent, une demande de résolution de type "A" est alors effectuée par la fonction de traduction DNS_IPv4toIPv6. Sur réception de la réponse d'un serveur DNS comprenant l'adresse IPv4 du correspondant (le serveur Web dans notre exemple), la fonction DNS_IPv4toIPv6 transforme l'adresse IPv4 reçue dans la réponse en adresse IPv6, suivant le formalisme présenté en relation avec la figure 4 et garde cette information dans son cache.

On notera que l'exemple de la **figure 4** n'est qu'un mode de réalisation, l'essentiel étant que l'adresse IPv4 du correspondant (ici le serveur Web) soit inscrite dans une adresse IPv6. Si aucune réponse n'est reçue de la part d'un serveur DNS, alors un message d'erreur est transmis au terminal demandeur.

Nous appellerons IPv6_remoteAddress_out_to_IPv4 l'adresse du destinataire (ici le serveur Web) ainsi transformée en IPv6. On notera que le terminal demandeur peut récupérer une adresse IPv6 de la machine distante à contacter par d'autres moyens, par exemple auprès d'un serveur.

Dans tous les cas, l'adresse IPv6 du correspondant (ici le serveur Web) peut être une adresse IPv6 native ou une adresse IPv6 respectant le formalisme introduit par la

présente invention. Dans le cas d'une adresse IPv6_remoteAddress_out_to_IPv4 construite, elle est incluse dans le préfixe IPv6/IPv4_Access_Node_Service_prefix.

En relation avec la **figure 4**, on remarque que la séquence de 2 octets la plus à droite est marquée "réservée" et mise à 0 par défaut. Cet emplacement correspond à celui des bits de ports dans une adresse IPv6 IPv4inIPv6_dest_address pour les paquets destinés à un terminal d'utilisateur. Il est réservé de manière à pouvoir indiquer un port sur lequel le correspondant (ici le serveur Web) désire se faire appeler en particulier. Il pourrait s'agir d'un correspondant IPv4 qui lui aussi se verrait affecté une adresse IPv4 partagée entre plusieurs correspondants et qui donc ne disposerait pas de tous les ports disponibles.

Le terminal 22 émet ensuite un paquet de données IPv6 comprenant l'adresse IPv6_remoteAddress_out_to_IPv4 comme adresse de destination.

La passerelle résidentielle 20 selon l'invention comprend un dispositif de réception d'un paquet de données selon l'invention. Sur réception de ce paquet IPv6, un tel

[redacted]

IPv4 selon le premier mode de réalisation de l'invention, qui va maintenant être décrit en référence à la **figure 5**.

Un tel procédé met en œuvre l'étape R1 d'identification de l'adresse de destination IPv6 précédemment décrite.

Selon un aspect de l'invention, la passerelle résidentielle 20 connaît la longueur du préfixe IPv4_Access_Node_Service_prefix pour aisément déterminer sa valeur en prenant les bits correspondants dans son IPv6 prefix ports range. Une telle identification consiste à classer comme une adresse construite une adresse IPv6 de destination qui s'inscrit dans le préfixe IPv6/IPv4_Access_Node_Service_prefix et à considérer toutes les adresses hors de ce préfixe comme des adresses natives.

Un avantage de cette identification est qu'elle est simple.

En relation avec la **figure 4**, on remarque que la séquence de 2 octets la plus à droite est marquée "réservée" et mise à 0 par défaut. Cet emplacement correspond à celui des bits de ports dans une adresse IPv6 IPv4inIPv6_dest_address pour les paquets destinés à un terminal d'utilisateur. Il est réservé de manière à pouvoir indiquer un port sur lequel le correspondant (ici le serveur Web) désire se faire appeler en particulier. Il pourrait s'agir d'un correspondant IPv4 qui lui aussi se verrait affecté une adresse IPv4 partagée entre plusieurs correspondants et qui donc ne disposerait pas de tous les ports disponibles.

Le terminal 22 émet ensuite un paquet de données IPv6 comprenant l'adresse IPv6_remoteAddress_out_to_IPv4 comme adresse de destination.

[redacted]

présente invention. Dans le cas d'une adresse IPv6_remoteAddress_out_to_IPv4 construite, elle est incluse dans le préfixe IPv6/IPv4_Access_Node_Service_prefix.

En relation avec la **figure 4**, on remarque que la séquence de 2 octets la plus à droite est marquée "réservée" et mise à 0 par défaut. Cet emplacement correspond à celui des bits de ports dans une adresse IPv6 IPv4inIPv6_dest_address pour les paquets destinés à un terminal d'utilisateur. Il est réservé de manière à pouvoir indiquer un port sur lequel le correspondant (ici le serveur Web) désire se faire appeler en particulier. Il pourrait s'agir d'un correspondant IPv4 qui lui aussi se verrait affecté une adresse IPv4 partagée entre plusieurs correspondants et qui donc ne disposerait pas de tous les ports disponibles.

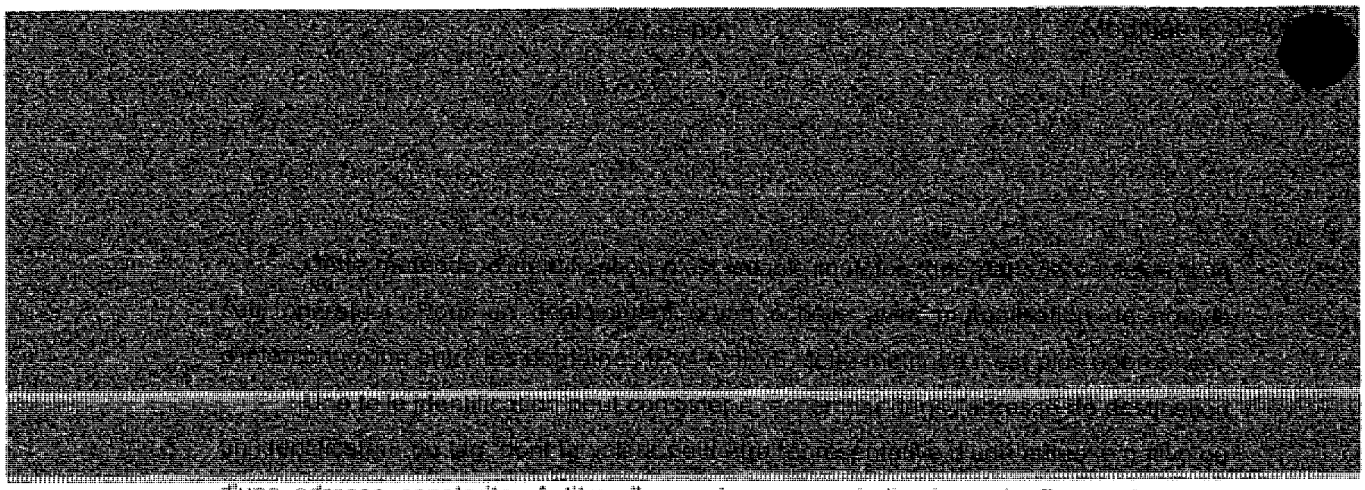
Le terminal 22 émet ensuite un paquet de données IPv6 comprenant l'adresse IPv6_remoteAddress_out_to_IPv4 comme adresse de destination.

La passerelle résidentielle 20 selon l'invention comprend un dispositif de réception d'un paquet de données selon l'invention. Sur réception de ce paquet IPv6, un tel dispositif est apte à mettre en œuvre le procédé de transmission d'un paquet IPv6 à destination d'une adresse IPv6 représentant une machine connectée à un domaine IPv4 selon le premier mode de réalisation de l'invention, qui va maintenant être décrit en référence à la **figure 5**.

Un tel procédé met en œuvre l'étape R1 d'identification de l'adresse de destination IPv6 précédemment décrite.

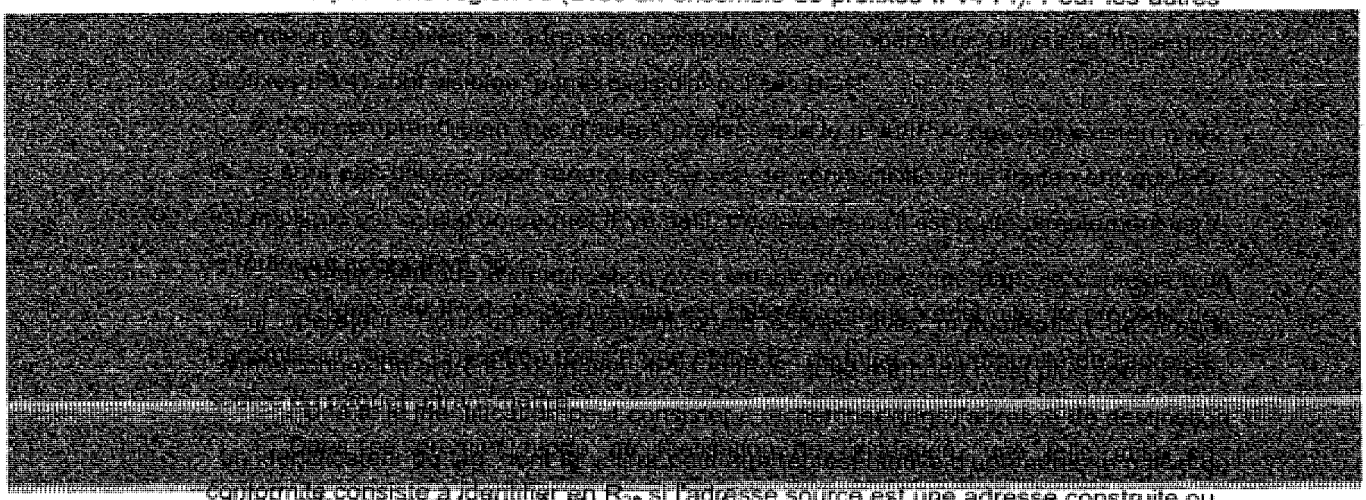
Selon un aspect de l'invention, la passerelle résidentielle 20 connaît la longueur du préfixe IPv4_Access_Node_Service_prefix, pour aisément déterminer sa valeur en prenant les bits correspondants dans son IPv6_prefix_ports_range. Une telle identification consiste à classer comme une adresse construite une adresse IPv6 de destination qui s'inscrit dans le préfixe IPv6/IPv4_Access_Node_Service_prefix et à considérer toutes les adresses hors de ce préfixe comme des adresses natives.

Un avantage de cette identification est qu'elle est simple.



d'une adresse construite. A titre d'exemple, comme indiqué sur la **figure 4**, un tel identificateur peut avoir une longueur d'un seul bit ADDR_TYPE_TAG, valorisé à 0 ou 1 pour indiquer qu'il s'agit d'une adresse native ou construite. L'identifiant ADDR_TYPE_TAG peut être positionné, par exemple, au début de l'adresse IPv6 construite pour faciliter les opérations de lecture, ou encore entre le IPv6/IPv4_Access_Node_Service_prefix et l'adresse IPv4.

Un avantage de l'identifiant ADDR_TYPE_TAG est qu'il permet une mutualisation des équipements d'interconnexion IPV4 IPv6 entre plusieurs opérateurs et donc un partage des coûts. Ainsi, un opérateur Oi peut assurer l'interconnexion IPv4-IPv6 pour une région Ri (avec un ensemble de préfixes IPv4 Pi). Pour les autres



conformité consiste à déterminer en R_{ij} si l'adresse source est une adresse construite ou native. Une adresse est considérée comme construite s'il s'agit d'une adresse IPv6 source qui s'inscrit dans le préfixe IPv6/IPv4_Access_Node_Service_prefix, toutes les adresses hors de ce préfixe étant considérées comme des adresses sources natives.

d'une adresse construite. A titre d'exemple, comme indiqué sur la **figure 4**, un tel identificateur peut avoir une longueur d'un seul bit ADDR_TYPE_TAG, valorisé à 0 ou 1 pour indiquer qu'il s'agit d'une adresse native ou construite. L'identifiant ADDR_TYPE_TAG peut être positionné, par exemple, au début de l'adresse IPv6 construite pour faciliter les opérations de lecture, ou encore entre le IPv6/IPv4_Access_Node_Service_prefix et l'adresse IPv4.

Un avantage de l'identifiant ADDR_TYPE_TAG est qu'il permet une mutualisation des équipements d'interconnexion IPV4 IPv6 entre plusieurs opérateurs

Cette méthode d'identification n'est valable toutefois que dans le contexte d'un seul opérateur. Pour un déploiement grand échelle avec mutualisation de nœuds d'interconnexion entre les domaines IPv4 et IPv6, cette méthode n'est plus appropriée.

Une telle identification peut consister à rechercher dans l'adresse de destination un identificateur ou tag, dont la valeur peut être représentative d'une adresse native ou d'une adresse construite. A titre d'exemple, comme indiqué sur la **figure 4**, un tel identificateur peut avoir une longueur d'un seul bit ADDR_TYPE_TAG, valorisé à 0 ou 1 pour indiquer qu'il s'agit d'une adresse native ou construite. L'identifiant ADDR_TYPE_TAG peut être positionné, par exemple, au début de l'adresse IPv6 construite pour faciliter les opérations de lecture, ou encore entre le IPv6/IPv4_Access_Node_Service_prefix et l'adresse IPv4.

Un avantage de l'identifiant ADDR_TYPE_TAG est qu'il permet une mutualisation des équipements d'interconnexion IPV4 IPv6 entre plusieurs opérateurs et donc un partage des coûts. Ainsi, un opérateur Oi peut assurer l'interconnexion IPv4-IPv6 pour une région Ri (avec un ensemble de préfixes IPv4 Pi). Pour les autres opérateurs Oj, seules les adresses construites par un opérateur Oi (sur la base des préfixes IPv4) sont visibles, par le biais d'annonces BGP.

On comprend bien que d'autres préfixes que le IPv6/IPv4 peuvent exister, mais ils ne sont pas utilisés pour rendre ce service de connectivité et le traitement qui leur est appliqué est celui d'un paquet IPv6 natif, c'est-à-dire qu'il est routé directement vers le routeur d'accès IPv6 30;

Si l'adresse IPv6 de destination est classée comme construite, le procédé de transmission selon l'invention réalise une étape R2 de mise en conformité de l'adresse source du paquet à transmettre.

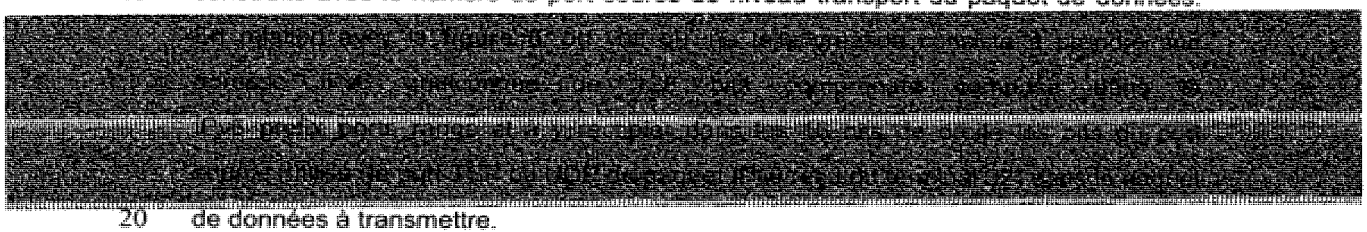
Dans ce premier mode de réalisation de l'invention, une telle mise en conformité consiste à identifier en R_{21} si l'adresse source est une adresse construite ou native. Une adresse est considérée comme construite s'il s'agit d'une adresse IPv6 source qui s'inscrit dans le préfixe IPv6/IPv4_Access_Node_Service_prefix, toutes les adresses hors de ce préfixe étant considérées comme des adresses sources natives.

Si l'identifiant ADDR_TYPE_TAG est utilisé, alors une adresse est identifiée comme construite si l'identifiant ADDR_TYPE_TAG est positionné à « 1 ».

Si l'adresse source est construite, le paquet de données est routé vers sa destination en R3.

Si l'adresse IPv6 source est classée comme native, le procédé selon l'invention met en œuvre, préalablement à cette étape de routage, une étape R_{22} destinée à choisir une adresse IPv6 source construite dont le numéro de port source est dans la plage autorisée ports_pattern/length_of_unvariable affectée à la passerelle 20 et à modifier le paquet de données en remplaçant l'adresse source native par cette adresse construite. En R_{24}, le procédé selon l'invention crée une entrée dans la table de traduction d'adresses de la passerelle, ladite entrée comprenant une association de l'adresse source native et de l'adresse source ainsi construite.

De façon avantageuse, le procédé selon l'invention peut en outre de vérifier en R_{23} une concordance du numéro de port source contenu dans l'adresse source construite avec le numéro de port source de niveau transport du paquet de données.



de données à transmettre.

On comprendra que cette étape est nécessaire pour que le nœud d'accès IPv6/IPv4 40 puisse traduire le paquet de données IPv6 en un paquet de données IPv4 avant de le router vers le domaine IPv4 destinataire. Elle présente un autre avantage dans le cas où l'adresse IPv4 affectée à la passerelle résidentielle 20 est une adresse partagée par plusieurs passerelles résidentielles du domaine IPv6 1. En effet, comme évoqué précédemment, la passerelle résidentielle 20 ne peut utiliser que les numéros de port source appartenant à une plage de numéros de port restreinte qui lui a été réservée.

Si l'identifiant ADDR_TYPE_TAG est utilisé, alors une adresse est identifiée comme construite si l'identifiant ADDR_TYPE_TAG est positionné à « 1 ».

Si l'adresse source est construite, le paquet de données est routé vers sa destination en R3.

Si l'adresse IPv6 source est classée comme native, le procédé selon l'invention met en œuvre, préalablement à cette étape de routage, une étape R_{22} destinée à choisir une adresse IPv6 source construite dont le numéro de port source est dans la plage autorisée ports_pattern/length_of_unvariable affectée à la passerelle 20 et à modifier le paquet de données en remplaçant l'adresse source native par cette adresse construite. En R_{24}, le procédé selon l'invention crée une entrée dans la table de traduction d'adresses de la passerelle, ladite entrée comprenant une association de l'adresse source native et de l'adresse source ainsi construite.

De façon avantageuse, le procédé selon l'invention peut en outre de vérifier en

Si l'identifiant ADDR_TYPE_TAG est utilisé, alors une adresse est identifiée comme construite si l'identifiant ADDR_TYPE_TAG est positionné à « 1 ».

Si l'adresse source est construite, le paquet de données est routé vers sa destination en R3.

Si l'adresse IPv6 source est classée comme native, le procédé selon l'invention met en œuvre, préalablement à cette étape de routage, une étape R_{22} destinée à choisir une adresse IPv6 source construite dont le numéro de port source est dans la plage autorisée ports_pattern/length_of_unvariable affectée à la passerelle 20 et à modifier le paquet de données en remplaçant l'adresse source native par cette adresse construite. En R_{24}, le procédé selon l'invention crée une entrée dans la table de traduction d'adresses de la passerelle, ladite entrée comprenant une association de l'adresse source native et de l'adresse source ainsi construite.

De façon avantageuse, le procédé selon l'invention peut en outre de vérifier en R_{23} une concordance du numéro de port source contenu dans l'adresse source construite avec le numéro de port source de niveau transport du paquet de données. En relation avec la **figure 6**, on voit qu'une telle création consiste à prendre une adresse IPv6 quelconque de 128 bits comprenant comprise dans le IPv6_prefix_ports_range et à y recopier dans les 16 bits de droite les bits du port source utilisé (le port TCP ou UDP du paquet IPv6 reçu du terminal 22) dans le paquet de données à transmettre.

On comprendra que cette étape est nécessaire pour que le nœud d'accès IPv6/IPv4 40 puisse traduire le paquet de données IPv6 en un paquet de données IPv4 avant de le router vers le domaine IPv4 destinataire. Elle présente un autre avantage dans le cas où l'adresse IPv4 affectée à la passerelle résidentielle 20 est une adresse partagée par plusieurs passerelles résidentielles du domaine IPv6 1. En effet, comme évoqué précédemment, la passerelle résidentielle 20 ne peut utiliser que les numéros de port source appartenant à une plage de numéros de port restreinte qui lui a été réservée.

On notera également que si la passerelle résidentielle 20 a bien contraint le port source à être dans la plage de numéros de ports autorisés ports_pattern/length_of_unvariable, alors l'adresse source construite:

- est inscrite dans le préfixe IPv6_prefix_ports_range; et
- ses 16 derniers bits sont identiques au numéro de port source du paquet IPv6 reçu du terminal par la passerelle;

Dans la suite, on appellera IPv6_address_source_ports_range l'adresse source IPv6 ainsi formée.

En R3, le paquet IPv6 comprenant l'adresse IPv6 source contrainte IPv6_address_source_ports_range est ensuite routé vers le routeur d'accès IPv6 30 qui dessert la passerelle.

Le routeur d'accès IPv6 30 vérifie que l'adresse source IPv6 IPv6_address_source_ports_range est bien autorisée pour la passerelle résidentielle 20. Il vérifie en d'autres termes qu'il n'y a pas de "spoofing", c'est-à-dire que la passerelle résidentielle 20 émet bien des paquets IPv6 dans son préfixe IPv6_prefix_ports_range autorisé. Pour cela le routeur d'accès IPv6 30 vérifie que l'adresse source IPv6 IPv6_address_source_ports_range du paquet IPv6 reçu de la passerelle 20 est bien inscrite dans le préfixe IPv6_prefix_ports_range affecté à cette passerelle résidentielle. Cette vérification est effectuée de façon classique selon un principe déjà utilisé pour le trafic IPv6 natif.

24

Si cette vérification est positive, le routeur d'accès IPv6 30 route le paquet IPv6 vers sa destination.

On notera également que si la passerelle résidentielle 20 a bien contraint le port source à être dans la plage de numéros de ports autorisés ports_pattern/length_of_unvariable, alors l'adresse source construite:

- est inscrite dans le préfixe IPv6_prefix_ports_range; et
- ses 16 derniers bits sont identiques au numéro de port source du paquet IPv6 reçu du terminal par la passerelle;

Dans la suite, on appellera IPv6_address_source_ports_range l'adresse source IPv6 ainsi formée.

En R3, le paquet IPv6 comprenant l'adresse IPv6 source contrainte IPv6_address_source_ports_range est ensuite routé vers le routeur d'accès IPv6 30 qui dessert la passerelle.

Le routeur d'accès IPv6 30 vérifie que l'adresse source IPv6 IPv6_address_source_ports_range est bien autorisée pour la passerelle résidentielle

Puisque l'adresse IPv6 de destination s'inscrit dans le préfixe IPv6/IPv4 Access Node prefix caractérisant le nœud d'accès IPv6/IPv4 Access Node 40 au domaine IPv6, le paquet de données est routé vers ce nœud d'accès. On suppose, par exemple, qu'un tel nœud est placé dans le domaine IPv6 1 au plus près du ou des domaines IPv4 qu'il dessert, afin d'optimiser le routage des paquets de données vers ces domaines, mais l'invention ne se limite pas à une telle situation du nœud d'accès 40, ledit nœud d'accès pouvant être situé n'importe où dans le domaine 1.

On notera également que si la passerelle résidentielle 20 a bien contraint le port source à être dans la plage de numéros de ports autorisés ports_pattern/length_of_unvariable, alors l'adresse source construite:

- est inscrite dans le préfixe IPv6_prefix_ports_range; et
- ses 16 derniers bits sont identiques au numéro de port source du paquet IPv6 reçu du terminal par la passerelle;

Dans la suite, on appellera IPv6_address_source_ports_range l'adresse source IPv6 ainsi formée.

En R3, le paquet IPv6 comprenant l'adresse IPv6 source contrainte IPv6_address_source_ports_range est ensuite routé vers le routeur d'accès IPv6 30 qui dessert la passerelle.

Le routeur d'accès IPv6 30 vérifie que l'adresse source IPv6 IPv6_address_source_ports_range est bien autorisée pour la passerelle résidentielle 20. Il vérifie en d'autres termes qu'il n'y a pas de "spoofing", c'est-à-dire que la passerelle résidentielle 20 émet bien des paquets IPv6 dans son préfixe IPv6_prefix_ports_range autorisé. Pour cela le routeur d'accès IPv6 30 vérifie que l'adresse source IPv6 IPv6_address_source_ports_range du paquet IPv6 reçu de la passerelle 20 est bien inscrite dans le préfixe IPv6_prefix_ports_range affecté à cette passerelle résidentielle. Cette vérification est effectuée de façon classique selon un principe déjà utilisé pour le trafic IPv6 natif.

Si cette vérification est positive, le routeur d'accès IPv6 30 route le paquet IPv6 vers sa destination.

Puisque l'adresse IPv6 de destination s'inscrit dans le préfixe IPv6/IPv4_Access_Node_prefix caractérisant le nœud d'accès IPv6/IPv4_Access_Node 40 au domaine IPv6, le paquet de données est routé vers ce nœud d'accès. On suppose, par exemple, qu'un tel nœud est placé dans le domaine IPv6 1 au plus près du ou des domaines IPv4 qu'il dessert, afin d'optimiser le routage des paquets de données vers ces domaines, mais l'invention ne se limite pas à une telle situation du nœud d'accès 40, ledit nœud d'accès pouvant être situé n'importe où dans le domaine 1.

Sur réception du paquet IPv6, le nœud d'accès IPv6/IPv4_Access_Node 40 achemine le paquet de données sortant à destination d'un domaine IPv4 de la façon suivante :

- Il extrait une adresse de destination IPv4 et d'un port de destination de l'adresse de destination IPv6 et une adresse source IPv4 et d'un port source de l'adresse source IPv6 ;
- Il traduit ensuite le paquet IPv6 en un paquet IPv4 qui a les caractéristiques suivantes :
  - son adresse source IPv4 est l'adresse IPv4 Shared_@IPv4 de la passerelle résidentielle 20. C'est cette adresse Shared_@IPv4 que verra le destinataire du paquet de données IPv4 transmis (le serveur Web). Pour rappel, cette adresse IPv4 Shared_@IPv4 est incluse dans le préfixe IPv6_prefix_ports_range et donc dans l'adresse IPv6 source IPv6_address_source_ports_range. En relation avec la figure 8, l'adresse IPv4 Shared_@IPv4 peut être extraite des bits 24 à 55 ;
  - son adresse de destination IPv4 est l'adresse IPv4 du correspondant. En relation avec la figure 4, l'adresse IPv4 du destinataire peut être extraite des bits 24 à 55 de l'adresse IPv6_remoteAddress_out_to_IPv4 du paquet de données IPv6 reçu par le nœud d'accès 40 ;
  - la valeur du numéro de port source du paquet de données IPv4 traduit est le numéro du port source du paquet IPv6 reçu ;
  - le numéro de port de destination du paquet de données IPv4 traduit est le même que celui du paquet IPv6 ;
  - la partie utile du paquet IPv6 est la partie utile du paquet IPv4 traduit.

On notera que les champs de l'en-tête du paquet IPv6 sont traduits en champs IPv4 correspondant de façon classique, par exemple selon les principes du standard NAT-PT (*Network Address Translation- Protocol Translation*).

- Il route enfin le paquet IPv4 traduit vers son destinataire (le serveur Web IPv4, dans notre exemple).

Sur réception du paquet IPv6, le nœud d'accès IPv6/IPv4_Access_Node 40 achemine le paquet de données sortant à destination d'un domaine IPv4 de la façon suivante :

- Il extrait une adresse de destination IPv4 et d'un port de destination de l'adresse de destination IPv6 et une adresse source IPv4 et d'un port source de l'adresse source IPv6 ;
- Il traduit ensuite le paquet IPv6 en un paquet IPv4 qui a les caractéristiques suivantes :
  - son adresse source IPv4 est l'adresse IPv4 Shared_@IPv4 de la passerelle résidentielle 20. C'est cette adresse Shared_@IPv4 que verra le destinataire du paquet de données IPv4 transmis (le serveur Web). Pour rappel, cette adresse IPv4 Shared_@IPv4 est incluse dans le préfixe IPv6_prefix_ports_range et donc dans l'adresse IPv6 source IPv6_address_source_ports_range. [illegible]

Sur réception du paquet IPv6, le nœud d'accès IPv6/IPv4_Access_Node 40 achemine le paquet de données sortant à destination d'un domaine IPv4 de la façon suivante :

- Il extrait une adresse de destination IPv4 et d'un port de destination de l'adresse de destination IPv6 et une adresse source IPv4 et d'un port source de l'adresse source IPv6 ;
- Il traduit ensuite le paquet IPv6 en un paquet IPv4 qui a les caractéristiques suivantes :
  - o son adresse source IPv4 est l'adresse IPv4 Shared_@IPv4 de la passerelle résidentielle 20. C'est cette adresse Shared_@IPv4 que verra le destinataire du paquet de données IPv4 transmis (le serveur Web). Pour rappel, cette adresse IPv4 Shared_@IPv4 est incluse dans le préfixe IPv6_prefix_ports_range et donc dans l'adresse IPv6 source IPv6_address_source_ports_range. En relation avec la figure 8, l'adresse IPv4 Shared_@IPv4 peut être extraite des bits 24 à 55 ;
  - o son adresse de destination IPv4 est l'adresse IPv4 du correspondant. En relation avec la figure 4, l'adresse IPv4 du destinataire peut être extraite des bits 24 à 55 de l'adresse IPv6_remoteAddress_out_to_IPv4 du paquet de données IPv6 reçu par le nœud d'accès 40 ;
  - o la valeur du numéro de port source du paquet de données IPv4 traduit est le numéro du port source du paquet IPv6 reçu ;
  - o le numéro de port de destination du paquet de données IPv4 traduit est le même que celui du paquet IPv6 ;
  - o la partie utile du paquet IPv6 est la partie utile du paquet IPv4 traduit;

On notera que les champs de l'en-tête du paquet IPv6 sont traduits en champs IPv4 correspondant de façon classique, par exemple selon les principes du standard NAT-PT (*Network Address Translation- Protocol Translation*).

- Il route enfin le paquet IPv4 traduit vers son destinataire (le serveur Web IPv4 dans notre exemple).

On comprend que, lorsque l'adresse IPv4 affectée à la passerelle résidentielle 20 est une adresse publique partagée entre plusieurs passerelles, il est nécessaire que le numéro de port source contenu dans l'adresse IPv6 source construite du paquet de données reçu appartienne bien à la plage de numéros de ports réservés à cette passerelle. En effet, si ce n'était pas le cas, le nœud d'accès pourrait traduire le paquet IPv6 à transmettre en un paquet de données IPv4, mais les éventuels paquets de réponse émis par le destinataire ne parviendraient pas à la passerelle résidentielle.

De façon avantageuse, le nœud d'accès 40 contrôle l'appartenance du port source à la plage de numéros de ports source affectée à la passerelle 20. Une telle étape consiste à contrôler que les derniers 16 bits de l'adresse source IPv6 du paquet sont identiques aux 16 bits du port source dans le champ correspondant TCP ou UDP du paquet IPv6. Il s'agit d'un contrôle indirect, qui peut faire suite à la vérification par le routeur d'accès du fait que la passerelle résidentielle a bien envoyé un paquet dont l'adresse source est dans son préfixe. A l'issue de ces deux étapes, on peut être certain que la passerelle résidentielle 20 a bien émis un paquet de données comprenant un port source inclus dans sa plage de ports autorisés et n'a pas utilisé celle d'une autre passerelle résidentielle.

Selon un deuxième mode de réalisation de l'invention, on considère le cas d'un paquet de données IPv4-in-pt entrant dans un domaine IPv6 en provenance d'un domaine IPv4 et destiné à un terminal d'utilisateur du domaine IPv6 1, par exemple le terminal 21. Le terminal se situe derrière la passerelle résidentielle 20 qui dispose d'une adresse IPv4 @IPv4 ou Shared @IPv4 et d'une plage de ports autorisés ports_pattern/length_of_unvariable.

Le paquet IPv4-in-pt entrant, s'il est destiné au terminal d'utilisateur 21 du réseau résidentiel de la passerelle résidentielle 20, comprend une adresse de destination IPv4 égale à Shared @IPv4 et un port de destination s'inscrivant dans la plage de numéros de ports autorisés ports_pattern/length_of_unvariable de la passerelle résidentielle 20.

On comprend que, lorsque l'adresse IPv4 affectée à la passerelle résidentielle 20 est une adresse publique partagée entre plusieurs passerelles, il est nécessaire que le numéro de port source contenu dans l'adresse IPv6 source construite du paquet de données reçu appartienne bien à la plage de numéros de ports réservés à cette passerelle. En effet, si ce n'était pas le cas, le nœud d'accès pourrait traduire le paquet IPv6 à transmettre en un paquet de données IPv4, mais les éventuels paquets de réponse émis par le destinataire ne parviendraient pas à la passerelle résidentielle.

De façon avantageuse, le nœud d'accès 40 contrôle l'appartenance du port source à la plage de numéros de ports source affectée à la passerelle 20. Une telle étape consiste à contrôler que les derniers 16 bits de l'adresse source IPv6 du paquet sont identiques aux 16 bits du port source dans le champ correspondant TCP ou UDP du paquet IPv6. Il s'agit d'un contrôle indirect, qui peut faire suite à la vérification par le routeur d'accès du fait que la passerelle résidentielle a bien envoyé un paquet dont l'adresse source est dans son préfixe. A l'issue

On comprend que, lorsque l'adresse IPv4 affectée à la passerelle résidentielle 20 est une adresse publique partagée entre plusieurs passerelles, il est nécessaire que le numéro de port source contenu dans l'adresse IPv6 source construite du paquet de données reçu appartienne bien à la plage de numéros de ports réservés à cette passerelle. En effet, si ce n'était pas le cas, le nœud d'accès pourrait traduire le paquet IPv6 à transmettre en un paquet de données IPv4, mais les éventuels paquets de réponse émis par le destinataire ne parviendraient pas à la passerelle résidentielle.

De façon avantageuse, le nœud d'accès 40 contrôle l'appartenance du port source à la plage de numéros de ports source affectée à la passerelle 20. Une telle étape consiste à contrôler que les derniers 16 bits de l'adresse source IPv6 du paquet sont identiques aux 16 bits du port source dans le champ correspondant TCP ou UDP du paquet IPv6. Il s'agit d'un contrôle indirect, qui peut faire suite à la vérification par le routeur d'accès du fait que la passerelle résidentielle a bien envoyé un paquet dont l'adresse source est dans son préfixe. A l'issue de ces deux étapes, on peut être certain que la passerelle résidentielle 20 a bien émis un paquet de données comprenant un port source inclus dans sa plage de ports autorisés et n'a pas utilisé celle d'une autre passerelle résidentielle.

Selon un deuxième mode de réalisation de l'invention, on considère le cas d'un paquet de données IPv4-in-pt entrant dans un domaine IPv6 en provenance d'un domaine IPv4 et destiné à un terminal d'utilisateur du domaine IPv6 1, par exemple le terminal 21. Le terminal se situe derrière la passerelle résidentielle 20 qui dispose d'une adresse IPv4 @IPv4 ou Shared_@IPv4 et d'une plage de ports autorisés ports_pattern/length_of_unvariable.

Le paquet IPv4-in-pt entrant, s'il est destiné au terminal d'utilisateur 21 du réseau résidentiel de la passerelle résidentielle 20, comprend une adresse de destination IPv4 égale à Shared_@IPv4 et un port de destination s'inscrivant dans la plage de numéros de ports autorisés ports_pattern/length_of_unvariable de la passerelle résidentielle 20.

Comme évoqué précédemment en relation avec la **figure 2**, l'adresse Shared_@IPv4 et la plage de numéros de ports ports_pattern/lenght_of_unvariable se retrouvent dans le préfixe IPv6_prefix_ports_range de la passerelle résidentielle 20.

Le paquet IPv4-in-pt est reçu par le nœud d'accès 40. En effet, dans une étape préalable, le fournisseur de connectivité IP a annoncé aux domaines IPv4 avec lesquels il a une interface, les adresses IPv4 affectées à des passerelles résidentielles du domaine 1 à destination desquelles il avait la charge d'acheminer les paquets IPv4. Il a fait cette annonce, soit par l'intermédiaire du nœud d'accès 40 lui-même ou d'un ASBR (Autonomous System Border Router) selon une technique connue de l'homme de métier.

Le paquet IPv4-in-pt comprend une adresse de destination @IPv4 ou shared@IPv4 gérée par le nœud d'accès 40 et un port de destination dest-port. Le nœud d'accès 40 est apte à construire une adresse de destination IPv6 IPv4inIPv6_dest_address par concaténation d'un préfixe IPv6/IPv4_Access_Node_prefix du nœud d'accès 40, de ladite adresse de destination IPv4 shared-@IPv4 et du numéro de port de destination dest-port, comme décrit en relation avec la **figure 7**.

27

Le numéro de port de destination dest-port est inséré dans la partie droite de l'adresse de destination IPv6 construite. Il insère donc à la fois les 32 bits de l'adresse IPv4 de destination du paquet IPv4 reçu et les 16 bits du port de destination dest-port pour constituer une adresse IPv6 de destination construite que nous appelons IPv4inIPv6_dest_address.

Comme évoqué précédemment en relation avec la **figure 2**, l'adresse Shared_@IPv4 et la plage de numéros de ports ports_pattern/lenght_of_unvariable se retrouvent dans le préfixe IPv6_prefix_ports_range de la passerelle résidentielle 20.

Le paquet IPv4-in-pt est reçu par le nœud d'accès 40. En effet, dans une étape préalable, le fournisseur de connectivité IP a annoncé aux domaines IPv4 avec lesquels il a une interface, les adresses IPv4 affectées à des passerelles résidentielles du domaine 1 à destination desquelles il avait la charge d'acheminer les paquets IPv4. Il a fait cette annonce, soit par l'intermédiaire du nœud d'accès 40 lui-même ou d'un ASBR (Autonomous System Border Router) selon une technique connue de l'homme de métier.

Le nœud d'accès 40 génère ensuite un paquet de données IPv6 IPv4inIPv6-pt à partir de l'adresse de destination IPv6 IPv4inIPv6_dest_address construite et du paquet de données IPv4 reçu. Un mode de réalisation consiste à traduire le paquet IPv4 reçu dans un paquet IPv6:

- dont l'adresse source IPv6 est une des adresses IPv6 dont dispose l'IPv6/IPv4_Access_Node 40 en propre (pour une de ses interfaces),
- et dont l'adresse de destination IPv6 est l'adresse IPv4inIPv6_dest_address.

Le paquet IPv4-in-pt comprend une adresse de destination @IPv4 ou shared@IPv4 gérée par le nœud d'accès 40 et un port de destination dest-port. Le nœud d'accès 40 est apte à construire une adresse de destination IPv6 IPv4inIPv6_dest_address par concaténation d'un préfix

Comme évoqué précédemment en relation avec la **figure 2**, l'adresse Shared_@IPv4 et la plage de numéros de ports ports_pattern/lenght_of_unvariable se retrouvent dans le préfixe IPv6_prefix_ports_range de la passerelle résidentielle 20.

Le paquet IPv4-in-pt est reçu par le nœud d'accès 40. En effet, dans une étape préalable, le fournisseur de connectivité IP a annoncé aux domaines IPv4 avec lesquels il a une interface, les adresses IPv4 affectées à des passerelles résidentielles du domaine 1 à destination desquelles il avait la charge d'acheminer les paquets IPv4. Il a fait cette annonce, soit par l'intermédiaire du nœud d'accès 40 lui-même ou d'un ASBR (Autonomous System Border Router) selon une technique connue de l'homme de métier.

Le paquet IPv4-in-pt comprend une adresse de destination @IPv4 ou shared@IPv4 gérée par le nœud d'accès 40 et un port de destination dest-port. Le nœud d'accès 40 est apte à construire une adresse de destination IPv6 IPv4inIPv6_dest_address par concaténation d'un préfixe IPv6/IPv4_Access_Node_prefix du nœud d'accès 40, de ladite adresse de destination IPv4 shared-@IPv4 et du numéro de port de destination dest-port, comme décrit en relation avec la **figure 7**.

Le numéro de port de destination dest-port est inséré dans la partie droite de l'adresse de destination IPv6 construite. Il insère donc à la fois les 32 bits de l'adresse IPv4 de destination du paquet IPv4 reçu et les 16 bits du port de destination dest-port pour constituer une adresse IPv6 de destination construite que nous appelons IPv4inIPv6_dest_address.

Le nœud d'accès 40 génère ensuite un paquet de données IPv6 IPv4inIPv6-pt à partir de l'adresse de destination IPv6 IPv4inIPv6_dest_address construite et du paquet de données IPv4 reçu. Un mode de réalisation consiste à traduire le paquet IPv4 reçu dans un paquet IPv6:

- dont l'adresse source IPv6 est une des adresses IPv6 dont dispose l'IPv6/IPv4_Access_Node 40 en propre (pour une de ses interfaces);
- et dont l'adresse de destination IPv6 est l'adresse IPv4inIPv6_dest_address.

Un autre mode de réalisation consiste à traduire le paquet IPv4 IPv4-in-pt reçu en un paquet IPv6 auquel on associe l'adresse IPv6 construite après avoir préalablement extrait du paquet IPv4 reçu son adresse IPv4 de destination, son port de destination, son adresse IPv4 source et son port source.

Le paquet de données IPv6 IPv4inIPv6-pt généré à l'aide de l'adresse de destination IPv6 construite est routé dans le domaine IPv6 1. Le paquet IPv4inIPv6-pt passe donc dans le cœur de routage IPv6 du nœud d'accès 40 IPv6/IPv4_Access_Node.

Par construction, son adresse de destination IPv4inIPv6_dest_address s'inscrit dans le préfixe IPv6_prefix_ports_range de la passerelle résidentielle 20. Le paquet IPv4inIPv6-pt est routé vers l'interface du nœud d'accès IPv6/IPv4_Access_Node 40 qui dessert la route IPv6 correspondante vers de la passerelle résidentielle 20.

On notera que si l'adresse de destination IPv4inIPv6_dest_address ne s'inscrivait dans aucun préfixe IPv6_prefix_ports_range (ou aucun préfixe englobant), le paquet serait détruit à un moment à un autre sur la route, car il ne pourrait être routé vers aucun préfixe IPv6_prefix_ports_range et donc vers aucune passerelle résidentielle.

28

Si l'adresse de destination IPv4inIPv6_dest_address s'inscrit bien dans le préfixe IPv6_prefix_ports_range, le paquet IPv4inIPv6-pt parvient au routeur_d'acces_dual_stack 30 desservant la passerelle résidentielle 20 qui héberge le terminal d'utilisateur 21 dans son réseau résidentiel 2. Il est routé par le routeur d'acces dual stack 30 vers la passerelle résidentielle, lequel connaît la route vers le préfixe IPv6 prefix ports range.

Selon ce deuxième mode de réalisation de l'invention, la passerelle résidentielle 20 comprend un dispositif mettant en œuvre le procédé de réception du paquet de données IPv4inIPv6-pt selon l'invention. Un tel procédé va maintenant être décrit en relation avec la **figure 8**.

Lorsque le paquet IPv4inIPv6-pt parvient à la passerelle résidentielle 20, celle-ci met en œuvre l'étape R'1 d'identification de l'adresse de destination précédemment décrite.

Un autre mode de réalisation consiste à traduire le paquet IPv4 IPv4-in-pt reçu en un paquet IPv6 auquel on associe l'adresse IPv6 construite après avoir préalablement extrait du paquet IPv4 reçu son adresse IPv4 de destination, son port de destination, son adresse IPv4 source et son port source.

Le paquet de données IPv6 IPv4inIPv6-pt généré à l'aide de l'adresse de destination IPv6 construite est routé dans le domaine IPv6 1. Le paquet IPv4inIPv6-pt passe donc dans le cœur de routage IPv6 du nœud d'accès 40 IPv6/IPv4_Access_Node.

Par construction, son adresse de destination IPv4inIPv6_dest_address s'inscrit dans le préfixe IPv6_prefix_ports_range de la passerelle résidentielle 20. Le paquet IPv4inIPv6-pt est routé vers l'interface du nœud d'accès IPv6/IPv4_Access_Node 40 qui dessert la route IPv6 correspondante vers de la passerelle résidentielle 20.

On notera que si l'adresse de destination IPv4inIPv6_dest_address ne s'inscrivait dans aucun préfixe IPv6_prefix_ports_range (ou aucun préfixe englobant),

Un autre mode de réalisation consiste à traduire le paquet IPv4 IPv4-in-pt reçu en un paquet IPv6 auquel on associe l'adresse IPv6 construite après avoir préalablement extrait du paquet IPv4 reçu son adresse IPv4 de destination, son port de destination, son adresse IPv4 source et son port source.

Le paquet de données IPv6 IPv4inIPv6-pt généré à l'aide de l'adresse de destination IPv6 construite est routé dans le domaine IPv6 1. Le paquet IPv4inIPv6-pt passe donc dans le cœur de routage IPv6 du nœud d'accès 40 IPv6/IPv4_Access_Node.

Par construction, son adresse de destination IPv4inIPv6_dest_address s'inscrit dans le préfixe IPv6_prefix_ports_range de la passerelle résidentielle 20. Le paquet IPv4inIPv6-pt est routé vers l'interface du nœud d'accès IPv6/IPv4_Access_Node 40 qui dessert la route IPv6 correspondante vers de la passerelle résidentielle 20.

On notera que si l'adresse de destination IPv4inIPv6_dest_address ne s'inscrivait dans aucun préfixe IPv6_prefix_ports_range (ou aucun préfixe englobant), le paquet serait détruit à un moment à un autre sur la route, car il ne pourrait être routé vers aucun préfixe IPv6_prefix_ports_range et donc vers aucune passerelle résidentielle.

Si l'adresse de destination IPv4inIPv6_dest_address s'inscrit bien dans le préfixe IPv6_prefix_ports_range, le paquet IPv4inIPv6-pt parvient au routeur_d'acces_dual_stack 30 desservant la passerelle résidentielle 20 qui héberge le terminal d'utilisateur 21 dans son réseau résidentiel 2. Il est routé par le routeur_d'acces_dual_stack 30 vers la passerelle résidentielle, lequel connaît la route vers le préfixe IPv6_prefix_ports_range.

Selon ce deuxième mode de réalisation de l'invention, la passerelle résidentielle 20 comprend un dispositif mettant en œuvre le procédé de réception du paquet de données IPv4inIPv6-pt selon l'invention. Un tel procédé va maintenant être décrit en relation avec la **figure 8**.

Lorsque le paquet IPv4inIPv6-pt parvient à la passerelle résidentielle 20, celle-ci met en œuvre l'étape R'1 d'identification de l'adresse de destination précédemment décrite.

Si une adresse de destination native est identifiée, le paquet de données est routé directement vers le terminal d'utilisateur destinataire, dans une étape R'3.

Si une adresse de destination construite est identifiée, par exemple à l'aide d'un identifiant compris dans l'adresse de destination, l'étape de mise en conformité du procédé de réception d'un paquet de données selon l'invention comprend une étape R'_{21} de recherche dans la table de traduction de la passerelle résidentielle d'une entrée comprenant l'adresse de destination construite. Si cette recherche est positive, une telle entrée associe à l'adresse de destination construite une adresse de destination native IPv6_address_native-UE du terminal destinataire. En R'_{23}, le procédé selon l'invention remplace l'adresse de destination construite par cette adresse native dans le paquet de données IPv6. Ce remplacement est particulièrement avantageux dans le cas où le paquet de données IPv4-in-pt fait partie d'une réponse à un paquet de données émis préalablement par le terminal destinataire 21 avec son adresse source IPv6 native, et pour lequel la passerelle avait en effet préalablement stocké cette adresse native dans sa table de NAT avant sa transmission, comme décrit dans le mode de réalisation précédent de l'invention. A ce moment-là, elle avait crée l'entrée dans sa table de traduction et remplacé cette adresse native par l'adresse construite du terminal 21, afin de permettre au nœud d'accès 40 d'en extraire une adresse source IPv4 lors de la transformation du paquet IPv6 sortant en un paquet IPv4.

29

De façon avantageuse, l'étape de mise en conformité comprend en outre une étape R'22 de vérification d'une concordance du port de destination de niveau transport du paquet de données avec le numéro de port de destination contenu dans l'adresse de destination du paquet. Si les deux numéros de port ne concordent pas, le paquet est rejeté. Ceci ne doit pas avoir lieu si la traduction a été effectuée par le nœud d'accès, mais cette étape peut être utilisée pour réaliser un contrôle de flux en provenance du nœud d'accès.

En R'3, le paquet de données est routé par la passerelle vers le terminal destinataire de son réseau résidentiel.

Si une adresse de destination native est identifiée, le paquet de données est routé directement vers le terminal d'utilisateur destinataire, dans une étape R'3.

Si une adresse de destination construite est identifiée, par exemple à l'aide d'un identifiant compris dans l'adresse de destination, l'étape de mise en conformité du procédé de réception d'un paquet de données selon l'invention comprend une étape R'_{21} de recherche dans la table de traduction de la passerelle résidentielle d'une entrée comprenant l'adresse de destination construite. Si cette recherche est positive, une telle entrée associe à l'adresse de destination construite une adresse de destination native IPv6_address_native-UE du terminal destinataire. En R'_{23}, le procédé selon l'invention remplace l'adresse de destination construite par cette adresse native dans le paquet de données IPv6. Ce remplacement est particulièrement avantageux dans le cas où le paquet de données IPv4-in-pt fait partie d'une réponse à un paquet de données émis préalablement par le terminal destinataire 21 avec son adresse source IPv6 native, et pour lequel la passerelle avait en effet préalablement stocké cette

Si une adresse de destination native est identifiée, le paquet de données est routé directement vers le terminal d'utilisateur destinataire, dans une étape R'3.

Si une adresse de destination construite est identifiée, par exemple à l'aide d'un identifiant compris dans l'adresse de destination, l'étape de mise en conformité du procédé de réception d'un paquet de données selon l'invention comprend une étape R'_{21} de recherche dans la table de traduction de la passerelle résidentielle d'une entrée comprenant l'adresse de destination construite. Si cette recherche est positive, une telle entrée associe à l'adresse de destination construite une adresse de destination native IPv6_address_native-UE du terminal destinataire. En R'_{23}, le procédé selon l'invention remplace l'adresse de destination construite par cette adresse native dans le paquet de données IPv6. Ce remplacement est particulièrement avantageux dans le cas où le paquet de données IPv4-in-pt fait partie d'une réponse à un paquet de données émis préalablement par le terminal destinataire 21 avec son adresse source IPv6 native, et pour lequel la passerelle avait en effet préalablement stocké cette adresse native dans sa table de NAT avant sa transmission, comme décrit dans le mode de réalisation précédent de l'invention. A ce moment-là, elle avait crée l'entrée dans sa table de traduction et remplacé cette adresse native par l'adresse construite du terminal 21, afin de permettre au nœud d'accès 40 d'en extraire une adresse source IPv4 lors de la transformation du paquet IPv6 sortant en un paquet IPv4.

De façon avantageuse, l'étape de mise en conformité comprend en outre une étape R'22 de vérification d'une concordance du port de destination de niveau transport du paquet de données avec le numéro de port de destination contenu dans l'adresse de destination du paquet. Si les deux numéros de port ne concordent pas, le paquet est rejeté. Ceci ne doit pas avoir lieu si la traduction a été effectuée par le nœud d'accès, mais cette étape peut être utilisée pour réaliser un contrôle de flux en provenance du nœud d'accès.

En R'3, le paquet de données est routé par la passerelle vers le terminal destinataire de son réseau résidentiel.

Dans l'exemple décrit en relation avec la **figure 1**, la passerelle résidentielle 20 selon l'invention comporte un dispositif 25 de réception d'un paquet de données dans un domaine IPv6, qui va être maintenant décrit en relation avec la **figure 10**. Il comprend les éléments matériels que l'on retrouve classiquement dans un ordinateur conventionnel ou un routeur spécialisé, à savoir un processeur 25_1, une mémoire vive de type RAM 25_2, une mémoire morte de type ROM 25_3 et des moyens 25_4 de télécommunications avec le réseau 1.

Conformément à l'invention, le dispositif 25 comporte une mémoire 25_5 comprenant une base de données dans laquelle est stockée une table de traduction d'adresses ou NAT entre le domaine 1 et son réseau résidentiel 3.
On notera que cette mémoire peut aussi bien être externe au dispositif 25 pourvu qu'il puisse y accéder.

La mémoire morte 25_5 constitue un support d'enregistrement conforme à l'invention. Ce support mémorise le programme d'ordinateur conforme à l'invention. Ce programme comporte des instructions pour l'exécution des étapes du procédé de réception d'un paquet entrant conforme à l'invention qui vient d'être décrit en référence aux figures 3, 5 et 8.

30

On notera également que le dispositif de réception peut aussi bien être inclus dans un terminal d'utilisateur connecté directement au réseau 1 du fournisseur de service de connectivité.

Dans l'exemple décrit en relation avec la **figure 1**, la passerelle résidentielle 20 selon l'invention comporte un dispositif 25 de réception d'un paquet de données dans un domaine IPv6, qui va être maintenant décrit en relation avec la **figure 10**. Il comprend les éléments matériels que l'on retrouve classiquement dans un ordinateur conventionnel ou un routeur spécialisé, à savoir un processeur 25_1, une mémoire vive de type RAM 25_2, une mémoire morte de type ROM 25_3 et des moyens 25_4 de télécommunications avec le réseau 1.

Conformément à l'invention, le dispositif 25 comporte une mémoire 25_5 comprenant une base de données dans laquelle est stockée une table de traduction d'adresses ou NAT entre le domaine 1 et son réseau résidentiel 3.
On notera que cette mémoire peut aussi bien être externe au dispositif 25 pourvu qu'il puisse y accéder.

La mémoire morte 25_5 constitue un support d'enregistrement conforme à l'invention. Ce support mémorise le programme d'ordinateur conforme à l'invention. Ce

En résumé, l'invention permet une deuxième phase de migration des services de connectivité IP vers IPv6 à l'aide de mécanismes d'acheminement des paquets qui prennent en compte les faits suivants :

- La migration finale vers IPv6 prendrait plusieurs années (une échelle de 10 ans minimum). Ceci est dû principalement au nombre important des acteurs à « convaincre » pour un passage vers IPv6, le nombre important des AS (Autonomous System) (plus de 17000) ; de la diversité des mécanismes d'interconnexion. De plus, nous tenons à préciser que le problème des adresses ne concerne à priori que les opérateurs, les clients n'ont aucune raison de modifier l'architecture de leurs réseaux locaux. Une entreprise "Méchu" n'a pas de

Dans l'exemple décrit en relation avec la **figure 1**, la passerelle résidentielle 20 selon l'invention comporte un dispositif 25 de réception d'un paquet de données dans un domaine IPv6, qui va être maintenant décrit en relation avec la **figure 10**. Il comprend les éléments matériels que l'on retrouve classiquement dans un ordinateur conventionnel ou un routeur spécialisé, à savoir un processeur 25_1, une mémoire vive de type RAM 25_2, une mémoire morte de type ROM 25_3 et des moyens 25_4 de télécommunications avec le réseau 1.

Conformément à l'invention, le dispositif 25 comporte une mémoire 25_5 comprenant une base de données dans laquelle est stockée une table de traduction d'adresses ou NAT entre le domaine 1 et son réseau résidentiel 3.
On notera que cette mémoire peut aussi bien être externe au dispositif 25 pourvu qu'il puisse y accéder.

La mémoire morte 25_5 constitue un support d'enregistrement conforme à l'invention. Ce support mémorise le programme d'ordinateur conforme à l'invention. Ce programme comporte des instructions pour l'exécution des étapes du procédé de réception d'un paquet entrant conforme à l'invention qui vient d'être décrit en référence aux figures 3, 5 et 8.

On notera également que le dispositif de réception peut aussi bien être inclus dans un terminal d'utilisateur connecté directement au réseau 1 du fournisseur de service de connectivité.

En résumé, l'invention permet une deuxième phase de migration des services de connectivité IP vers IPv6 à l'aide de mécanismes d'acheminement des paquets qui prennent en compte les faits suivants :

- La migration finale vers IPv6 prendrait plusieurs années (une échelle de 10 ans minimum). Ceci est dû principalement au nombre important des acteurs à « convaincre » pour un passage vers IPv6, le nombre important des AS (Autonomous System) (plus de 17000) ; de la diversité des mécanismes d'interconnexion. De plus, nous tenons à préciser que le problème des adresses ne concerne à priori que les opérateurs. Les clients n'ont aucune raison pour modifier l'architecture de leurs réseaux locaux. Une entreprise "Méchu" n'a pas de

motivations pour migrer ses serveurs FTP, HTTP, etc. vers IPv6. Les opérateurs doivent s'attendre à un long travail d'accompagnement pour le passage vers IPv6 ;

- Les opérateurs de services souffrent d'un problème d'épuisement d'adresses IPv4 tel que décrit dans la section plus-haut ;
- La simple migration vers IPv6 d'un domaine donné ne résout pas le problème de la connectivité globale (joindre n'importe quelle machine distante présente sur Internet). En effet, une interconnexion avec le monde IPv4 doit être mise en place ;
- Une solution à base de NAT-PT avec état n'est pas recommandée. Le service fourni en serait dégradé, vu que les services à valeur ajoutée liés au « port forwarding » configuré par les clients ne fonctionneront pas et dépendront du comportement du « boitier » d'interconnexion entre un nuage IPv4 et un autre IPv6.

Les mécanismes d'acheminement des paquets IP selon l'invention permettent de promouvoir l'utilisation du protocole IPv6 de la façon suivante :

- activation d'IPv6 et mise en place d'une solution permettant de promouvoir le trafic IPv6 basée sur une fonction d'interconnexion placée dans le réseau, qui est sans état. La solution de l'invention n'utilise que la connectivité IPv6 des passerelles résidentielles et implique l'utilisation de terminaux d'utilisateurs et passerelles résidentielles IPv6. De ce fait ces équipements ne sont en mesure de traiter (recevoir et émettre) que des paquets de données de type IPv6.

31

La solution de l'invention permet :

- que le réseau d'accès ne soit qu'IPv6 et ainsi que l'opérateur d'accès n'ait pas à gérer le routage IPv4 à l'accès ;
- que les passerelles résidentielles n'aient aucune notion d'IPv4 et ne gèrent que l'IPv6 ;
- que les terminaux du réseau résidentiel de la passerelle résidentielle puissent n'utiliser qu'IPv6.

motivations pour migrer ses serveurs FTP, HTTP, etc. vers IPv6. Les opérateurs doivent s'attendre à un long travail d'accompagnement pour le passage vers IPv6 ;

- Les opérateurs de services souffrent d'un problème d'épuisement d'adresses IPv4 tel que décrit dans la section plus-haut ;

Une [illegible] IPv4 vers IPv6 affectant [illegible] ne résout pas le problème de connectivité globale (joindre n'importe quelle machine distante présente sur Internet). En effet, au niveau de la passerelle résidentielle IPv4, plusieurs [illegible] ;

- Une solution à base de NAT-PT avec état n'est pas recommandée. Le service fourni en serait dégradé, vu que les services à valeur ajoutée liés au « port forwarding » configuré par les clients ne fonctionneront pas et dépendront du comportement du « boitier » d'interconnexion entre un nuage IPv4 et un autre IPv6.

Les mécanismes d'acheminement des paquets IP selon l'invention permettent de promouvoir l'utilisation du protocole IPv6 de la façon suivante :

- activation d'IPv6 et mise en place d'une solution permettant de promouvoir le

résidentielles ne gèrent pas le routage IPv4. Les principes de bases sont les suivants :

- plage de ports source autorisés au niveau de chaque passerelle pour les communications sortantes ;

motivations pour migrer ses serveurs FTP, HTTP, etc. vers IPv6. Les opérateurs doivent s'attendre à un long travail d'accompagnement pour le passage vers IPv6 ;

- Les opérateurs de services souffrent d'un problème d'épuisement d'adresses IPv4 tel que décrit dans la section plus-haut ;
- La simple migration vers IPv6 d'un domaine donné ne résout pas le problème de la connectivité globale (joindre n'importe quelle machine distante présente sur Internet). En effet, une interconnexion avec le monde IPv4 doit être mise en place ;
- Une solution à base de NAT-PT avec état n'est pas recommandée. Le service fourni en serait dégradé, vu que les services à valeur ajoutée liés au « port forwarding » configuré par les clients ne fonctionneront pas et dépendront du comportement du « boitier » d'interconnexion entre un nuage IPv4 et un autre IPv6.

Les mécanismes d'acheminement des paquets IP selon l'invention permettent de promouvoir l'utilisation du protocole IPv6 de la façon suivante :

- activation d'IPv6 et mise en place d'une solution permettant de promouvoir le trafic IPv6 basée sur une fonction d'interconnexion placée dans le réseau, qui est sans état. La solution de l'invention n'utilise que la connectivité IPv6 des passerelles résidentielles et implique l'utilisation de terminaux d'utilisateurs et passerelles résidentielles IPv6. De ce fait ces équipements ne sont en mesure de traiter (recevoir et émettre) que des paquets de données de type IPv6.

La solution de l'invention permet :

- que le réseau d'accès ne soit qu'IPv6 et ainsi que l'opérateur d'accès n'ait pas à gérer le routage IPv4 à l'accès ;
- que les passerelles résidentielles n'aient aucune notion d'IPv4 et ne gèrent que l'IPv6 ;
- que les terminaux du réseau résidentiel de la passerelle résidentielle puissent n'utiliser qu'IPv6.

Une même adresse IPv4 peut être affectée à plusieurs passerelles résidentielles (ou autres équipements dans des contextes autres que l'accès Internet résidentiel). Il s'agit d'une affectation fictive au niveau de la passerelle résidentielle, puisque les passerelles résidentielles ne gèrent pas le routage IPv4. Les principes de bases sont les suivants :

- plage de ports source autorisés au niveau de chaque passerelle pour les communications sortantes ;

- préfixe IPv6 particulier IPv6_prefix_ports_range.

Les paquets IPv4 entrants dans le domaine IPv6 ne sont pas encapsulés par l'IPv6/IPv4_Access_Node pour être routés vers la passerelle résidentielle, mais ils sont traduits en paquets IPv6.

- Pour les communications sortantes, sur résolution DNS d'un correspondant IPv4, on retourne au terminal d'utilisateur initiateur une adresse IPv6 construite sur la base de l'adresse IPv4 du correspondant. Le terminal d'utilisateur utilise alors cette adresse de destination IPv6 pour émettre les paquets de données. Pour émettre ce paquet, il peut utiliser son adresse source IPv6 native ou construite.
- S'il a utilisé son adresse source native, la passerelle résidentielle transforme l'adresse IPv6 native source en une adresse source construite IPv6 contenant sa propre adresse IPv4 partagée entre les passerelles (Shared_@IPv4) et le port source (inscrit dans la plage source autorisée).
- Un équipement d'interconnexion du domaine IPv6 au domaine IPv4 vérifie que la passerelle résidentielle a bien utilisé sa plage de ports source autorisés en comparant la partie de l'adresse source qui contient les bits port source et le port source dans le champ port du paquet IPv6. Il traduit le paquet IPv6 en paquet IPv4 pour le transmettre au correspondant en utilisant :
  - pour l'adresse source IPv4 : les bits dans l'adresse IPv6 source qui contiennent Shared_@IPv4[32]
  - pour l'adresse destination IPv4 : les bits dans l'adresse IPv6 qui contiennent l'adresse IPv4 du correspondant.

- préfixe IPv6 particulier IPv6_prefix_ports_range.

Les paquets IPv4 entrants dans le domaine IPv6 ne sont pas encapsulés par l'IPv6/IPv4_Access_Node pour être routés vers la passerelle résidentielle, mais ils sont traduits en paquets IPv6.

- Pour les communications sortantes, sur résolution DNS d'un correspondant IPv4, on retourne au terminal d'utilisateur initiateur une adresse IPv6 construite sur la base de l'adresse IPv4 du correspondant. Le terminal d'utilisateur utilise alors cette adresse de destination IPv6 pour émettre les paquets de données. Pour émettre ce paquet, il peut utiliser son adresse source IPv6 native ou construite.
- S'il a utilisé son adresse source native, la passerelle résidentielle transforme l'adresse IPv6 native source en une adresse source construite IPv6 contenant sa propre adresse IPv4 partagée entre les passerelles (Shared_@IPv4) et le port source (inscrit dans la plage source autorisée).
- Un équipement d'interconnexion du domaine IPv6 au domaine IPv4 vérifie que la passerelle résidentielle a bien utilisé sa plage de ports source autorisés en

- préfixe IPv6 particulier IPv6_prefix_ports_range.

Les paquets IPv4 entrants dans le domaine IPv6 ne sont pas encapsulés par l'IPv6/IPv4_Access_Node pour être routés vers la passerelle résidentielle, mais ils sont traduits en paquets IPv6.

- Pour les communications sortantes, sur résolution DNS d'un correspondant IPv4, on retourne au terminal d'utilisateur initiateur une adresse IPv6 construite sur la base de l'adresse IPv4 du correspondant. Le terminal d'utilisateur utilise alors cette adresse de destination IPv6 pour émettre les paquets de données. Pour émettre ce paquet, il peut utiliser son adresse source IPv6 native ou construite.
- S'il a utilisé son adresse source native, la passerelle résidentielle transforme l'adresse IPv6 native source en une adresse source construite IPv6 contenant sa propre adresse IPv4 partagée entre les passerelles (Shared_@IPv4) et le port source (inscrit dans la plage source autorisée).
- Un équipement d'interconnexion du domaine IPv6 au domaine IPv4 vérifie que la passerelle résidentielle a bien utilisé sa plage de ports source autorisés en comparant la partie de l'adresse source qui contient les bits port source et le port source dans le champ port du paquet IPv6. Il traduit le paquet IPv6 en paquet IPv4 pour le transmettre au correspondant en utilisant :
    - pour l'adresse source IPv4 : les bits dans l'adresse IPv6 source qui contiennent Shared_@IPv4
    - pour l'adresse destination IPv4 : les bits dans l'adresse IPv6 qui contiennent l'adresse IPv4 du correspondant.

REVENDICATIONS

1. Procédé de réception d'un paquet de données IPv6 dans un domaine IPv6 interconnecté avec un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, caractérisé en ce qu'il comprend les étapes suivantes :

- identification d'une adresse IPv6 de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données et modification du paquet de données; et
- routage du paquet de données modifié vers sa destination.

2. Procédé de réception selon la revendication 1, caractérisé en ce que, lorsque le paquet est en provenance d'un terminal d'utilisateur connecté au domaine IPv6 par une passerelle résidentielle et à destination d'un domaine IPv4, l'étape de mise en conformité de l'adresse source comprend en outre les étapes suivantes :

- identification d'une adresse IPv6 source native;
- création d'une entrée dans une table de traduction d'adresses, ladite entrée associant ladite adresse source native à une adresse source construite par concaténation d'un préfixe opérateur, d'une adresse IPv4 affectée à la passerelle et d'un numéro de port source appartenant à une plage de numéros de ports autorisés pour ladite passerelle; et
- remplacement de l'adresse source native du paquet de données par l'adresse source construite.

3. Procédé de réception selon la revendication 2, caractérisé en ce que l'identification d'adresse est réalisée à l'aide d'un identifiant compris dans l'adresse de destination.

4. Procédé de réception selon la revendication 2, caractérisé en ce qu'il comprend en outre une étape de vérification d'une correspondance entre le numéro de port source du paquet de données et le numéro de port de source

33

REVENDICATIONS

1. Procédé de réception d'un paquet de données IPv6 dans un domaine IPv6 interconnecté avec un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, caractérisé en ce qu'il comprend les étapes suivantes :

- identification d'une adresse IPv6 de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données et modification du paquet de données; et
- routage du paquet de données modifié vers sa destination.

2. Procédé de réception selon la revendication 1, caractérisé en ce que, lorsque le paquet est en provenance d'un terminal d'utilisateur connecté au domaine IPv6 par une passerelle résidentielle et à

REVENDICATIONS

1. Procédé de réception d'un paquet de données IPv6 dans un domaine IPv6 interconnecté avec un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, caractérisé en ce qu'il comprend les étapes suivantes :

- identification d'une adresse IPv6 de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données et modification du paquet de données; et
- routage du paquet de données modifié vers sa destination.

2. Procédé de réception selon la revendication 1, caractérisé en ce que, lorsque le paquet est en provenance d'un terminal d'utilisateur connecté au domaine IPv6 par une passerelle résidentielle et à destination d'un domaine IPv4, l'étape de mise en conformité de l'adresse source comprend en outre les étapes suivantes :

- identification d'une adresse IPv6 source native;
- création d'une entrée dans une table de traduction d'adresses, ladite entrée associant ladite adresse source native à une adresse source construite par concaténation d'un préfixe opérateur, d'une adresse IPv4 affectée à la passerelle et d'un numéro de port source appartenant à une plage de numéros de ports autorisés pour ladite passerelle; et
- remplacement de l'adresse source native du paquet de données par l'adresse source construite.

3. Procédé de réception selon la revendication 2, caractérisé en ce que l'identification d'adresse est réalisée à l'aide d'un identifiant compris dans l'adresse de destination.

4. Procédé de réception selon la revendication 2, caractérisé en ce qu'il comprend en outre une étape de vérification d'une correspondance entre le numéro de port source du paquet de données et le numéro de port de source

de l'adresse source construite.

5. Procédé de réception selon la revendication 1, caractérisé en ce que, lorsque le paquet de données est en provenance d'un domaine IPv4 et à destination d'un terminal d'utilisateur connecté au domaine IPv6, l'étape de mise en conformité de l'adresse source comprend les étapes suivantes :

- recherche dans une table de traduction d'adresses de la passerelle d'une entrée associant à ladite adresse de destination construite une adresse de destination native.
- si une entrée a été trouvée, remplacement de l'adresse de destination du paquet de données par l'adresse de destination native de l'entrée.

6. Procédé de réception selon la revendication **5**, caractérisé en ce qu'il comprend en outre une étape de vérification d'une correspondance entre le numéro de port de destination du paquet de données et le numéro de port de destination contenu dans l'adresse de destination construite,

7. Dispositif de réception d'un paquet de données dans un domaine IPv6 interconnecté à un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, caractérisé en ce qu'il comprend les étapes suivantes :

- identification d'une adresse de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données et modification du paquet de données; et
- routage du paquet de données modifié vers sa destination.

8. Passerelle résidentielle apte à connecter des terminaux d'utilisateurs d'un réseau résidentiel à un domaine IPv6 interconnecté à un domaine IPv4, caractérisée en ce qu'elle comprend :

- des moyens d'obtention d'une adresse IPv4, d'une plage de numéros de ports autorisés pour ladite passerelle et d'une plage d'adresses IPv6 autorisées pour ladite passerelle, ladite plage d'adresses IPv6 étant construite par

Juniper Exhibit 1002, page 214

de l'adresse source construite.

5. Procédé de réception selon la revendication 1, caractérisé en ce que, lorsque le paquet de données est en provenance d'un domaine IPv4 et à destination d'un terminal d'utilisateur connecté au domaine IPv6, l'étape de mise en conformité de l'adresse source comprend les étapes suivantes :

- recherche dans une table de traduction d'adresses de la passerelle d'une entrée associant à ladite adresse de destination construite une adresse de destination native.
- si une entrée a été trouvée, remplacement de l'adresse de destination du paquet de données par l'adresse de destination native de l'entrée.

6. Procédé de réception selon la revendication **5**, caractérisé en ce qu'il comprend en outre une étape de vérification d'une correspondance entre le numéro de port de destination du paquet de données et le numéro de port de destination contenu dans l'adresse de destination construite,

7. Dispositif de réception d'un paquet de données dans un domaine IPv6 interconnecté à un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, caractérisé en ce qu'il comprend les étapes suivantes :

- identification d'une adresse de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;
- si nécessaire, mise en conformité d'au moins une adresse du paquet de données et modification du paquet de données; et
- routage du paquet de données modifié vers sa destination.

8. Passerelle résidentielle apte à connecter des terminaux d'utilisateurs d'un réseau résidentiel à un domaine IPv6 interconnecté à un domaine IPv4, caractérisée en ce qu'elle comprend :

- des moyens d'obtention d'une adresse IPv4, d'une plage de numéros de ports autorisés pour ladite passerelle et d'une plage d'adresses IPv6 autorisées pour ladite passerelle, ladite plage d'adresses IPv6 étant construite par

concaténation d'un préfixe opérateur, de ladite adresse IPv4 et de la plage de numéros de ports IPv4 autorisés; et

- un dispositif de réception d'un paquet de données IPv6 dans le domaine IPv6 interconnecté au domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, comprenant les étapes suivantes :

- identification d'une adresse de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;

- si nécessaire, mise en conformité de l'adresse source dans le paquet de données; et

- routage du paquet de données modifié vers sa destination.

9. Passerelle résidentielle selon la revendication **8**, comprenant une table de traduction d'adresses, comprenant des entrées, associant, pour une session de communication impliquant terminal d'utilisateur de son réseau résidentiel, au moins une adresse source, caractérisée en ce que ladite passerelle est apte à enregistrer dans ladite entrée, une adresse source IPv6 construite et une adresse source IPv6 native.

10. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution du procédé de réception d'un paquet de données dans un domaine IPv6 selon la revendication **1**.

concaténation d'un préfixe opérateur, de ladite adresse IPv4 et de la plage de numéros de ports IPv4 autorisés; et

- un dispositif de réception d'un paquet de données IPv6 dans le domaine IPv6 interconnecté au domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, comprenant les étapes suivantes :

- identification d'une adresse de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;

- si nécessaire, mise en conformité de l'adresse source dans le paquet de données; et

- routage du paquet de données modifié vers sa destination.

9. Passerelle résidentielle selon la revendication **8**, comprenant une table de traduction d'adresses, comprenant des entrées, associant, pour une session de communication impliquant terminal d'utilisateur de son réseau résidentiel, au moins

concaténation d'un préfixe opérateur, de ladite adresse IPv4 et de la plage de numéros de ports IPv4 autorisés; et

- un dispositif de réception d'un paquet de données IPv6 dans le domaine IPv6 interconnecté au domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source, comprenant les étapes suivantes :

- identification d'une adresse de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination;

- si nécessaire, mise en conformité de l'adresse source dans le paquet de données; et

- routage du paquet de données modifié vers sa destination.

9. Passerelle résidentielle selon la revendication **8**, comprenant une table de traduction d'adresses, comprenant des entrées, associant, pour une session de communication impliquant terminal d'utilisateur de son réseau résidentiel, au moins une adresse source, caractérisée en ce que ladite passerelle est apte à enregistrer dans ladite entrée, une adresse source IPv6 construite et une adresse source IPv6 native.

10. Produit programme d'ordinateur téléchargeable depuis un réseau de communication et/ou stocké sur un support lisible par ordinateur et/ou exécutable par un microprocesseur, caractérisé en ce qu'il comprend des instructions de code de programme pour l'exécution du procédé de réception d'un paquet de données dans un domaine IPv6 selon la revendication **1**.

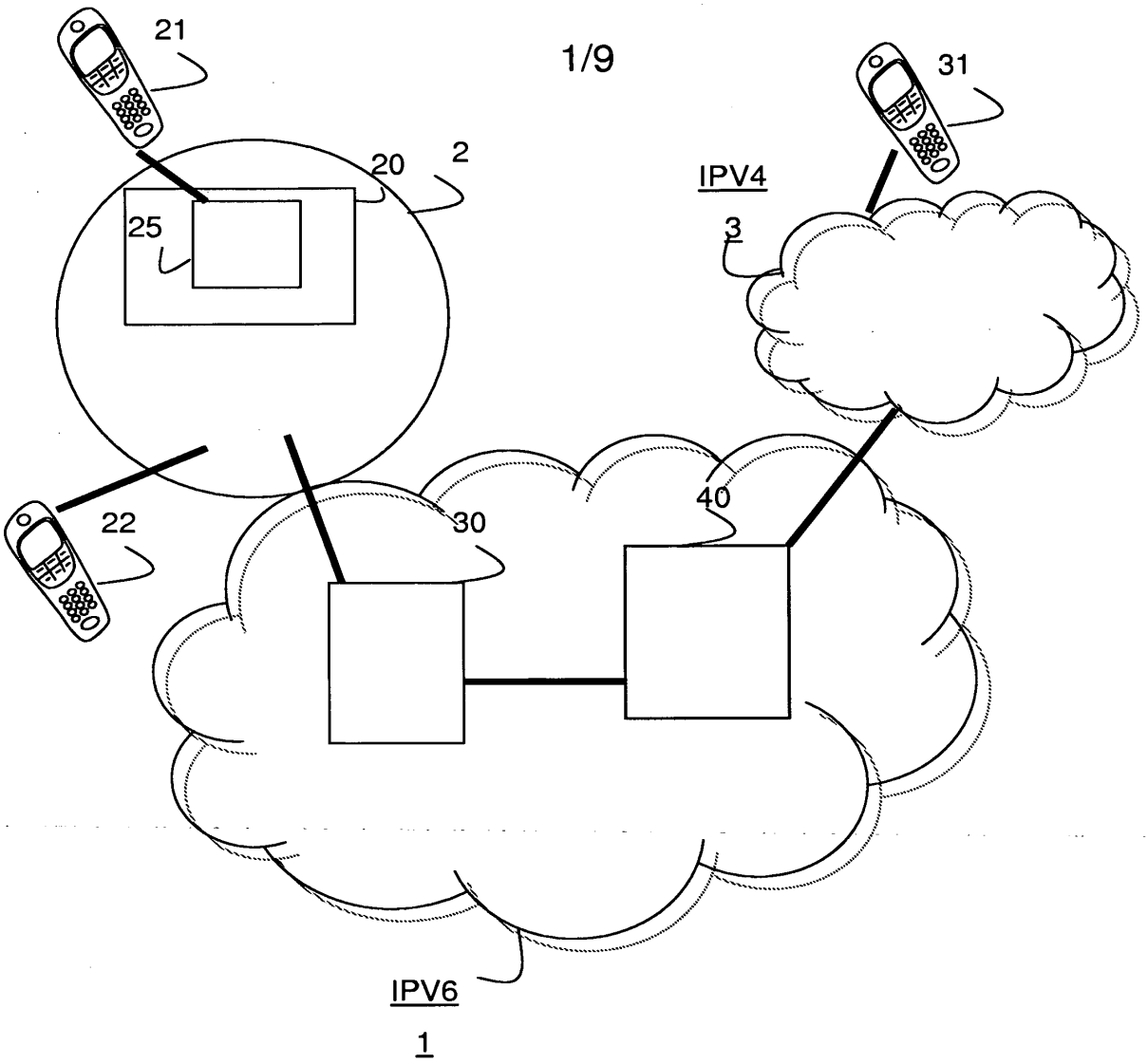


FIG. 1

Juniper Exhibit 1002, page 218

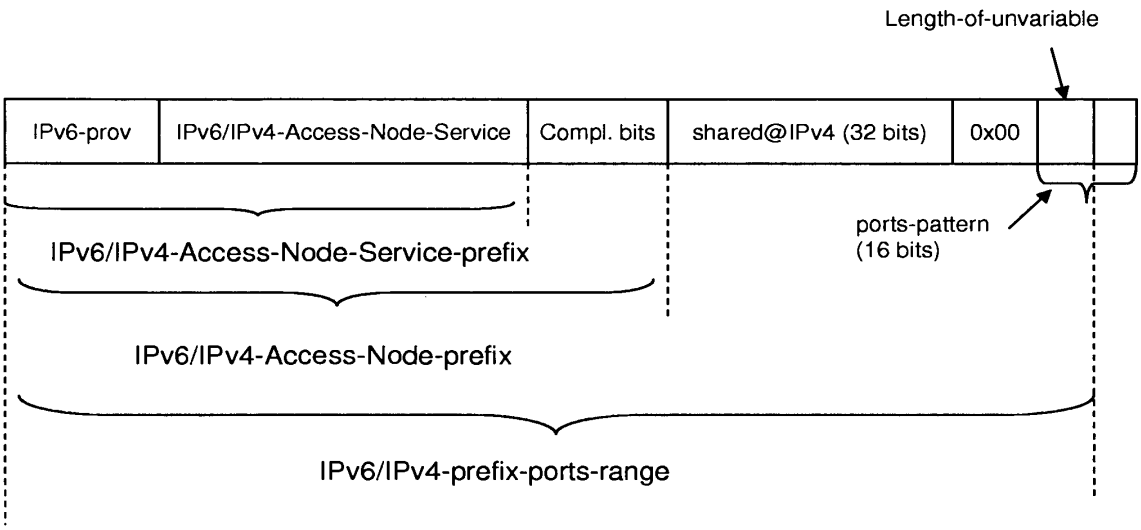

Length-of-unvariable
IPv6-prov
IPv6/IPv4-Access-Node-Service
Compl. bits
shared@IPv4 (32 bits)
0x00
ports-pattern
(16 bits)
IPv6/IPv4-Access-Node-Service-prefix
IPv6/IPv4-Access-Node-prefix
IPv6/IPv4-prefix-ports-range

FIG. 2

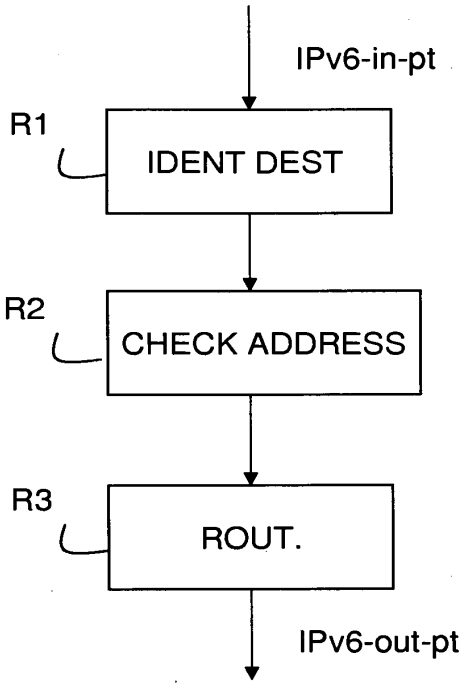


FIG. 3

Juniper Exhibit 1002, page 220

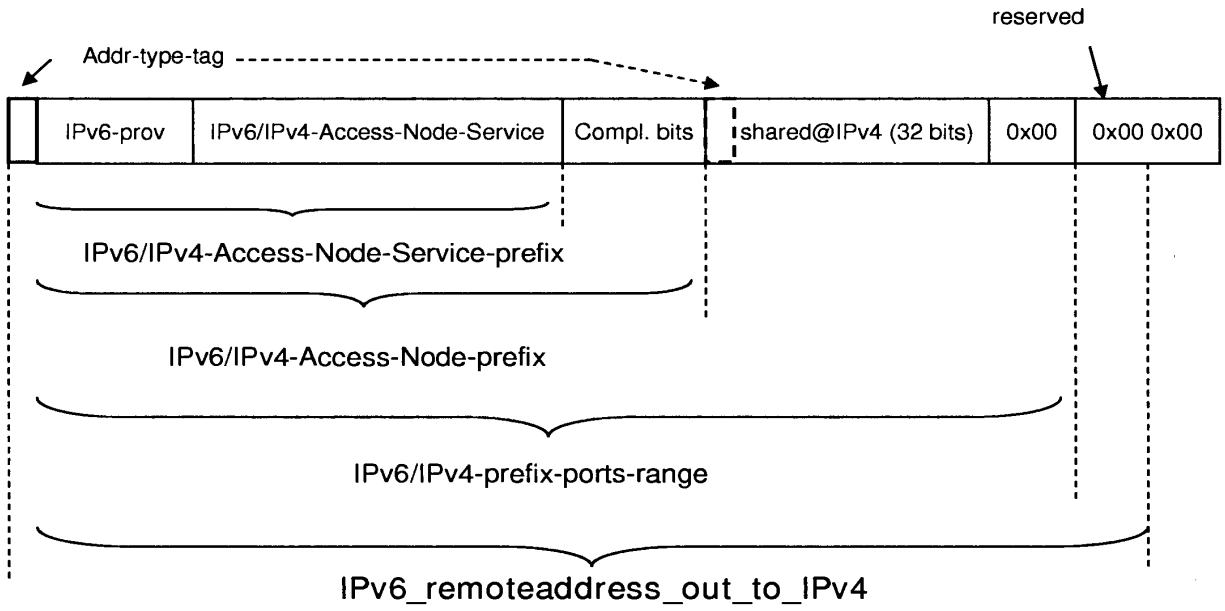


FIG. 4

Juniper Exhibit 1002, page 221

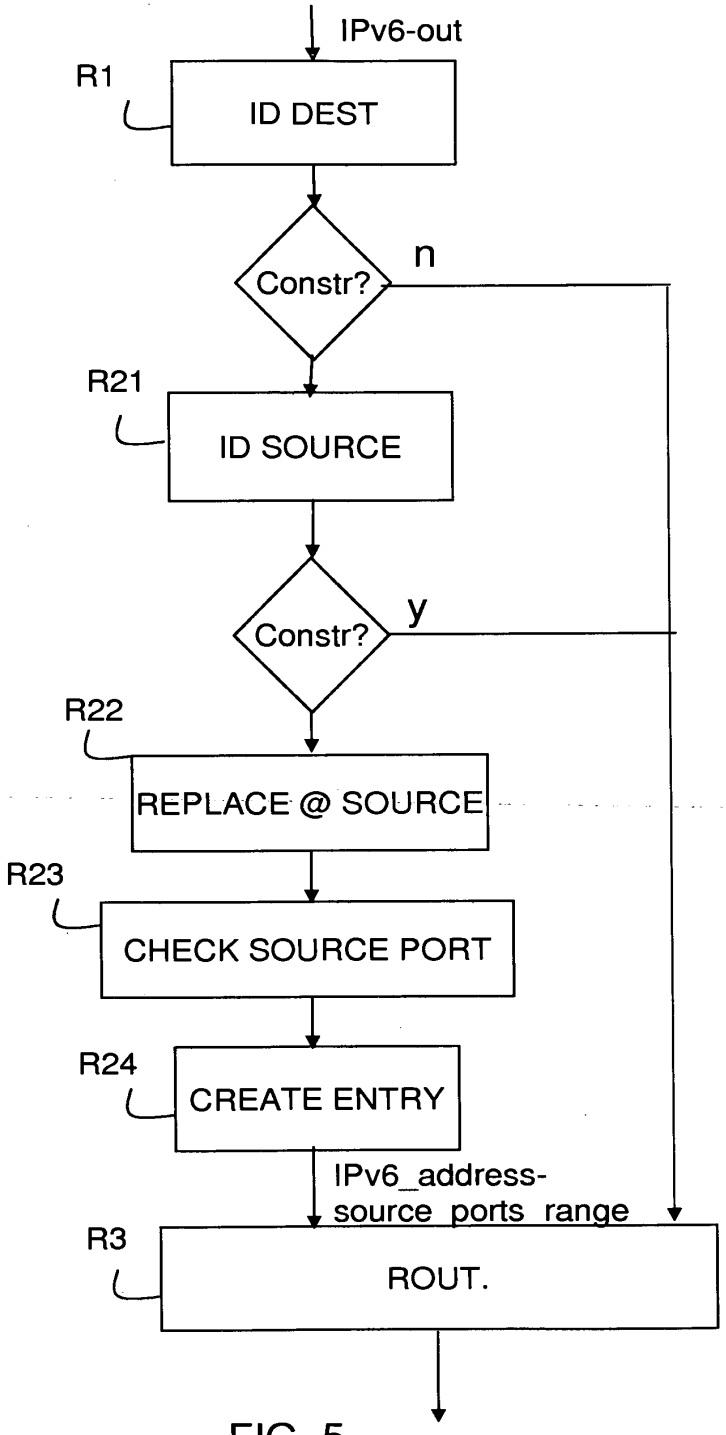


FIG. 5

Juniper Exhibit 1002, page 222

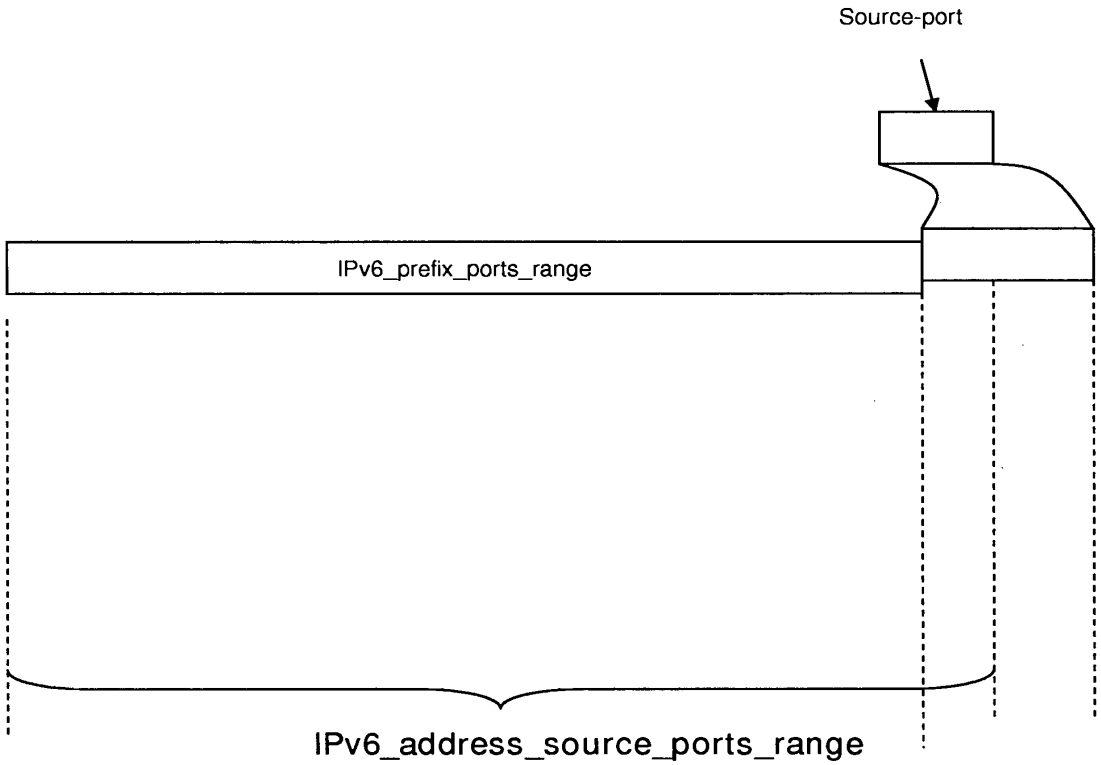


FIG. 6

Juniper Exhibit 1002, page 223

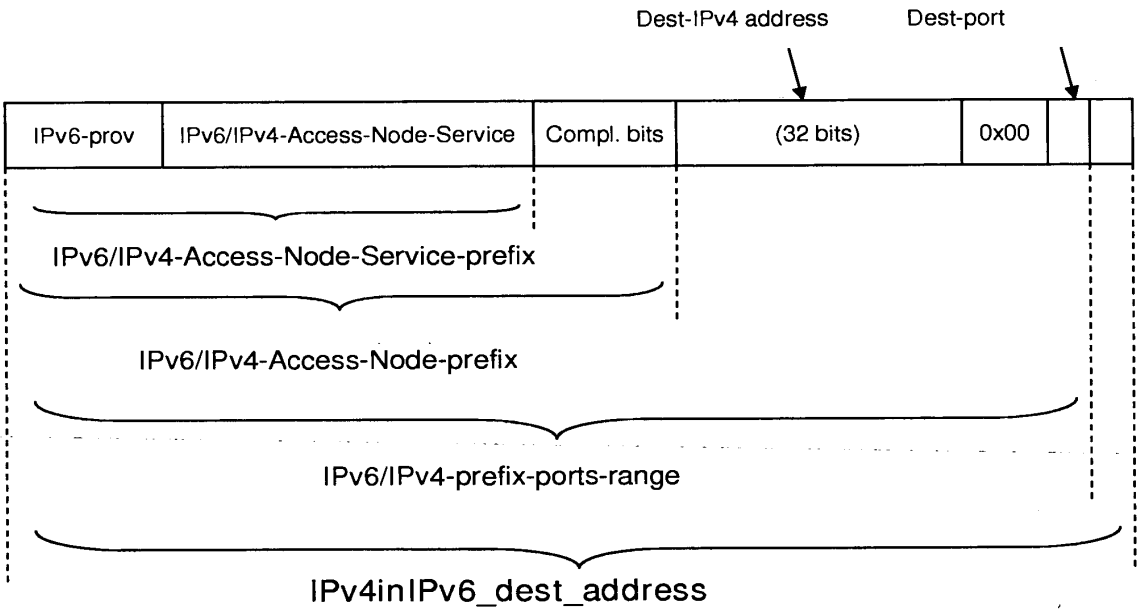

Dest-IPv4 address
Dest-port
IPv6-prov
IPv6/IPv4-Access-Node-Service
Compl. bits
(32 bits)
0x00
IPv6/IPv4-Access-Node-Service-prefix
IPv6/IPv4-Access-Node-prefix
IPv6/IPv4-prefix-ports-range
IPv4inIPv6_dest_address

FIG. 7

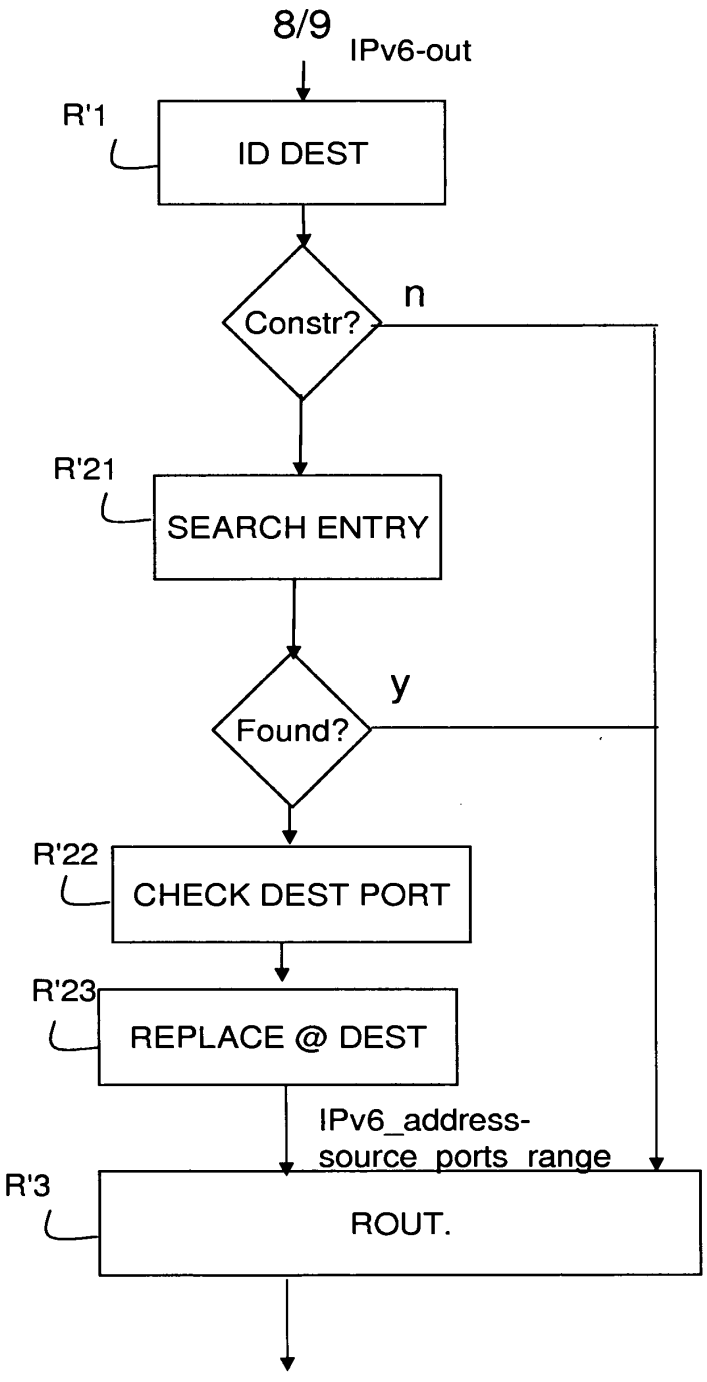


FIG. 8

Juniper Exhibit 1002, page 225

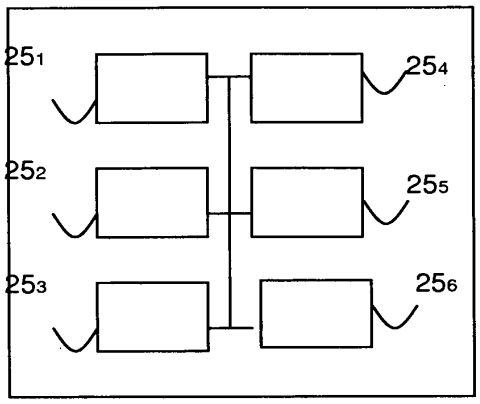


FIG. 9

Juniper Exhibit 1002, page 226

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITE

cerfa N°12236*01

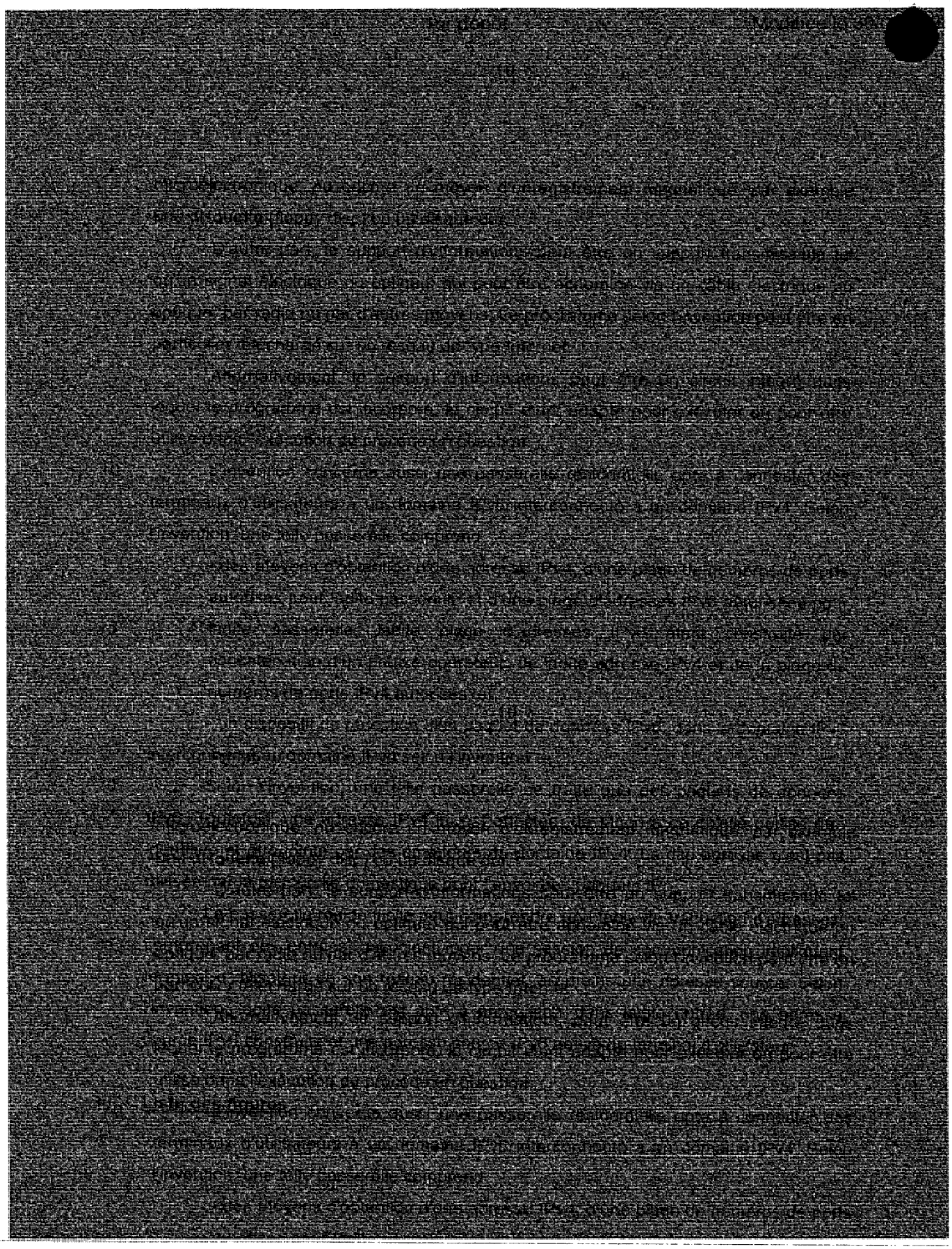
Désignation de l'inventeur

Vos références pour ce dossier	07049
N°D'ENREGISTREMENT NATIONAL	
TITRE DE L'INVENTION	
	PROCEDE DE RECEPTION D'UN PAQUET DE DONNEES DANS UN DOMAINE IPv6, DISPOSITIF ET PASSERELLE RESIDENTIELLE ASSOCIES
LE(S) DEMANDEUR(S) OU LE(S) MANDATAIRE(S):	
DESIGNE(NT) EN TANT QU'INVENTEUR(S):	
Inventeur 1	
Nom	BOUCADAIR
Prénoms	Mohamed
Rue	124, rue Saint Jean
Code postal et ville	14000 CAEN
Société d'appartenance	FRANCE TELECOM
Inventeur 2	
Nom	GRIMAULT
Prénoms	Jean-Luc
Rue	7, Impasse de l'Europe
Code postal et ville	14120 MONDEVILLE
Société d'appartenance	FRANCE TELECOM

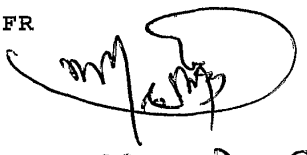
La loi n°78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Signé par
Signataire: FR, FRANCE TELECOM RD, Myriam PLAT
Emetteur du certificat: FR, INPI, INPI-EN-LIGNE 1.0
Fonction
(Demandeur)





VIII-4-1	**Déclaration : Qualité d'inventeur (seulement aux fins de la désignation des États-Unis d'Amérique)** Déclaration relative à la qualité d'inventeur (règles 4.17.iv) et 51bis.1.a)iv)) aux fins de la désignation des États-Unis d'Amérique :	Par la présente, je declare que je crois être le premier inventeur original et unique (si un seul inventeur est mentionné ci-dessous) ou l'un des premiers coïnventeurs (si plusieurs inventeurs sont mentionnés ci-dessous) de l'objet revendiqué pour lequel un brevet est demandé. La présente déclaration a trait à la demande internationale PCT/FR2009/051228 (si la déclaration est remise en vertu de la règle 26ter) Par la présente, je déclare que mon domicile, mon adresse postale et ma nationalité sont tels qu'indiqués près de mon nom. Par la présente, je déclare avoir passé en revue et comprendre le contenu de la demande internationale à laquelle il est fait référence ci-dessus, y compris les revendications de ladite demande. J'ai indiqué dans la requête de ladite demande, conformément à la règle 4.10 du PCT, toute revendication de priorité d'une demande étrangère et j'ai identifié ci-dessous, sous l'intitulé "Demandes antérieures", au moyen du numéro de demande, du pays ou du membre de l'Organisation mondiale du commerce, du jour, du mois et de l'année du dépôt, toute demande de brevet ou de certificat d'auteur d'invention déposée dans un pays autre que les États-Unis d'Amérique, y compris toute demande internationale selon le PCT désignant au moins un pays autre que les États-Unis d'Amérique, dont la date de dépôt est antérieure à celle de la demande étrangère dont la priorité est revendiquée.
VIII-4-1-1	Demandes antérieures :	

		Par la présente, je reconnais l'obligation qui m'est faite de divulguer les renseignements dont j'ai connaissance et qui sont pertinents quant à la brevetabilité de l'invention, tels qu'ils sont définis dans le Titre 37, § 1.56, du Code fédéral des réglementations, y compris, en ce qui concerne les demandes de continuation-in-part les renseignements pertinents qui sont devenus accessibles entre la date de dépôt de la demande antérieure et la date du dépôt international de la demande de continuation-in-part. Je déclare par la présente que toute déclaration ci-incluse est, à ma connaissance, véridique et que toute déclaration formulée à partir de renseignements ou de suppositions est tenue pour véridique; et de plus, que toutes ces déclarations ont été formulées en sachant que toute fausse déclaration volontaire ou son équivalent est passible d'une amende ou d'une incarcération, ou des deux, en vertu de la Section 1001 du Titre 18 du Code des États-Unis, et que de telles déclarations volontairement fausses risquent de compromettre la validité de la demande de brevet ou du brevet délivré à partir de celle-ci.
VIII-4-1-1-1	Nom (NOM DE FAMILLE, prénom) :	BOUCADAIR, Mohamed
VIII-4-1-1-2	Domicile : (ville et État (des États-Unis d'Amérique), le cas échéant, ou pays)	RENNES, France
VIII-4-1-1-3	Adresse postale :	1 square Louis Harel de la Nöe 35000 RENNES France
VIII-4-1-1-4	Nationalité :	FR
VIII-4-1-1-5	Signature de l'inventeur : (La signature doit être celle de l'inventeur, il ne peut s'agir de celle du mandataire)	
VIII-4-1-1-6	Date :	02-07-09

VIII-4-1-2-1	Nom (NOM DE FAMILLE, prénom) :	GRIMAULT, Jean-Luc
VIII-4-1-2-2	Domicile : (ville et État (des États-Unis d'Amérique), le cas échéant, ou pays)	MONDEVILLE, France
VIII-4-1-2-3	Adresse postale :	7 impasse de l'Europe 14120 MONDEVILLE France
VIII-4-1-2-4	Nationalité :	FR
VIII-4-1-2-5	Signature de l'inventeur : (La signature doit être celle de l'inventeur, il ne peut s'agir de celle du mandataire)	
VIII-4-1-2-6	Date	30/6/2009

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATIONEN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
14 janvier 2010 (14.01.2010)

PCT

(10) Numéro de publication internationale
WO 2010/004180 A1

(51) Classification internationale des brevets :
H04L 29/12 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2009/051228

(22) Date de dépôt international :
26 juin 2009 (26.06.2009)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0854405 30 juin 2008 (30.06.2008) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BOUCADAIR, Mohamed** [FR/FR]; 1, square Louis Harel de la Nöe, F-35000 Rennes (FR). **GRIMAULT, Jean-Luc** [FR/FR]; 7, impasse de l'Europe, F-14120 Mondeville (FR).

(74) Mandataire : **FRANCE TELECOM R&D/PIV/BREVETS**; BENETIERE Marion, 38-40, rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, 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, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Suite sur la page suivante]

(54) Title : METHOD FOR RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AND ASSOCIATED DEVICE AND RESIDENTIAL GATEWAY

(54) Titre : PROCEDE DE RECEPTION D'UN PAQUET DE DONNEES DANS UN DOMAINE IPV6, DISPOSITIF ET PASSERELLE RESIDENTIELLE ASSOCIES

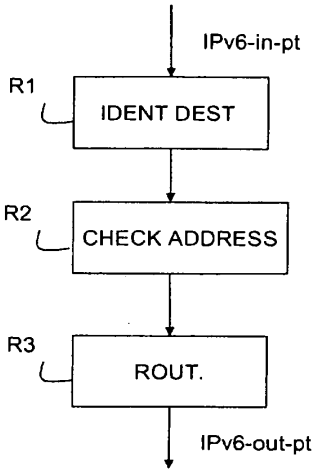


FIG. 3

(57) Abstract : The invention relates to a method for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet comprising an IPv6 destination address and an IPv6 source address. According to the invention, such a method comprises the following steps: an IPv6 destination address constructed by concatenation of an operator prefix, an IPv4 destination address and a destination port number is identified; if necessary, at least one address of the data packet is brought into compliance and the data packet is modified; and the modified data packet is routed towards its destination.

(57) Abrégé : L'invention concerne un procédé de réception d'un paquet de données IPv6 dans un domaine IPv6 interconnecté avec un domaine IPv4, ledit paquet comprenant une adresse IPv6 de destination et une adresse IPv6 source. Selon l'invention, un tel procédé comprend les étapes suivantes : identification d'une adresse IPv6 de destination construite par concaténation d'un préfixe opérateur, d'une adresse de destination IPv4 et d'un numéro de port de destination; si nécessaire, mise en conformité d'au moins une adresse du paquet de données et modification du paquet de données; et routage du paquet de données modifié vers sa destination.

WO 2010/004180 A1

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number	Filing Date	☐ To be Mailed
13/001,907	12/29/2010	

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐ RATE ($)	SMALL ENTITY ☐ FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
FOR	NUMBER FILED	NUMBER EXTRA					
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

AMENDMENT 12/29/2010	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 10	Minus	** 20	= 0	X $ =		OR	X $52=	0
Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $220=	0
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**0**

AMENDMENT	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
☐ Application Size Fee (37 CFR 1.16(s))									
☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.

** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".

*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DIANIECE JACOBS/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING or 371(c) DATE	GRP ART UNIT	FIL FEE REC'D	ATTY.DOCKET.NO	TOT CLAIMS	IND CLAIMS
13/001,907	12/29/2010		980	P3714US	10	2

CONFIRMATION NO. 5439

8968
DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

FILING RECEIPT

OC000000045755221

Date Mailed: 02/03/2011

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. **If an error is noted on this Filing Receipt, please submit a written request for a Filing Receipt Correction. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections**

Applicant(s)

Mohamed Boucadair, Rennes, FRANCE;
Jean-Luc Grimault, Mondeville, FRANCE;

Assignment For Published Patent Application

FRANCE TELECOM, Paris, FRANCE

Power of Attorney: The patent practitioners associated with Customer Number 08968

Domestic Priority data as claimed by applicant

This application is a 371 of PCT/FR2009/051228 06/26/2009

Foreign Applications (You may be eligible to benefit from the **Patent Prosecution Highway** program at the USPTO. Please see http://www.uspto.gov for more information.)
FRANCE 0854405 06/30/2008

If Required, Foreign Filing License Granted: 01/31/2011

The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is **US 13/001,907**

Projected Publication Date: 05/12/2011

Non-Publication Request: No

Early Publication Request: No

CI

Title

METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at http://www.uspto.gov/web/offices/pac/doc/general/index.html.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, http://www.stopfakes.gov. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as

Juniper Exhibit 1002, page 236

set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign AssetsControl, Department of Treasury (31 CFR Parts 500+) and the Department of Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

CI

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 13/001,907

APPLICATION AS FILED - PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY FEE($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	330
SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	430
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	220
TOTAL CLAIMS (37 CFR 1.16(i))	10 minus 20 =	*			OR	x 52 =	0.00
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2 minus 3 =	*				x 220 =	0.00
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						0.00
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							0.00
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	980

APPLICATION AS AMENDED - PART II

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE($)	SMALL ENTITY ADDITIONAL FEE($)	OR	OTHER THAN SMALL ENTITY RATE($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE($)
AMENDMENT A	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

		(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE($)	ADDITIONAL FEE($)	OR	RATE($)	ADDITIONAL FEE($)
AMENDMENT B	Total (37 CFR 1.16(i))	*	Minus	**	=	x =		OR	x =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	x =		OR	x =	
	Application Size Fee (37 CFR 1.16(s))									
	FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest found in the appropriate box in column 1.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY. DOCKET NO.
13/001,907	Mohamed Boucadair	P3714US

8968
DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

INTERNATIONAL APPLICATION NO.	
PCT/FR2009/051228	
I.A. FILING DATE	PRIORITY DATE
06/26/2009	06/30/2008

CONFIRMATION NO. 5439
371 ACCEPTANCE LETTER

OC000000045755222

Date Mailed: 02/03/2011

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office in its capacity as a Designated / Elected Office (37 CFR 1.495), has determined that the above identified international application has met the requirements of 35 U.S.C. 371, and is ACCEPTED for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

12/29/2010	12/29/2010
DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS	DATE OF COMPLETION OF ALL 35 U.S.C. 371 REQUIREMENTS

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 (c)(1), (c)(2) and (c)(4) REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE.** *The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363).* Once the Filing Receipt has been received, send all correspondence to the Group Art Unit designated thereon.

The following items have been received:

- Copy of the International Application filed on 12/29/2010
- English Translation of the IA filed on 12/29/2010
- Copy of the International Search Report filed on 12/29/2010
- Preliminary Amendments filed on 12/29/2010
- Oath or Declaration filed on 12/29/2010
- Request for Immediate Examination filed on 12/29/2010
- U.S. Basic National Fees filed on 12/29/2010
- Priority Documents filed on 12/29/2010

FORM PCT/DO/EO/903 (371 Acceptance Notice)

CI

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

SHAKEEL AHMED

Telephone: (703) 756-1423

FORM PCT/DO/EO/903 (371 Acceptance Notice)

CI

MULTIPLE DEPENDENT CLAIM FEE CALCULATION SHEET Substitute for Form PTO-1360 (For use with Form PTO/SB/06)	Application Number 13001907	Filing Date
	Applicant(s) Mohamed BOUCADAIR	

* May be used for additional claims or amendments

CLAIMS	AS FILED		AFTER FIRST AMENDMENT		AFTER SECOND AMENDMENT	
	Indep	Depend	Indep	Depend	Indep	Depend
1	1		1			
2		1		1		
3		1		1		
4		1		1		
5		1		1		
6		1		1		
7	1		1			
8		1		1		
9		1		1		
10		1		1		
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
Total Indep	2		2		0	
Total Depend	8	↵	8	↵	0	↵
Total Claims	10		10		0	

	*		*		*	
	Indep	Depend	Indep	Depend	Indep	Depend
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

CI

Please type a plus sign (+) inside this box →

Substitute for form 1449A/B/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/001,907
				Filing Date	December 29, 2010
				First Named Inventor	Mohamed BOUCADAIR
				Group Art Unit	Unassigned
(Use as many sheets as necessary)				Examiner Name	Unassigned
Sheet	1	of	1	Attorney Docket Number	P3714US

U.S. PATENT DOCUMENTS						
Examiner Initials	Doc. No.	U.S. Patent Document: Application or Patent Number	U.S. Patent Document: Kind Code	Name of Patentee or Applicant	Date of Publication	Filing Date If Appropriate

FOREIGN PATENT DOCUMENTS								
Examiner Initials	Doc. No.	Foreign Patent Document: Office	Foreign Patent Document: Application or Patent Number	Foreign Patent Document: Kind Code	Name of Patentee or Applicant	Date of Publication	Translation: Yes	Translation: No*+
	A A	WO	2004/039014	A1	Cisco Technology, Inc.	May 6, 2004		
	A B	EP	1 420 559	A1	Thomson Licensing S.A.	May 19, 2004		
	A C	WO	2007/099248	A2	France Telecom	September 7, 2007		X+
	A D	WO	2008/001007	A2	France Telecom	January 3, 2008		X+

OTHER - NON PATENT LITERATURE DOCUMENTS				
Examiner Initials	Doc. No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number (s), publisher, city and/or country where published.	Translation: Yes	Translation: No*+
	A E	AFIFI et al., "Methods for IPv4-IPv6 Transition," IEEE International Symposium on Computers and Communications, Red Sea, Egypt 6-8 July 1999, Proceedings, Los Alamitos, CA, USA, IEEE Comput. Soc., US, pp. 478-484 (July 6, 1999)		
	A F	KAWARASAKI et al., "IPv4/IPv6 SIP interworking methods in dual-stack network," The 9th Asia-Pacific Conference on Communications, 2003, APCC 2003, 21-24 September 2003, Piscataway, NJ, USA, IEEE, vol. 3, pp. 1124-1128 (September 21, 2003)		
	A G	PARK et al., "Network Address Translation – Protocol Translation (NAT-PT); draft-daniel-natpt-bis-01.txt," Internet Engineering Task Force, IETF, pp. 1-21 (October 22, 2005)		
	A H	SHIN et al., "Ports Option Support in Dual Stack Transition Mechanism (DSTM)," The 6th International Conference on Advanced Communication Technology, Phoenix Park, Korea, February 9-11, 2004, Piscataway, NJ, USA, IEEE, vol. 1, pp. 225-228 (February 9, 2004)		
	A I	SRISURESH et al., "RFC 2663 – IP Network Address Translator (NAT) Terminology and Considerations, " Network Working Group, retrieved from internet website: http://www.ietf.org/rfc/rfc2663.txt, pp. 1-30 (1999)		

Examiner Signature		Date Considered	

* A concise statement of relevance is being submitted in lieu of a translation. 37 CFR 1.98(a)(3).

\+ An English-language equivalent/patent, or an English-language abstract, or an English-language version of the search report or action by a foreign patent office in a counterpart foreign application indicating the degree of relevance found by the foreign office is being submitted in lieu of a concise explanation of relevance under 37 CFR 1.98(a)(3).

CH01/ 25685885.1

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 May 2004 (06.05.2004)

PCT

(10) International Publication Number
WO 2004/039014 A1

(51) International Patent Classification[7]: H04L 12/46, 29/06

(21) International Application Number:
PCT/US2003/032959

(22) International Filing Date: 16 October 2003 (16.10.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/278,327 22 October 2002 (22.10.2002) US

(71) Applicant: CISCO TECHNOLOGY, INC. [US/US]; 170 West Tasman Drive, San Jose, CA 95134-1706 (US).

(72) Inventors: SATAPATI, Suresh, K.; 1711 Warburton Avenue, #8, Santa Clara, CA 95050 (US). SIVAKUMAR, Senthil, M.; 1235 Wildwood Avenue, #108, Sunnyvale, CA 94089 (US). CHEN, Jieping; 760 S. Saratoga Avenue, #Z208, San Jose, CA 95129 (US).

(74) Agent: OLYNICK, Mary, R.; Beyer Weaver & Thomas, LLP, P.O. Box 778, Berkeley, CA 94704-0778 (US).

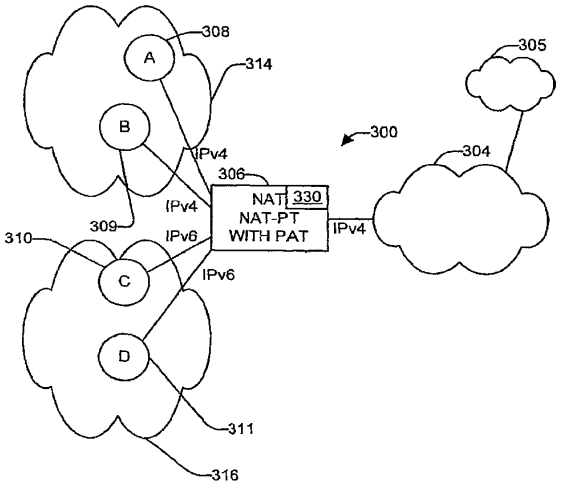
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, 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.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, 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, 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*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

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.

(54) Title: SHARED PORT ADDRESS TRANSLATION ON A ROUTER BEHAVING AS NAT & NAT-PT GATEWAY



(57) Abstract: A method for transparently sharing at least one IPv4 address among a plurality of hosts (308, 309, 310, 311) wherein at least a first host of the plurality of hosts uses the IPv4 protocol (314) and wherein at least a second host of the plurality of hosts uses an IPv6 protocol (316) is provided. A first data having a first source address and a first destination address is received. A network address translation with port address translation is performed (306), if the first data is in an IPv4 protocol. A network address translation protocol translation with port address translation is performed (306), if the first data is in an IPv6 protocol.

WO 2004/039014 A1

SHARED PORT ADDRESS TRANSLATION ON A ROUTER BEHAVING AS NAT & NAT-PT GATEWAY

BACKGROUND OF THE INVENTION

The present invention relates to methods and apparatus for processing data within a computer network. More specifically, this invention relates to performing network address translation on data.

In a network, devices on the network are provided network addresses, which are used to identify the different devices, when devices communicate between each other. IP protocol version 4 (IPv4) is a protocol used to provide addresses for public and private networks. A private network, such as an enterprise system, may be connected to a public network, such as the Internet. Such private networks may have more devices than available Internet IPv4 addresses allocated to the private network. In such a situation, a network address translator (NAT) may be connected between the private network and the Internet. The NAT may dynamically assign IPv4 addresses, so that the number of devices using the Internet at one time is limited to the available number of IPv4 addresses allocated to the private network. In the alternative, the NAT may use port address translation, where port numbers are used to further identify different devices with the same address.

IPv4 uses a 32-bit address. Even with these various multiplexing methods to allow multiple devices for each Internet IPv4 address, the number of devices that are desired to be connected to the Internet will exceed the limits of a 32-bit address. IPv6 is a protocol that is designed to replace IPv4. IPv6 provides for a 128-bit address to overcome address depletion and other problems caused by IPv4. Because a large number of devices and routers using IPv4 are in existence, IPv6 should replace IPv4 gradually, instead of instantaneously. As a result, networks using IPv6 need to be able to communicate with networks using IPv4 for a long period of time.

FIG. 1 is a schematic illustration of a system 100 that allows a network address translator (NAT) 106 to provide network address translations between a private IPv4 network with a plurality of IPv4 users 101, 102, 103 and a public network 104, such as an Internet, which is connected to a plurality of web servers 105, using the IPv4 protocol. The NAT 106 is able to provide a plurality of users Internet access, using a

Juniper Exhibit 1002, page 244

small number of IPv4 addresses. In this example, a single IPv4 address of 128.1.1.1 is assigned to the NAT 106. The NAT 106 may assign the plurality of users 101, 102, 103 private network addresses. For example, a user A 101 may be assigned a private network address of 10.1.1.1, a user B 102 may be assigned a private network address of 10.1.1.2, and a user C 103 may be assigned a private network address of 10.1.1.3. In this example, the web server 105 has a public address of 130.1.1.10. In this example, since the NAT 106 has a single Internet public address, the NAT 106 uses port address translation (PAT) to multiplex the single address by port number. In IPv4, the port number is 16 bits, providing 65,536 port numbers. Generally, port numbers 0-1024 are reserved for defined standard Internet uses. Therefore, the NAT 106 may use user definable ports 1025-65,535 for port address translation.

If user A 101 sends a packet to the web server 105, the packet sent from user A 101 to the NAT 106 may have the following protocol, source address, source port, destination address, and destination port numbers.

Protocol	SA	SP	DA	DP
TCP	10.1.1.1	10,000	130.1.1.10	80

The NAT 106 uses a lookup table such as Table 1 to translate the packet source and destination address and ports.

Table 1

Private					Public			
Protocol	SA	SP	DA	DP	SA	SP	DA	DP
TCP	10.1.1.1	10,000	130.1.1.10	80	128.1.1.1	10,000	130.1.1.10	80

As a result, the packet's destination and source address and ports are translated to:

SA	SP	DA	DP
128.1.1.1	10,000	130.1.1.10	80

Then the packet is sent from the NAT 106 to the web server 105 at the destination address.

The web server 105 may then send a packet back to user A 101 in reply. The packet sent from the web server 105 to the NAT 106 may have address and port designations as follows:

Protocol	SA	SP	DA	DP
TCP	130.1.1.10	80	128.1.1.1	10,000

Using Table 1, the NAT 106 translates the destination and source address and port of the packet to:

SA	SP	DA	DP
130.1.1.10	80	10.1.1.1	10,000

FIG. 2 is a schematic illustration of a system 200 that allows a network address translator-protocol translator (NAT-PT) 206 to provide network address and protocol translations between an IPv6 network with a plurality of IPv6 users 201, 202, 203 and a public network 204, such as an Internet, which is connected to a plurality of web servers 205, using the IPv4 protocol. The NAT-PT 206 is able to provide a protocol translation to a plurality of IPv6 users, using a small number of IPv4 addresses. In this example, a single IPv4 address of 128.1.1.1 is assigned to the NAT-PT 206 host. The plurality of users 201, 202, 203 may be assigned public IPv6 addresses. For example, a user A 201 may be assigned an IPv6 network address of 3000: :1, a user B 202 may be assigned an IPv6 network address of 3000: :2, and a user C 203 may be assigned an IPv6 network address of 3000: :3. In this example, the web server 205 has a public IPv4 address of 130.1.1.10. In this example, since the NAT-PT 206 has a single Internet public address, the NAT-PT 206 uses port address translation (PAT) to multiplex the single address by port number.

If user A 201 sends an IPv6 packet to the web server 205, the packet sent from user A 201 to the NAT-PT 206 may have the following protocol, source address, source port, destination address, and destination port numbers:

Juniper Exhibit 1002, page 246

Protocol	SA	SP	DA	DP
TCP	3000: :1	20,000	5000: :10	80

Although the web server 205 has an IPv4 address of 130.1.1.10, the NAT-PT 206 assigns an IPv6 address of 5000: :10 to it, so that user A 201 may address the web server 205 in an IPv6 format. This IPv6 address assignment to the web server could be due to prior configuration on the NAT-PT device, statistically or through a dynamic binding.

The NAT-PT 206 uses a lookup table such as Table 2 to translate the packet source and destination address and ports.

Table 2

	Protocol	SA	SP	DA	DP
IPv6	TCP	3000: :1	20,000	5000: :10	80
IPv4	TCP	128.1.1.1	20,000	130.1.1.10	80

As a result, the packet's destination and source address and ports are translated to:

SA	SP	DA	DP
128.1.1.1	20,000	130.1.1.10	80

Then the IPv4 packet is sent from the NAT-PT 206 to the web server 205 at the destination address.

The web server 205 may then send a packet back to user A 201 in reply. The IPv4 packet sent from the web server 205 to the NAT-PT 206 may have protocol, address and port designations as follows:

Protocol	SA	SP	DA	DP
TCP	130.1.1.10	80	128.1.1.1	10,000

Juniper Exhibit 1002, page 247

Using Table 2, the NAT-PT 206 translates the destination and source address and port of the packet to:

SA	SP	DA	DP
5000: :10	80	3000: :1	20,000

Therefore, the prior art NAT with PAT is able to connect a plurality of IPv4 users to the Internet and the prior art NAT-PT with PAT is able to connect a plurality of IPv6 users to IPv4 web servers on the Internet.

BRIEF SUMMARY OF THE INVENTION

To achieve the foregoing, and in accordance with the purpose of the present invention, a method for transparently sharing at least one IPv4 address among a plurality of hosts wherein at least a first host of the plurality of hosts uses the IPv4 protocol and wherein at least a second host of the plurality of hosts uses an IPv6 protocol is provided. A first data having a first source address and a first destination address is received. A network address translation with port address translation is performed, if the first data is in an IPv4 protocol. A network address translation-protocol translation with port address translation is performed, if the first data is in an IPv6 protocol.

In another embodiment of the invention, the invention pertains to a computer system operable for transparently sharing at least one IPv4 address among a plurality of hosts wherein at least a first host of the plurality of hosts uses the IPv4 protocol and wherein at least a second host of the plurality of hosts uses an IPv6 protocol. The computer system includes one or more processors and one or more memory. At least one of the memory processors is adapted to provide at least some of the above-described method operations. In yet a further embodiment of the invention, the invention pertains to a computer program product for transparently sharing at least one IPv4 address among a plurality of hosts wherein at least a first host of the plurality of hosts uses the IPv4 protocol and wherein at least a second host of the plurality of hosts uses an IPv6 protocol. The computer program product has at least one computer

Juniper Exhibit 1002, page 248

readable medium and computer program instructions stored within at least one of the computer readable product configured to perform at least some of the described method operations. In yet another embodiment, the invention pertains to an apparatus that includes one or more means for transparently sharing at least one IPv4 address among a plurality of hosts wherein at least a first host of the plurality of hosts uses the IPv4 protocol and wherein at least a second host of the plurality of hosts uses an IPv6 protocol.

These and other features of the present invention will be described in more detail below in the detailed description of the invention and in conjunction with the following figures.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

FIG. 1 is a schematic illustration of a system that allows a network address translator (NAT) to provide network address translations between a private IPv4 network with a plurality of IPv4 users and a public network such as an Internet in the prior art.

FIG. 2 is a schematic illustration of a system that allows a network address translator-protocol translator (NAT-PT) to provide network address translations between an IPv6 network with a plurality of IPv6 users and a public IPv4 network.

FIG. 3 is a schematic illustration of a system that allows at least a first device and second device of a first protocol, such as IPv4, and at least a third device and a fourth device of a second protocol, such as IPv6, to communicate with devices of the first protocol, through a router behaving as a gateway.

FIG. 4 is a high level flow chart of a process that may be used in an embodiment of the invention for sending packets to a public Internet.

FIG. 5 is a high level flow chart of a process for receiving packets from the public Internet.

FIG. 6 is a diagrammatic representation of a router in which embodiments of the present invention may be implemented.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention will now be described in detail with reference to a few preferred embodiments thereof as illustrated in the accompanying drawings. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art, that the present invention may be practiced without some or all of these specific details. In other instances, well known process steps and/or structures have not been described in detail in order to not unnecessarily obscure the present invention.

It is desirable to have a combination NAT and NAT-PT with PAT that is able to connect a combination of both IPv4 and IPv6 users to the Internet.

To facilitate understanding, FIG. 3 is a schematic illustration of a system 300 that allows a first device 308 and second device 309 of a first protocol, such as IPv4, and a third device 310 and a fourth device 311 of a second protocol, such as IPv6, to communicate with devices of the first protocol, through a Network Address Translation and Network Address Translation-Protocol Translation with Port Address Translation (NAT NAT-PT with PAT) device or NAT-PAT NAT-PT-PAT device, which in this embodiment is a router 306 behaving as a gateway. In the specification and claims, a router is defined as any device that performs routing/forwarding. The router may be an independent device or may be part of a larger device that does other functions. To facilitate understanding, devices such as the first device 308 and the second device 309, which use the IPv4 protocol, are drawn as part of an IPv4 network 314 and devices such as the third device 310 and the fourth device 311, which use the IPv6 protocol, are drawn as part of an IPv6 network 316. In the illustrated embodiment, although two devices are shown for each network having a different protocol, of course any suitable number of devices may be coupled with each network.

Juniper Exhibit 1002, page 250

Additionally, the devices coupled with router 306 may implement any suitable number and type of protocol, besides IPv4 and IPv6.

The router 306 may assign the first device 308 a private IPv4 address, such as 10.1.1.1 and the second device 309 a private IPv4 address, such as 10.1.1.2, since the first device 308 and the second device 309 are IPv4 devices. The router 306 may assign the third device 310 an IPv6 address, such as 3000: :1 and the fourth device 311 an IPv6 address, such as 3000: :2, since the third device 310 and the fourth device 311 are IPv6 devices. The router 306 is connected to the public Internet 304 or a network consisting of devices that have been assigned unique IPv4 addresses.

In a preferred embodiment, the router 306 may have an NAT NAT-PT database 330, which is able to hold NAT entries and NAT-PT entries. The NAT NAT-PT database may comprise smaller databases or tables, such as a NAT table for the NAT entries that lists all network address translations for current connections from private IPv4 devices to public IPv4 devices and a NAT-PT table for NAT-PT entries that lists all network address translation-protocol translations for current connections from IPv6 devices to IPv4 devices. An example of a NAT table that lists all network address translations (NAT entries) for current connections from private IPv4 devices to public IPv4 devices is shown in Table 3.

Table 3

Private					Public			
Protocol	SA	SP	DA	DP	SA	SP	DA	DP
TCP	10.1.1.1	10,000	130.1.1.20	80	128.1.1.1	10,000	130.1.1.20	80

Table 3 shows an existing connection for the first device 308, which is assigned the single public IPv4 address 128.1.1.1, with a port designation of 10,000.

An example of a NAT-PT table that lists all network address translations-protocol translations (NAT-PT entries) for current connections from private IPv4 and IPv6devices to public IPv4 devices is shown in Table 4.

Juniper Exhibit 1002, page 251

Table 4

	IPv6				IPv4			
Protocol	SA	SP	DA	DP	SA	SP	DA	DP
TCP	3000: :1	10,001	5000: :10	80	128.1.1.1	10,001	130.1.2.1	80

Table 4 shows an existing connection for the third device 310, which is assigned the single public IPv4 address 128.1.1.1 with a port designation of 10,001.

User A

FIG. 4 is a high level flow chart of a process that may be used by the router 306 in an embodiment of the invention for sending packets to a public Internet. In an example of the operation of the invention with an NAT NAT-PT database comprising Table 3 and Table 4, if user A, at the first device 308, sends a packet to the web server 305, the packet sent from the first device 308 to the router 306 may have the following protocol source address, source port, destination address, and destination port numbers:

Protocol	SA	SP	DA	DP
TCP	10.1.1.1	10,000	130.1.1.20	80

The router 306 receives the data packet (step 402). A search is made of the NAT NAT-PT database for a match (step 406). Since the packet is from the private network and is in IPv4 format, only the NAT entries in the NAT table, shown as Table 3, part of the NAT NAT-PT database, are searched. This is because such packets should only come from an IPv4 device, in this example. It is found that the NAT entry in the NAT table, shown as Table 3, matches the data packet (step 410). The packet is then translated (step 414) according to Table 3, so that the resulting packet has the protocol, source address, source port, destination address, and destination port of:

Protocol	SA	SP	DA	DP

Juniper Exhibit 1002, page 252

TCP	128.1.1.1	10,000	130.1.1.20	80

Then the packet is sent from the router 306 to the web server 305 at the destination address (step 418).

The web server 305 may then send a packet back to user A in reply. FIG. 5 is a high level flow chart of a process used by the router 306 for receiving packets from the public Internet. The packet is sent from the web server 305 to the router 306. The router 306 receives the packet (step 502). The packet may have protocol, address and port designations as follows:

Protocol	SA	SP	DA	DP
TCP	130.1.1.20	80	128.1.1.1	10,000

The NAT NAT-PT database 330 is searched for a match (step 506). Since the packet is from the Internet side of the router 306, in this example both NAT entries and NAT-PT entries are searched. This is because the packet could be going to either an IPv4 or IPv6 device. It is found that the entry in the NAT table, shown as Table 3, matches the packet (step 510). The entry in the NAT table is used to translate the packet (step 514) to:

Protocol	SA	SP	DA	DP
TCP	130.1.1.20	80	10.1.1.1	10,000

The packet is then sent to the first device 308 from the router 306 (step 518). If a match is not found, an error step may be done (step 522), such as dropping the packet.

User B

In another example, a TCP data packet is sent from user B at the second device to an IPv4 web server with an address 130.1.1.10 through the Internet 304. The packet may have the following protocol source address, source port, destination address, and destination port numbers:

Protocol	SA	SP	DA	DP
TCP	10.1.1.2	10,000	130.1.1.10	80

The router receives the packet (step 402). The router 306 searches the NAT NAT-PT database to see if such a connection already exists (step 406). Since the packet is from the private network and is in IPv4 format, only the NAT entries in the NAT table, shown as Table 3, part of the NAT NAT-PT database, are searched. Since a match is not found in the NAT NAT-PT database (step 410), the router 306 designates the packet as a new connection. The router 306 assigns a port number to the data packet.

The assignment of a port number not in use may first require a search for a protocol, address, and port combination that is not in use (step 422). This search searches both NAT and NAT-PT entries. This is to avoid conflicts with both IPv4 and IPv6 devices. In one embodiment of the invention, the router 306 may first try to use the port number designated by the packet. In another embodiment, the router 306 may assign a port number, ignoring the port number designate by the packet. In this example, an attempt to assign a port number of 10,000 for a TCP protocol for address 128.1.1.1 may first be performed either because it is the port number designated by the packet or as a default choice by the router. A search of the NAT NAT-PT database is made to see if any existing connections in the NAT NAT-PT database (if any NAT entries or any NAT-PT entries) use port 10,000 of the router 306 for a TCP connection for address 128.1.1.1. It is found that the NAT entry in the NAT table (Table 3) uses port 10,000 for a TCP connection for address 128.1.1.1. Another port is then designated and checked to see if it matches any existing connection. In this embodiment, the port number is incremented from 10,000 to 10,001 for a TCP protocol for address 128.1.1.1. A search of the NAT NAT-PT database is made to see if any existing connections in the NAT NAT-PT database use port 10,001 of the router 306 for a TCP connection for address 128.1.1.1. It is found that the NAT-PT entry in NAT-PT table (Table 4) uses port 10,001 for a TCP connection for address 128.1.1.1. In this embodiment, the port number is incremented from 10,001 to 10,002. A search of the NAT NAT-PT database is made to see if any existing connections in the NAT NAT-PT database 330 use port 10,002 of the router 306 for a TCP connection for

Juniper Exhibit 1002, page 254

address 128.1.1.1. Since no such connection is found, the new connection is assigned the port number of 10,002 for a TCP protocol for address 128.1.1.1. An address, port, and protocol combination not in use has been successfully found.

The address, port, and protocol combination is placed in NAT NAT-PT database (step 426) by being placed in the NAT table, resulting in Table 5.

Table 5

Private					Public			
Protocol	SA	SP	DA	DP	SA	SP	DA	DP
TCP	10.1.1.1	10,000	130.1.1.20	80	128.1.1.1	10,000	130.1.1.20	80
TCP	10.1.1.2	10,000	130.1.1.30	80	128.1.1.1	10,002	130.1.1.30	80

The data packet is then translated, providing a new source address and source port, according to the entry in Table 5 (step 430), to yield:

Protocol	SA	SP	DA	DP
TCP	128.1.1.1	10,002	130.1.1.30	80

Then the packet is sent from the router 306 to the web server at the destination address (step 418).

The web server may then send a packet back to user B in reply. The packet sent from the web server to the router 306 may have address and port designations as follows:

SA	SP	DA	DP
130.1.1.30	80	128.1.1.1	10,002

The router 306 receives the packet (step 502). A search for a match in the NAT NAT-PT database is made (step 506). Both NAT entries and NAT-PT entries are searched in this example, since the packet is from the Internet and it is not known if the destination is an IPv4 or IPv6 device. It is found that the second NAT entry in

the NAT table, shown as Table 5, matches the packet (step 510). Using Table 5, the router 306 translates the destination and source address and port of the packet (step 514) to:

Protocol	SA	SP	DA	DP
TCP	130.1.1.30	80	10.1.1.2	10,000

The packet is sent to the second device 309 (step 518).

User C

Now if user C at the third device 310 sends another data packet, the packet is received by the router 306 (step 402) with the following protocol, addresses, and ports:

Protocol	SA	SP	DA	DP
TCP	3000: :1	10,001	5000: :10	80

Since the destination of the packet is an IPv4 device with an IPv4 address of 130.1.2.10, the router 306 may need to assign an IPv6 address to it, so that the third device 310 may address the packets in an IPv6 format (*e.g.*, in this example, an address of 5000::1 was previously assigned to the destination device).

A search is made of the NAT NAT-PT database for a match with the packet (step 406). Since it is known that the packet is in an IPv6 format, the search may only search through the NAT-PT entries in the NAT-PT part of the NAT NAT-PT database. A match is found with the NAT-PT entry in the NAT-PT database as shown in Table 4 (step 410). The packet is translated according to the match (step 414) to:

SA	SP	DA	DP
128.1.1.1	10,001	130.1.2.10	80

Then the packet is sent from the router 306 to the web server at the destination address (step 418).

The web server may then send a packet back to user C at the third device 310 in reply. The packet is sent from the web server and received by the router 306 (step 502). The packet may have the protocol, address, and port designations as follows:

Protocol	SA	SP	DA	DP
TCP	130.1.2.10	80	128.1.1.1	10,001

A search of the NAT NAT-PT database 330 is made to see if there is a match (step 506). Since the packet is from the Internet side of the router 306, a search of both the NAT entries and NAT-PT entries may be performed. It is found that the packet matches the entry in the NAT-PT table, shown in Table 4 (step 510). The packet is translated (step 514) to:

Protocol	SA	SP	DA	DP
TCP	5000: :10	80	3000: :1	10,001

The IPv6 packet is then sent to the third device 310 (step 518).

User D

In another example, a TCP data packet is sent from user D at the fourth device 311 to an IPv4 web server with an address 130.1.3.10 through the Internet 304. The packet may have the following protocol source address, source port, destination address, and destination port numbers.

Protocol	SA	SP	DA	DP
TCP	3000: :2	10,000	5000: :20	80

The router receives the packet (step 402). The router 306 searches the NAT NAT-PT database to see if such a connection already exists. Since the packet is in an IPv6 format, in this example only the NAT-PT entries in the NAT-PT table are searched to see if there is a matching entry to the source address, source port, destination address, destination port, and protocol combination (step 406). Since a match is not found in the NAT NAT-PT database (step 410), the router 306 designates

the packet as a new connection. The router 306 assigns a port number to the data packet.

The assignment of a port number not in use may first require a search for a protocol, address, and port combination that is not in use (step 422). In one embodiment of the invention, the router 306 may first try to use the port number designated by the packet. In another embodiment, the router 306 may assign a port number, ignoring the port number designated by the packet. In this example, an attempt to assign a port number of 10,000 for a TCP protocol for address 128.1.1.1 may first be performed either because it is the port number designated by the packet or as a default choice by the router. A search of the NAT NAT-PT database is made to see if any existing connections in the NAT NAT-PT database use port 10,000 of the router 306 for a TCP connection for address 128.1.1.1. In this embodiment, both NAT entries and NAT-PT entries are searched to avoid port conflicts with both NAT and NAT-PT connections. It is found that a NAT entry in the NAT table (Table 5) uses port 10,000 for a TCP connection for address 128.1.1.1. Another port is then designated and checked to see if it matches any existing connections. In this embodiment, the port number is incremented from 10,000 to 10,001 for a TCP protocol for address 128.1.1.1. A search of the NAT NAT-PT database is made to see if any existing connections in the NAT NAT-PT database use port 10,001 of the router 306 for a TCP connection for address 128.1.1.1. It is found that the NAT-PT entry in NAT-PT table (Table 4) uses port 10,001 for a TCP connection for address 128.1.1.1. In this embodiment, the port number is incremented from 10,001 to 10,002. A search of the NAT NAT-PT database is made to see if any existing connections in the NAT NAT-PT database 330 use port 10,002 of the router 306 for a TCP connection for address 128.1.1.1. It is found that a NAT entry in the NAT table (Table 5) uses port 10,002 for a TCP connection for address 128.1.1.1. In this embodiment, the port number is incremented from 10,002 to 10,003. A search of the NAT NAT-PT database is made to see if any existing connections in the NAT NAT-PT database 330 use port 10,003 of the router 306 for a TCP connection for address 128.1.1.1. Since no such connection is found, the new connection is assigned the port number of 10,003 for a TCP protocol for address 128.1.1.1. An address, port, and protocol combination not in use has been successfully found.

Juniper Exhibit 1002, page 258

The address, port, and protocol combination is placed in the NAT NAT-PT database (step 426) by being placed in the NAT-PT table, resulting in Table 6.

Table 6

	IPv6				IPv4			
Protocol	SA	SP	DA	DP	SA	SP	DA	DP
TCP	3000: :1	10,001	5000: :10	80	128.1.1.1	10,001	130.1.2.1	80
TCP	3000: :2	10,000	5000: :20	80	128.1.1.1	10,003	130.1.3.1	80

The data packet is then translated, providing a new source address and source port, according to the entry in Table 6 (step 430), to yield:

Protocol	SA	SP	DA	DP
TCP	128.1.1.1	10,003	130.1.3.1	80

Then the IPv4 packet is sent from the router 306 to the web server at the destination address (step 418).

The web server may then send a packet back to user D in reply. The packet sent from the web server to the router 306 may have address and port designations as follows:

SA	SP	DA	DP
130.1.3.1	80	128.1.1.1	10,003

The router 306 receives the packet (step 502). A search for a match in the NAT NAT-PT database is made (step 506). Since the packet is received from the Internet side of the router 306, a search of NAT entries and NAT-PT entries is made. It is found that the second entry in the NAT-PT table, shown as Table 6, matches the packet (step 510). Using Table 6, the router 306 translates the protocol, destination and source address and port of the packet (step 514) to:

Juniper Exhibit 1002, page 259

Protocol	SA	SP	DA	DP
TCP	130.1.3.1	80	3000: :2	10,000

The packet is sent to the fourth device 311 (step 518).

In this embodiment, different protocols may be assigned the same port and address combinations. For example, a UDP message using port 10,000 for 128.1.1.1 would not be a match with the TCP connection using port 10,000 for 128.1.1.1, so that both sessions may run concurrently.

A single IPv4 address was used for the router 306 in this example to show that the inventive device is able to provide NAT and NAT-PT with PAT for a mixture of IPv4 and IPv6 devices using a single address. If multiple IPv4 addresses are used, once all the ports for one address are in use, an algorithm may search a next address for available ports. Other searching algorithms for available ports may be used. For example, ports on different addresses may be used so that different addresses may be used equally, in addition to or alternatively to using different ports.

The invention allows the sharing of IPv4 addresses to provide both NAT and NAT-PT with PAT, instead of requiring that NAT used different IPv4 addresses than NAT-PT. In addition, the invention allows a mixture of IPv4 and IPv6 devices to be connected to the inventive device without needing to know whether a particular device is an IPv4 or IPv6 device, instead of requiring that all IPv4 devices be connected to a NAT device and all IPv6 devices be connected to a separate NAT-PT device or requiring knowledge of the whether a device uses IPv4 or IPv6.

In other embodiments, the NAT NAT-PT database may be divided according to ports instead of whether the translation is NAT or NAT-PT. In other embodiments, the database may be separated in other ways, however, the overall NAT NAT-PT database has both NAT and NAT-PT entries.

The NAT-PT may also be used to accomplish other functions. An example of another function provided by the NAT-PT is described in U.S. Patent Application No.

Juniper Exhibit 1002, page 260

09/920,533, filed July 31, 2001, entitled, "MECHANISMS FOR AVOIDING PROBLEMS ASSOCIATED WITH NETWORK ADDRESS PROTOCOL TRANSLATION", by Daniel C. Biederman.

Generally, the techniques for providing NAT NAT-PT with PAT of the present invention may be implemented on software and/or hardware. For example, it can be implemented in an operating system kernel, in a separate user process, in a library package bound into network applications, on a specially constructed machine, or on a network interface card. In a specific embodiment of this invention, the technique of the present invention is implemented in software, such as an operating system or in an application running on an operating system.

A software or software/hardware hybrid packet processing system of this invention is preferably implemented on a general-purpose programmable machine selectively activated or reconfigured by a computer program stored in memory. Such programmable machine may be a network device designed to handle network traffic. Such network devices typically have multiple network interfaces including frame relay and ISDN interfaces, for example. Specific examples of such network devices include routers and switches. For example, the packet processing systems of this invention may be specially configured routers such as specially configured router models 1600, 2500, 2600, 3600, 4500, 4700, 7200, 7500, and 12000 available from Cisco Systems, Inc. of San Jose, California. A general architecture for some of these machines will appear from the description given below. In an alternative embodiment, the packet processing system (*e.g.*, NAT NAT-PT with PAT device) may be implemented on a general-purpose network host machine such as a personal computer or workstation. Further, the invention may be at least partially implemented on a card (e.g., an interface card) for a network device or a general-purpose computing device.

Referring now to FIG. 6, a router 10 suitable for implementing the present invention includes a master central processing unit (CPU) 62, interfaces 68, and a bus 15 (e.g., a PCI bus). When acting under the control of appropriate software or firmware, the CPU 62 is responsible for such router tasks as routing table computations and network management. It may also be responsible for performing protocol conversions between a first and second protocol (*e.g.*, IPv6 and IPv4), performing port translation and address translations, maintaining NAT –PT or NAT

Juniper Exhibit 1002, page 261

tables, etc. It preferably accomplishes all these functions under the control of software including an operating system (e.g., the Internetwork Operating System (IOS®) of Cisco Systems, Inc.) and any appropriate applications software. CPU 62 may include one or more processors 63, such as a processor from the Motorola family of microprocessors or the MIPS family of microprocessors. In an alternative embodiment, processor 63 is specially designed hardware for controlling the operations of router 10. In a specific embodiment, a memory 61 (such as non-volatile RAM and/or ROM) also forms part of CPU 62. However, there are many different ways in which memory could be coupled to the system. Memory 61 may be used for a variety of purposes such as, for example, caching and/or storing data, programming instructions, etc.

The interfaces 68 are typically provided as interface cards (sometimes referred to as "line cards"). Generally, they control the sending and receiving of data packets or data segments over the network and sometimes support other peripherals used with the router 10. Among the interfaces that may be provided are Ethernet interfaces, frame relay interfaces, cable interfaces, DSL interfaces, token ring interfaces, and the like. In addition, various very high-speed interfaces may be provided such as fast Ethernet interfaces, Gigabit Ethernet interfaces, ATM interfaces, HSSI interfaces, POS interfaces, FDDI interfaces and the like. Generally, these interfaces may include ports appropriate for communication with the appropriate media. In some cases, they may also include an independent processor and, in some instances, volatile RAM. The independent processors may control such communications intensive tasks as packet switching, media control, and management. By providing separate processors for the communications intensive tasks, these interfaces allow the master microprocessor 62 to efficiently perform routing computations, network diagnostics, security functions, etc.

Although the system shown in FIG. 6 is one specific router of the present invention, it is by no means the only router architecture on which the present invention can be implemented. For example, an architecture having a single processor that handles communications as well as routing computations, etc., is often used. Further, other types of interfaces and media could also be used with the router.

Juniper Exhibit 1002, page 262

Regardless of the network device's configuration, it may employ one or more memories or memory modules (such as, for example, memory block 65) configured to store data, program instructions for the general-purpose network operations and/or the inventive techniques described herein. The program instructions may control the operation of an operating system and/or one or more applications, for example. The memory or memories may also be configured to store NAT and NAT-PT entries, received packets and identifiers to track each flow and the number of such flows, etc.

Because such information and program instructions may be employed to implement the systems/methods described herein, the present invention relates to machine-readable media that include program instructions, state information, etc. for performing various operations described herein. Examples of machine-readable media include, but are not limited to, magnetic media such as hard disks, floppy disks, and magnetic tape; optical media such as CD-ROM disks and DVDs; magneto-optical media such as floptical disks; and hardware devices that are specially configured to store and perform program instructions, such as read-only memory (ROM) and random access memory (RAM) devices. The invention may also be embodied in a carrier wave traveling over an appropriate medium such as airwaves, optical lines, electric lines, etc. Examples of program instructions include both machine code, such as produced by a compiler, and files containing higher level code that may be executed by the computer using an interpreter.

Although the foregoing invention has been described in some detail for purposes of clarity of understanding, it will be apparent that certain changes and modifications may be practiced within the scope of the appended claims. For example, the techniques of the present invention may be applied to other conversions besides IPv4 to IPv6 conversions. Therefore, the described embodiments should be taken as illustrative and not restrictive, and the invention should not be limited to the details given herein but should be defined by the following claims and their full scope of equivalents. There are alterations, permutations, and substitute equivalents, which fall within the scope of this invention. It should also be noted that there are many alternative ways of implementing the methods and apparatuses of the present invention. It is therefore intended that the following appended claims be interpreted as

Juniper Exhibit 1002, page 263

including all such alterations, permutations, and substitute equivalents as fall within the true spirit and scope of the present invention.

Juniper Exhibit 1002, page 264

CLAIMS

What is claimed is:

1. A method for transparently sharing at least one IPv4 address among a plurality of hosts wherein at least a first host of the plurality of hosts uses the IPv4 protocol and wherein at least a second host of the plurality of hosts uses an IPv6 protocol, comprising:

receiving a first data having a first source address and a first destination address;

performing a network address translation with port address translation if the first data is in an IPv4 protocol; and

performing a network address translation protocol translation with port address translation if the first data is in an IPv6 protocol.

2. The method, as recited in claim 1, wherein the performing a network address translation with port address translation if the first data is in an IPv4 protocol and the performing a network address translation protocol translation with port address translation if the first data is in an IPv6 protocol can share at least one common IPv4 address, while providing port address translation.

3. The method, as recited in claim 2, further comprising forwarding the first data to an IPv4 service on an Internet.

4. The method, as recited in claim 3, wherein the performing a network address translation with port address translation searches a Network Address Translation and Network Address Translation – Protocol Translation (NAT NAT-PT) database, and wherein the performing a network address translation protocol translation searches the NAT NAT-PT database.

5. The method, as recited in claim 3, wherein the performing the network address translation with port address translation, comprises:

searching at least part of an NAT NAT-PT database for a match with the first data; and

translating the packet if a match to an entry in the NAT NAT-PT is found,

Juniper Exhibit 1002, page 265

wherein the packet is translated according to the found entry.

6. The method, as recited in claim 5, wherein the performing the network address translation protocol translation with port address translation, comprises:

searching at least part of the NAT NAT-PT database for a match with the first data; and

translating the packet if a match to an entry in the NAT NAT-PT is found, wherein the packet is translated according to the found entry.

7. The method, as recited in claim 6, wherein the performing the network address translation with port address translation further comprises searching both network address translation entries and network address translation protocol translation entries for a protocol, address, and port combination not in use if a match with the first data not found.

8. The method, as recited in claim 3, wherein the performing the network address translation with port address translation comprises searching both network address translation entries and network address translation protocol translation entries for a protocol, address, and port combination not in use.

9. The method, as recited in claim 1, wherein the performing the network address translation with port address translation comprises searching both network address translation entries and network address translation protocol translation entries for a protocol, address, and port combination not in use.

10. A computer system operable for providing transparent sharing at least one IPv4 address among a plurality of hosts wherein at least a first host of the plurality of hosts uses the IPv4 protocol and wherein at least a second host of the plurality of hosts uses an IPv6 protocol, comprising:

one or more processors;

one or more memory, wherein at least one of the processors and memory are adapted to:

receive a first data having a first source address and a first destination address;

Juniper Exhibit 1002, page 266

perform a network address translation with port address translation if the first data is in an IPv4 protocol; and

perform a network address translation protocol translation with port address translation if the first data is in an IPv6 protocol.

11. The computer system, as recited in claim 10, wherein the processors and memory are further adapted to forward the first data to an IPv4 service on an Internet, and wherein the performing a network address translation with port address translation if the first data is in an IPv4 protocol and the performing a network address translation protocol translation with port address translation if the first data is in an IPv6 protocol share at least one common IPv4 address, while providing port address translation.

12. The computer system, as recited in claim 11, wherein the performing a network address translation with port address translation searches an NAT NAT-PT database, and wherein the performing a network address translation protocol translation searches the NAT NAT-PT database.

13. The computer system, as recited in claim 12, wherein the performing the network address translation with port address translation further comprises searching both network address translation entries and network address translation protocol translation entries for a protocol, address, and port combination not in use if a match with the first data is not found.

14. The computer system, as recited in claim 10, wherein the performing the network address translation with port address translation further comprises searching both network address translation entries and network address translation protocol translation entries for a protocol, address, and port combination not in use if a match with the first data is not found.

15. A computer program product for providing transparent sharing at least one IPv4 address among a plurality of hosts wherein at least a first host of the plurality of hosts uses the IPv4 protocol and wherein at least a second host of the plurality of hosts uses an IPv6 protocol, comprising:

Juniper Exhibit 1002, page 267

at least one computer readable medium;

computer program instructions stored within the at least one computer readable product configured to:

receive a first data having a first source address and a first destination address;

perform a network address translation with port address translation if the first data is in an IPv4 protocol; and

perform a network address translation protocol translation with port address translation if the first data is in an IPv6 protocol.

16. The computer program product, as recited in claim 15, wherein the computer instructions are further configured to forward the first data to an IPv4 service on an Internet, and wherein the performing a network address translation with port address translation if the first data is in an IPv4 protocol and the performing a network address translation protocol translation with port address translation if the first data is in an IPv6 protocol share at least one common IPv4 address, while providing port address translation.

17. The computer program product, as recited in claim 16, wherein the performing a network address translation with port address translation searches an NAT NAT-PT database, and wherein the performing a network address translation protocol translation searches the NAT NAT-PT database.

18. The computer program product, as recited in claim 17, wherein the performing the network address translation with port address translation further comprises searching both network address translation entries and network address translation protocol translation entries for a protocol, address, and port combination not in use.

19. The computer program product, as recited in claim 16, wherein the performing the network address translation with port address translation further comprises searching both network address translation entries and network address translation protocol translation entries for a protocol, address, and port combination not in use.

Juniper Exhibit 1002, page 268

20. An apparatus for providing transparent sharing at least one IPv4 address among a plurality of hosts wherein at least a first host of the plurality of hosts uses the IPv4 protocol and wherein at least a second host of the plurality of hosts uses an IPv6 protocol, comprising:

means for receiving a first data having a first source address and a first destination address;

means for performing a network address translation with port address translation if the first data is in an IPv4 protocol; and

means for performing a network address translation protocol translation with port address translation if the first data is in an IPv6 protocol.

21. The apparatus, as recited in claim 20, further comprising means for forwarding the first data to an IPv4 service on an Internet, and wherein the means for performing a network address translation with port address translation if the first data is in an IPv4 protocol and the means for performing a network address translation protocol translation with port address translation if the first data is in an IPv6 protocol share at least one common IPv4 address, while providing port address translation.

22. The apparatus, as recited in claim 21, wherein the means for performing a network address translation with port address translation comprises means for searching an NAT NAT-PT database, and wherein the means for performing a network address translation protocol translation comprises means for searching the NAT NAT-PT database.

23. The apparatus, as recited in claim 22, wherein the means for performing the network address translation with port address translation further comprises means for searching both network address translation entries and network address translation protocol translation entries for a protocol, address, and port combination not in use.

24. The apparatus, as recited in claim 21, wherein the means for performing the network address translation with port address translation further comprises means for searching both network address translation entries and network address translation protocol translation entries for a protocol, address, and port combination not in use.

Juniper Exhibit 1002, page 269

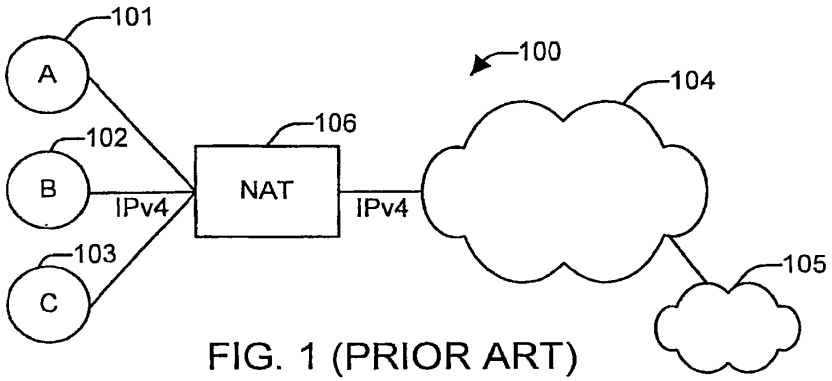


FIG. 1 (PRIOR ART)

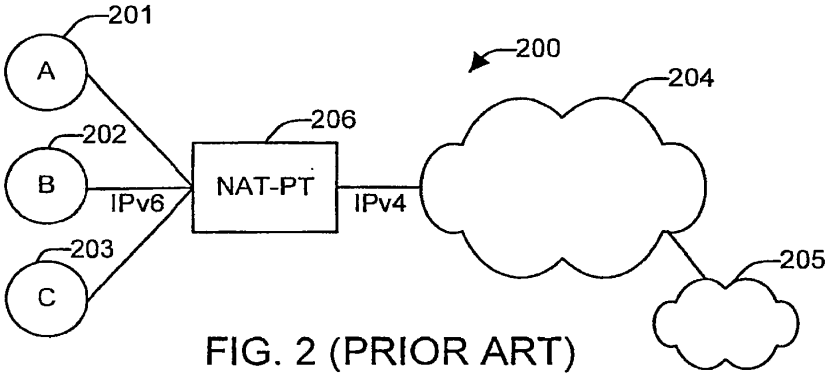


FIG. 2 (PRIOR ART)

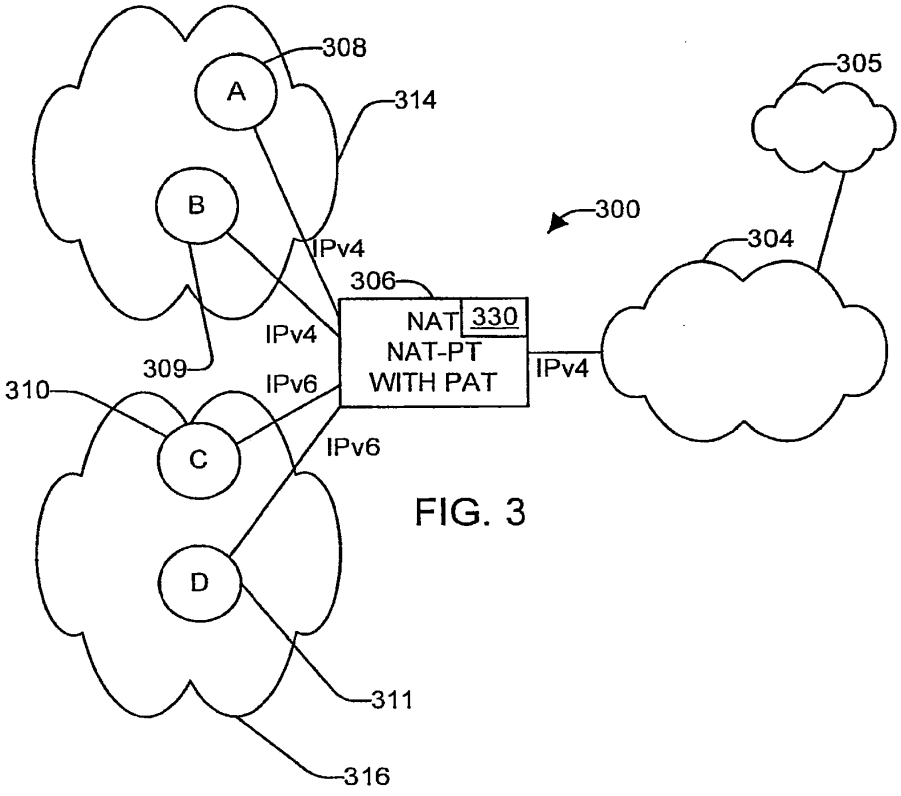

308
A
314
305
B
300
304
IPv4
306
NAT 330
NAT-PT
WITH PAT
IPv4
IPv4
309
IPv6
310
IPv6
C
D
311
316

FIG. 3

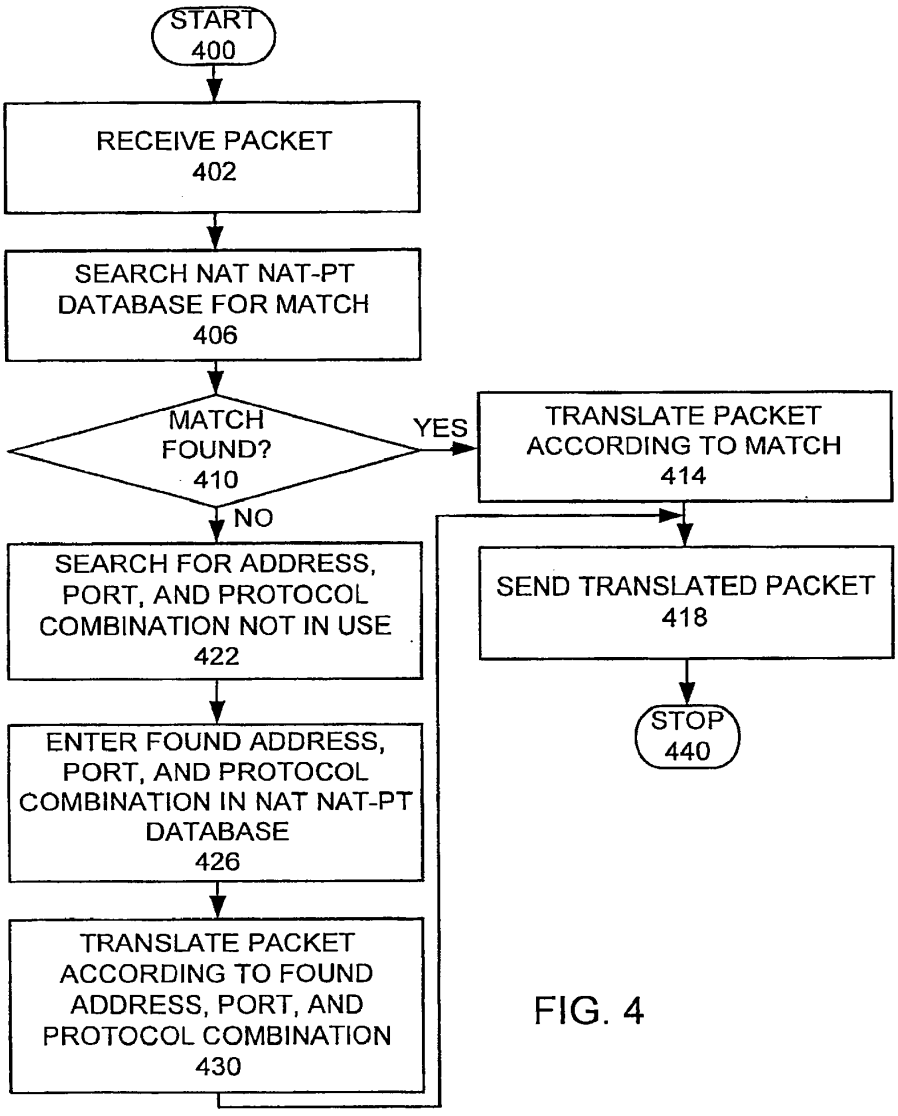

START
400
RECEIVE PACKET
402
SEARCH NAT NAT-PT DATABASE FOR MATCH
406
MATCH FOUND?
410
YES
NO
TRANSLATE PACKET ACCORDING TO MATCH
414
SEND TRANSLATED PACKET
418
STOP
440
SEARCH FOR ADDRESS, PORT, AND PROTOCOL COMBINATION NOT IN USE
422
ENTER FOUND ADDRESS, PORT, AND PROTOCOL COMBINATION IN NAT NAT-PT DATABASE
426
TRANSLATE PACKET ACCORDING TO FOUND ADDRESS, PORT, AND PROTOCOL COMBINATION
430

FIG. 4

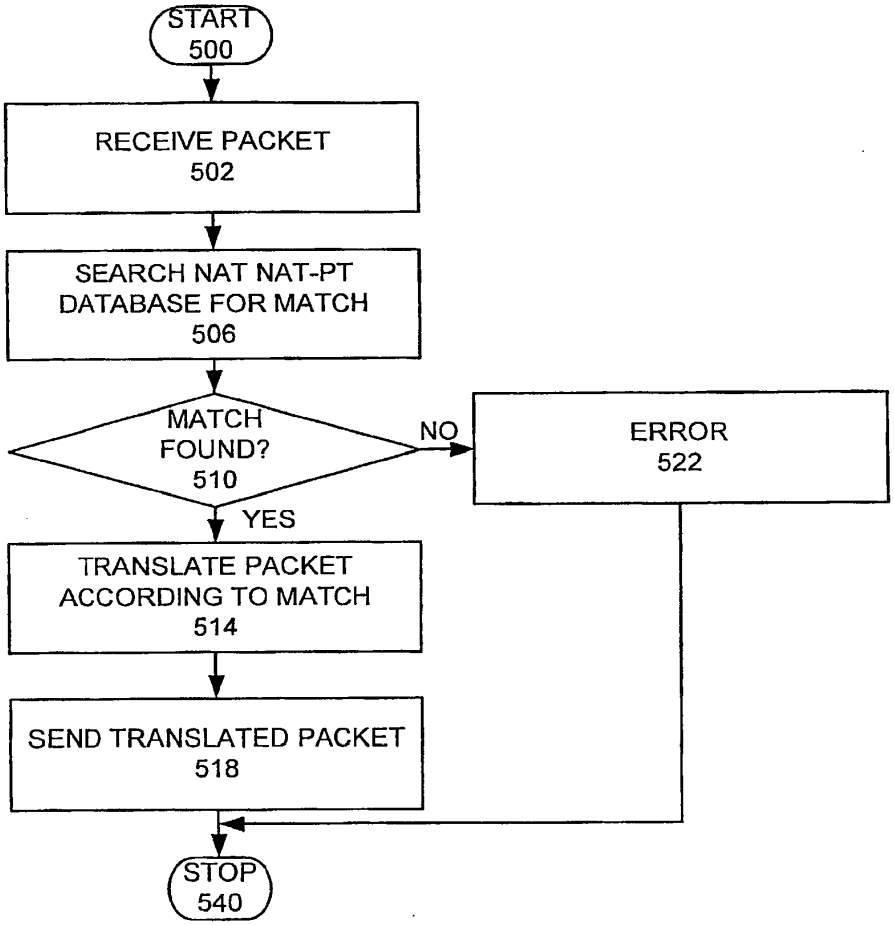

START
500
RECEIVE PACKET
502
SEARCH NAT NAT-PT
DATABASE FOR MATCH
506
MATCH
FOUND?
510
NO
ERROR
522
YES
TRANSLATE PACKET
ACCORDING TO MATCH
514
SEND TRANSLATED PACKET
518
STOP
540

FIG. 5

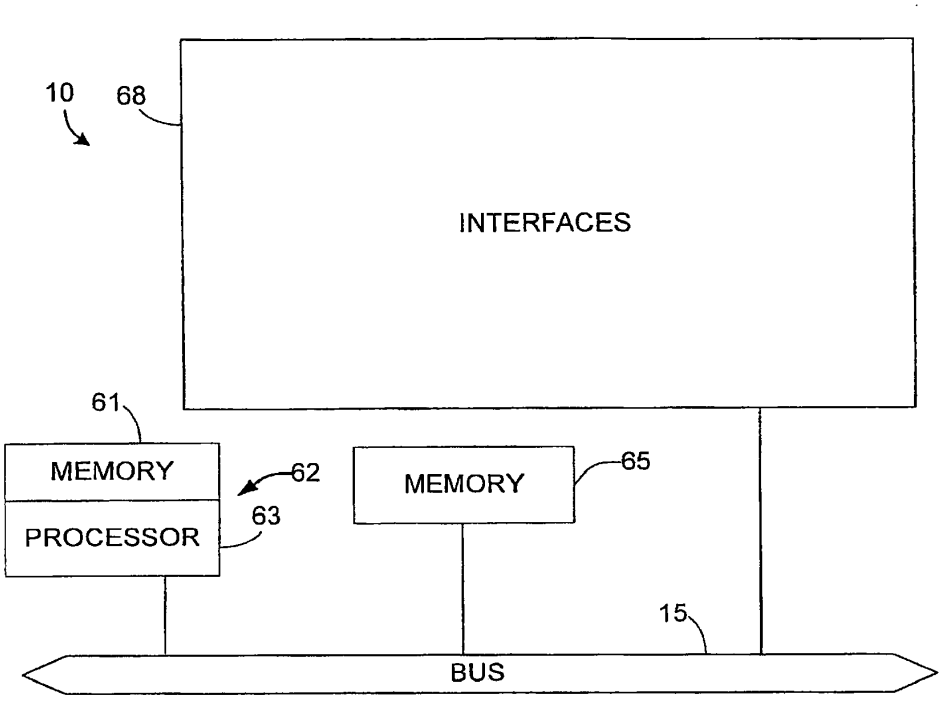


FIG. 6

INTERNATIONAL SEARCH REPORT

Internatio pplication No.
PCT/US 03/32959

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/46 H04L29/06

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, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	TSIRTSIS G ET AL: "Network Address Translation - Protocol Translation (NAT-PT)" RFC 2766, February 2000 (2000-02), XP002167711 Retrieved from the Internet: <URL:http://www.faqs.org/rfcs/rfc2766.html > 'retrieved on 2001-05-18! abstract paragraphs '0001!,'02.1!,'02.2!,'2.2.1!,'0003!,'03.1! ,'03.2!,'04.2!,'0010! --- -/--	1-24

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

[X] 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
13 February 2004	25/03/2004

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

Form PCT/ISA/210 (second sheet) (July 1992)

CI

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 03/32959

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	E. NORDMARK: "Stateless IP/ICMP Translation Algorithm (SIIT)" RFC 2765, 'Online! February 2000 (2000-02), XP002270294 Retrieved from the Internet: <URL:http://www.ietf.org/rfc/rfc2765.txt?number=2765> 'retrieved on 2004-02-12! abstract paragraphs '0001!,'01.2!,'0003!,'03.1!,'0004!,'04.1! ---	1-24
A	WO 02 073933 A (HOVELL PETER ;BRITISH TELECOMM (GB); KING JOHN ROBERT (GB)) 19 September 2002 (2002-09-19) figures 1,4 page 2, line 7 -page 3, line 23 page 4, line 30 -page 14, line 7 -----	1-24

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

Juniper Exhibit 1002, page 276

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US 03/32959

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 02073933 A	19-09-2002	CA 2435985 A1	19-09-2002
		EP 1366613 A1	03-12-2003
		WO 02073933 A1	19-09-2002

Form PCT/ISA/210 (patent family annex) (July 1992)

Juniper Exhibit 1002, page 277

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 420 559 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
19.05.2004 Bulletin 2004/21

(51) Int Cl.[7]: **H04L 29/06**, H04L 12/46

(21) Application number: **02292825.3**

(22) Date of filing: **13.11.2002**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL PT SE SK TR
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **Thomson Licensing S.A.**
92100 Boulogne-Billancourt (FR)

(72) Inventors:
- **Lepoil, Elisabeth**
  35135 Chantepie (FR)
- **Van Aken, Dirk**
  1083 Ganshoren (BE)

(74) Representative: **Kohrs, Martin et al**
Thomson multimedia
46, quai A. Le Gallo
92648 Boulogne Cedex (FR)

(54) Method and device for supporting a 6to4 tunneling protocol across a network address translation mechanism

(57) A method for supporting a 6to4 tunneling protocol across a network address translation mechanism. The method comprises the steps of receiving an outbound IPv6 packet encapsulated into an IPv4 packet, translating the private IPv4 source address in the IPv4 header of the outbound packet into a public IPv4 source address, transmitting the translated packet over the IPv4 network; and is characterized in that it further comprises the step of storing an association of the private IPv4 address and the Interface ID value of the 6to4 source address for opposite address translation of inbound packets.

A corresponding device is also claimed.

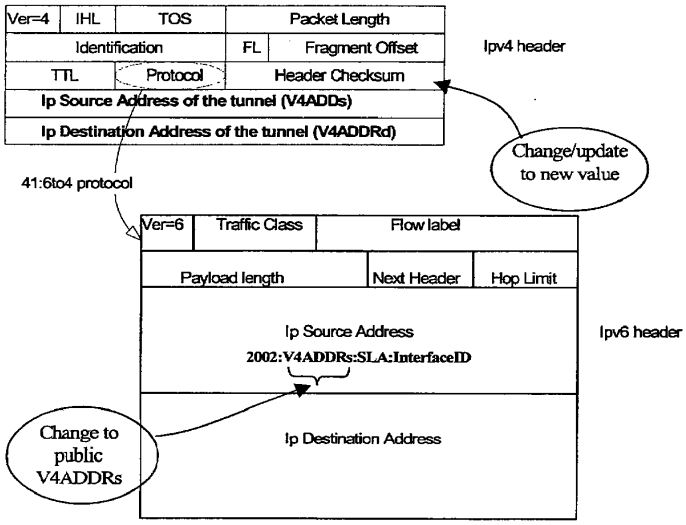


Fig. 4

Printed by Jouve, 75001 PARIS (FR)

EP 1 420 559 A1

Description

[0001] The invention concerns a method and device for supporting a 6to4 tunneling protocol across a network address translation mechanism.

[0002] As described in the IETF documents RFC 1631, RFC 2663 and RFC 3022, Network Address Translation ('NAT') translates IPv4 addresses of a first address domain ('Private IPv4 addresses') into IPv4 addresses of a second address domain ('Public IPv4 addresses'). The translation is carried out on the source addresses of outgoing packets and on destination addresses of incoming packets going through the NAT. Typically, the NAT is a function integrated in a router, connecting for example two IPv4 networks using different and incompatible IP addressing schemes.

[0003] There exist two basic types of NAT: either the process consists in substituting addresses with a one-to-one correspondence (i.e. each first domain address is associated with a unique second domain address) or in associating several first domain addresses with a single second domain address. The first NAT type is referred to as 'N:N NAT' and the second type as 'X:Y NAT', in the context of this document.

[0004] A problem linked to the use of X:Y NAT is that if the NAT's translation table solely consists of IP address mapping information it will not allow to uniquely identify the source host, since during the translation, X private addresses were translated into Y public addresses (with Y<X), which results in a loss of information. Consequently, the NAT has to use additional session information in order to be able to make the opposite translation, and to support a bi-directional communication. But, there aren't any fields in the IP header of a packet to unambiguously identify a session so a "multiplexing/de-multiplexing identifier" (abbreviated as "multiplexing identifier further in this document) needs to be defined for each protocol running over IP. Protocols such as TCP and UDP have the notion of 'port' which is used by NAT to create look-up tables to make the backward translation possible. For applications that run over other IP transport protocols or directly on IP, dedicated session information has to be identified for each protocol. Alternatives have been proposed to make those "portless protocols" transparently crossing NAT. For instance,

the document "Teredo: Tunneling IPv6 over UDP through NATs" by C. Huitema (Internet Draft of September 17, 2002) describes an alternative method for providing services to IPv6 nodes located behind a NAT device. However, transporting IPv6 over UDP introduces an additional overhead and consequently has an influence on performance. Furthermore, additional specific servers have to be introduced into the network and the IPv6 hosts have to be upgraded.

[0005] Another alternative is described in the document "Realm Specific IP: Framework" RFC 3102 of October 2001. However, as for the protocol described in the previous paragraph, additional servers are required and hosts need to be upgraded.

[0006] The document 'Setup of 6to4 (NAT version)' available from www.6to4.jp/settings/nat.html describes a NAT functionality in which the IPv4 address part of an 6to4 header of an IPv6 packet encapsulated in an IPv4 packet is updated with a public IPv4 address, resp. a private IPv4 address for outbound resp. inbound packets.

[0007] The invention concerns a method for supporting the 6to4 tunneling protocol (which is also a portless protocol), defined in RFC 3015, across NAT. The 6to4 protocol defines a mechanism for IPv6 sites to communicate with others IPv6 sites or with native IPv6 networks over an IPv4 network without explicit tunnel setup.

[0008] The method comprises the steps of :

- receiving an outbound IPv6 packet encapsulated into an IPv4 packet,
- translating the private IPv4 source address in the IPv4 header of the outbound packet into a public IPv4 source address,
- transmitting the translated packet over the IPv4 network;

characterized in that it further comprises the step of:

- storing an association of the private IPv4 address and the Interface ID value of the 6to4 source address for opposite address translation of inbound packets.

[0009] The value of the Interface Identifier is preserved by the destination host when sending back a response packet. It is used as a multiplexing identifier to enable the device to send the incoming packet to the right host, substituting the destination address with the previously stored address.

[0010] According to a particular embodiment of the invention, the method further comprises the steps of:

- receiving an inbound packet over the IPv4 network;
- determining whether the inbound packet encapsulates an IPv6 packet;
- in the affirmative, retrieving the Interface ID of the encapsulated IPv6 packet's destination address, and using the Interface ID to retrieve the corresponding stored private IPv4 address, and updating the destination address in the IPv4 header accordingly;

CI

Juniper Exhibit 1002, page 279

- forwarding the modified 6to4 packet on the first network.

[0011] According to a particular embodiment of the invention, the method further comprises the step of:

- changing the IPv4 address part of the 6to4 source address in the IPv6 header of an outbound packet to the public IPv4 address.

[0012] According to a particular embodiment of the invention, the method further comprises the steps of:

- changing the IPv4 address part of the 6to4 destination address of an inbound packet to the corresponding private IPv4 address

[0013] Figure 1 represents two IPv6 networks connected by an IPv4 network through respective routers. The left network router is connected to or integrates NAT, whether of the N:N NAT type or of the X:Y NAT type.

[0014] If, for example, in figure 1, Host 3 wishes to respond to a packet sent by Host 1, Host 3 will base the destination address of the response packet on the IPv6 source address contained in the IPv6 packet received from router r2. This IPv6 source address contains Host 1's private IPv4 address.

[0015] Router r2 builds the IPv4 header of the response packet from the IPv6 header of this packet; more precisely, the IPv4 destination address is extracted from the IPv6 destination address of Host 3 i.e the IPv4 destination address will be equal to Host1's private IPv4 address. The response packet will never be delivered (or it will be misrouted), because the private IPv4 address is not properly recognized on the IPv4 network.

[0016] This is solved by the above additional characteristic, according to which the inner IPv6 header of an outbound (6to4) packet is adapted to be coherent with the outer IPv4 header, as modified by the NAT process.

[0017] According to a particular embodiment of the invention, the method further comprises the step of modifying fields at least of the IPv4 header, such as checksums, whose values depend on the 6to4 source address.

[0018] According to a particular embodiment of the invention, the step of storing the association of the Interface ID and the source address of the 6to4 packets of the first network and the step of modifying the destination address of inbound packets as a function of the Interface ID, respectively the step of changing the IPv4 part of the 6to4 address are carried out by an application level gateway assisting the network address translation mechanism.

[0019] Another object of the invention is a device for supporting a 6to4 tunneling protocol across NAT, comprising:

- a network address translation mechanism for changing the private source address of an outbound IPv4 packet encapsulating an IPv6 packet into a public source address;

characterized in that it further comprises

an application for storing the private IPv4 addresses included in the 6to4 source address of a host of the IPv6 network, for outbound packets; and for updating the 6to4 destination address of an inbound packet with a stored private IPv4 address having same Interface ID as the 6to4 destination address.

[0020] According to an embodiment of the invention, the application is further adapted to carry out additional processing of an outbound packet, wherein the additional processing consists in replacing the private IPv4 address part of an 6to4 source address of an outbound packet with the device's public IPv4 address.

[0021] Other characteristics and advantages of the invention will appear in the description of a non-restrictive embodiment, explained with the help of the enclosed drawings, among which:

- Figure 1 is a diagram of two IPv6 networks connected through an IPv4 network using Network Address Translation (NAT) according to the embodiment of the invention;
- Figure 2, which as such is prior art, is a diagram of the '6to4' address format;
- Figure 3, which as such is prior art, is a diagram showing how an IPv6 packet is encapsulated into an IPv4 packet;
- Figure 4 is a diagram showing the modifications made to the IPv4 header and the encapsulated IPv6 header according to the embodiment.

[0022] Figure 1 is a diagram of two IPv6 networks A and B connected through an IPv4 network. Network A comprises two hosts, resp. 1 and 2, connected to the IPv4 network through a 6to4 router r1. Similarly, network B comprises two hosts 3 and 4, as well as a 6to4 router r2. By placing IPv6/IPv4 border routers between the IPv6 networks and the IPv4 network, the isolated IPv6 clusters can be linked via so-called 6to4 tunnels.

[0023] Figure 2 illustrates the IPv6 address format. Each IPv6 network is assigned a unique '6to4 format prefix', comprising a 3 bit format prefix ('FP'), a 13 bit predetermined identifier called the 'IPv6 Top Level Aggregator' ('TLA'), a globally unique IPv4 address ('V4ADDR'), a 16 bit Site Level Aggregator Identifier ('SLA ID') and lastly the 64-bit link

CI

Juniper Exhibit 1002, page 280

level host identifier (Interface ID). The latter two identifiers form a host's locally unique identifier. The Interface ID is, for instance, the host's MAC address. It can also be equal, for example, to the private, locally unique IPv4 address of the host.

[0024] Establishment of a tunnel by the 6to4 routers is conditioned by the use of predefined values for certain fields in the destination address of a packet. As described in RFC 3056 of February 2001, the concatenated FP and TLA fields have to have the value '2002'

[0025] The 6to4 address prefixes for networks A and B are respectively '2002:V4ADDR-r1/48' and '2002:V4ADDR-r2/48', where V4ADDR-r1 and V4ADDR-r2 are the globally unique IPv4 addresses assigned to the tunnel endpoints (router r1 and router r2, respectively).

[0026] Hosts of a IPv6 network are configured, or auto-configured via router advertisements, with IPv6 addresses composed of the 6to4 prefix assigned to the IPv6 network and the host's locally unique identifier (SLA / Interface ID).

[0027] Note that a 6to4 tunnel can also be defined directly between isolated 6to4 hosts without passing through a 6to4 router. In that case, the IPv4 address of the tunnel endpoint is the IPv4 address of the host.

[0028] All packets on a IPv6 network having a destination address comprising a 6to4 prefix different from the network's 6to4 prefix are forwarded to the 6to4 border router. The router is responsible for encapsulating the IPv6 packets in IPv4 packets, as illustrated by figure 3. The IPv4 header of such a packet encapsulating IPv6 can be referred to as an 'outer' header, while the IPv6 header of the encapsulated IPv6 packet can be referred to as an 'inner' header. The IPv4 header contains the IPv4 source and destination addresses of the tunnel endpoints (i.e. the 'V4ADDR' addresses of the routers). The IPv6 header contains the IPv6 source and destination addresses of the hosts.

[0029] Encapsulated 6to4 packets received by the destination router are extracted, and the native IPv6 packets are forwarded to the proper host.

[0030] Figure 4 illustrates IPv4 and IPv6 headers in the present encapsulation scheme. For the 6to4 protocol, the 'protocol' field in the outer IPv4 header has value '41'. Further details concerning the contents of the IPv6 header fields can be found in RFC 2460. Note that the items labeled as 'changes' are amendments to the headers made according to the present embodiment.

[0031] While traditional N:N NAT and X:Y NAT operate only on the outer header of the packets (the IPv4 address in the inner header remains unchanged), the NAT according to the present embodiment also reflects the translation at the level of the inner header.

[0032] As illustrated by figure 1, according to the present embodiment, the NAT is assisted by an "Application Level Gateway" for the specific processing required for the 6to4 protocol.. As defined in RFC 2663, an ALG is an application-specific translation agent that allows an application on a host in one address realm to connected to its counterpart running on a host in a different realm. In the present example, the ALG is integrated into the router, along with the NAT.

[0033] The 6to4 ALG operates on packets sent by applications running over the 6to4 protocol. It detects the 6to4 prefix of packets and, for the detected packets, carries out the following processing:

(a) In the inner IPv6 header, replace the private IPv4 address ('V4ADDR') of the 6to4 prefix with the public IPv4 address for outgoing packets and vice versa for incoming packets.

(b) Update fields depending on the 6to4 prefix. In particular, checksums are concerned. This applies for example to the transport header checksums (e.g. the TCP or the UDP header). This applies also to any upper layer fields embedding the 6to4 prefix, such as it is the case in FTP (e.g. the whole prefix has to be replaced in the payload of an FTP packet (EPTR field)).

[0034] The coherence between the inner and the outer header is then restored. This solves the problem of incorrect packet delivery, in particular a response packet to a 6to4 packet going through a NAT functionality. The responding host, e.g. when Host 3 of figure 1 responds to Host 1, Router 2 will use the public IPv4 address in the modified 6to4 prefix to generate an IPv4 destination address for Host3 response packet. The response packet will then be correctly sent to router r1.

[0035] For the same reason, incorrect DNS records and wrongly populated forwarding databases and routing tables are avoided.

(c) According to the present embodiment, the 6to4 ALG further has the task of uniquely associating inbound and outbound traffic packets. The 6to4 ALG carries out the following processing. The NAT ALG maintains a list for mapping 6to4 destination addresses of inbound packets to the correct private 6to4 host address for packets returned by a remote host. It picks up a 'multiplexing identifier' from the outbound packets, in order to allow this mapping to be carried out.

[0036] According to the present embodiment, the multiplexing identifier is picked up from field(s) of the IPv6 header of the outbound packet. In fact, according to the present embodiment, an identifier already present in the IPv6 header

CI

Juniper Exhibit 1002, page 281

is chosen as a multiplexing identifier. This identifier is chosen based on the characteristic that it is preserved by the remote host and unique on the originating network.

[0037] According to the present embodiment, the 'InterfaceID' field of the 6to4 source address is used as a unique identifier of the origin of an outbound packet by the 6to4 ALG. This field corresponds to the uniqueness and preservation criteria defined above. 'Preservation' does not mean that the identifier has to remain at the same location within the header, but simply that the 6to4 ALG will be able to recover it from a predetermined location in the header. In the present case, the remote host will of course swap the source and destination addresses in the response(s), so the location of the identifier within the header changes.

[0038] The 6to4 ALG consequently maintains a table having the following content:

Table 1

InterfaceID	IPv4 address of the host having sent an outbound packet (source address of the outbound packet before translation by NAT)
...	...

[0039] This table can also be stored under the form of a list of 6to4 addresses, since these addresses already contain the identifier.

[0040] The table is completed with a "6to4 entry" for each outbound session initiated from site 1. For each inbound packet, the 6to4 ALG will, based on the InterfaceID identifier in the destination address of the inbound packet, extract the corresponding private IPv4 address valid on the local network and replace the destination address in the inbound packet with this extracted value, before forwarding the packet on the local network.

[0041] A "6to4 entry" remains valid until the session timeout, managed by the NAT function, expires.

[0042] Although the present embodiment concerns IP addressing, the principles of the invention may be applied to other portless protocols, such as e.g. ICMP, ESP and GRE. The criteria of choice of the multiplexing identifier remain the same as those in the present embodiment. For ESP, the 'SPI' field can be used, while for GRE, the CallID field is appropriate.

Claims

1. Method for supporting a 6to4 tunneling protocol across a network address translation mechanism comprising the steps of :

   - receiving an outbound IPv6 packet encapsulated into an IPv4 packet,
   - translating the private IPv4 source address in the IPv4 header of the outbound packet into a public IPv4 source address,
   - transmitting the translated packet over the IPv4 network;

   characterized in that it further comprises the step of:

   - storing an association of the private IPv4 address and the Interface ID value of the 6to4 source address for opposite address translation of inbound packets.

2. Method according to claim 1, further comprising the steps of:

   - receiving an inbound packet over the IPv4 network;
   - determining whether the inbound packet encapsulates an IPv6 packet;
   - in the affirmative, retrieving the Interface ID of the encapsulated IPv6 packet's destination address, and using the Interface ID to retrieve the corresponding stored private IPv4 address, and updating the destination address in the IPv4 header accordingly;
   - forwarding the modified 6to4 packet on the first network.

3. Method according to one of the claims 1 or 2, further comprising the step of:

   - changing the IPv4 address part of the 6to4 source address in the IPv6 header of an outbound packet to the public IPv4 address; and
   - changing the IPv4 address part of the 6to4 destination address of an inbound packet to the corresponding

CI

Juniper Exhibit 1002, page 282

private IPv4 address.

4. Method according to claim 3, comprising the step of modifying fields at least of the IPv4 header, such as checksums, whose values depend on the 6to4 source address.

5. Method according to claim 2, wherein the step of storing the association of the Interface ID and the source address of the 6to4 packets of the first network and the step of modifying the destination address of inbound packets or the source address of outbound packets as a function of the Interface ID is carried out by an application level gateway assisting the network address translation mechanism.

6. Method according to claim 3 or 4, wherein the step of changing the IPv4 part of the 6to4 address are carried out by an application level gateway assisting the network address translation mechanism.

7. Device for supporting a 6to4 tunneling protocol across a network address translation mechanism, comprising:

- a network address translation mechanism (NAT) for changing the private source address of an outbound IPv4 packet encapsulating an IPv6 packet into a public source address;

characterized in that it further comprises
an application (ALG) for storing the private IPv4 addresses included in the 6to4 source address of a host of the IPv6 network, for outbound packets; and for updating the 6to4 destination address of an inbound packet with a stored private IPv4 address having same Interface ID as the 6to4 destination address.

8. Device according to claim 7, wherein the application is further adapted to carry out additional processing of an outbound packet, wherein the additional processing consists in replacing the private IPv4 address part of an 6to4 source address of an outbound packet with the device's public IPv4 address.

CI

Juniper Exhibit 1002, page 283

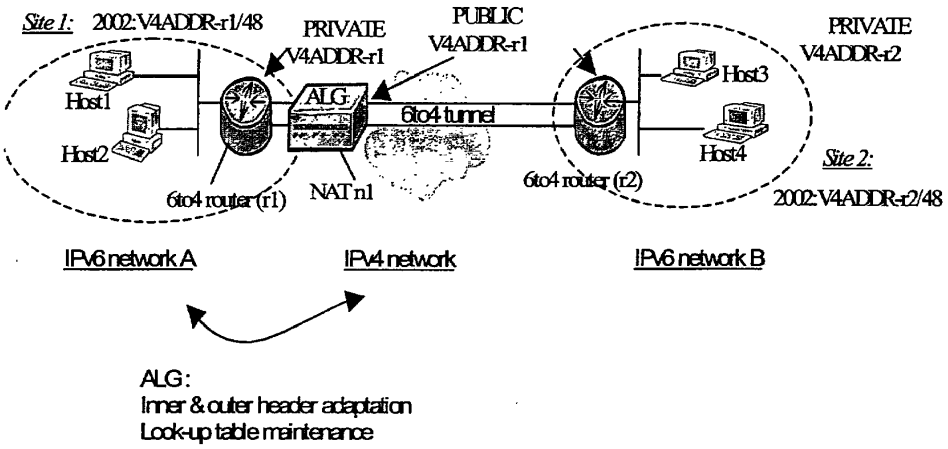


Fig. 1

FP	TLA ID	V4ADDR	SLA ID	Interface ID
001 (3 bits)	0x0002 (13 bits)	(32 bits)	(16 bits)	(64 bits)

6to4 address prefix (2002:V4ADDR::/48)

FP : Format prefix
TLA ID : Top Level Aggregator ID
V4ADDR : IPv4 address of the tunnel
SLA ID : Site Level Aggregator ID
Interface ID : Link Level Host identifier

Fig. 2 (Prior art)

CI

Juniper Exhibit 1002, page 284

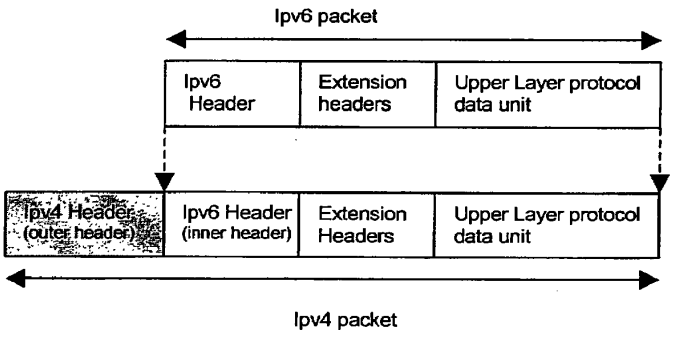


Fig. 3 (Prior art)

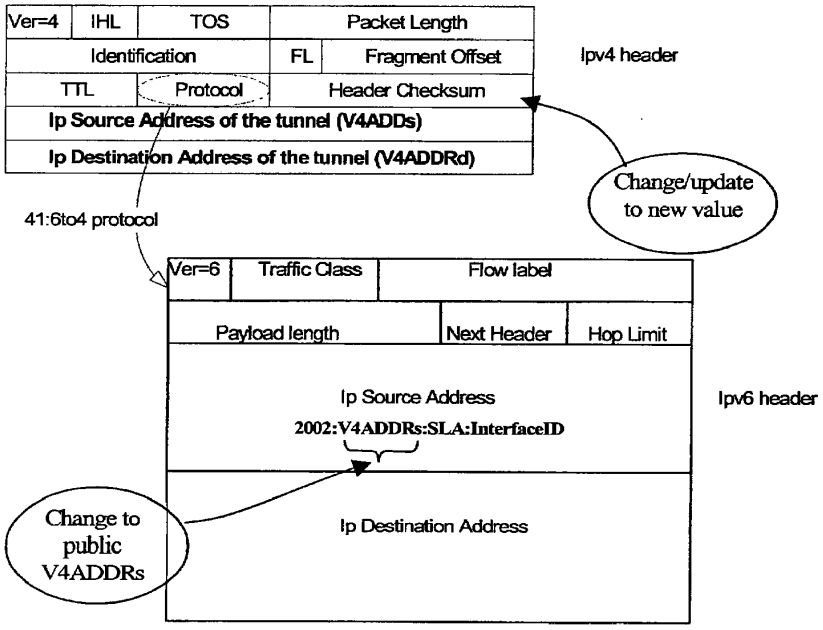


Fig. 4

CI

Juniper Exhibit 1002, page 285

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 02 29 2825

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
D,Y	"Connection of IPv6 Domains via IPv4 Clouds" RFC 3056, XP002240357 * page 6, paragraphs 5,6 * * page 17, paragraphs 1,2 *	1-8	H04L29/06 H04L12/46
Y	US 2002/062388 A1 (OGIER RICHARD G ET AL) 23 May 2002 (2002-05-23)	1,2,7,8	
A	* paragraphs [0282],[0302],[0306]-[0309],[0312] *	3-6	
D,Y	"Setup of 6to4 (NAT version)" INTERNET, [Online] XP002240358 Retrieved from the Internet: <URL:www.6to4.jp/settings/nat.html> [retrieved on 2003-05-07] * the whole document *	3	
D,Y	SRISURESH P ET AL: "RFC 2663 - IP Network Address Translator (NAT) Terminology and Considerations" RFC 2663, August 1999 (1999-08), XP002204216 * page 5, paragraphs 3,4 * * page 9, paragraph 3 *	4-6	
A	BIEMOLT W ET AL: "- An overview of the introduction of IPv6 in the Internet" XP002198867, July 2001 (2001-07), XP002198867 sections 3,4	1-8	
A	EP 1 087 575 A (BRITISH TELECOMM) 28 March 2001 (2001-03-28) * the whole document *	1-8	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)
H04L

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
MUNICH	8 May 2003	Hackl, A

CATEGORY OF CITED DOCUMENTS
X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

CI

Juniper Exhibit 1002, page 286

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 02 29 2825

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

08-05-2003

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002062388 A1	23-05-2002	AU 9455001 A	26-03-2002
		WO 0223832 A2	21-03-2002
		AU 4748801 A	24-09-2001
		WO 0169862 A2	20-09-2001
		US 2002012320 A1	31-01-2002
EP 1087575 A	28-03-2001	EP 1087575 A1	28-03-2001
		AU 7437200 A	24-04-2001
		EP 1214816 A1	19-06-2002
		WO 0122664 A1	29-03-2001

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

CI

Juniper Exhibit 1002, page 287

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

PCT

(43) Date de la publication internationale
7 septembre 2007 (07.09.2007)

(10) Numéro de publication internationale
WO 2007/099248 A2

(51) Classification internationale des brevets :
H04L 29/12 (2006.01) *H04L 29/06* (2006.01)
H04L 29/08 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2007/050808

(22) Date de dépôt international :
15 février 2007 (15.02.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0650681 28 février 2006 (28.02.2006) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 Place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BOUCADAIR, Mohamed** [FR/FR]; 124, rue Saint Jean, F-14000 Caen (FR). **NOISETTE, Yoann** [FR/FR]; 2, rue Dom Aubourg, F-14320 May Sur Orne (FR).

(74) Mandataire : **FRANCE TELECOM**; R & D/PIV/Brevets, WINDAL-VERCASSON Gaëlle, 38-40 rue du Général Leclerc, F-92794 Issy Les Moulineaux Cedex 9 (FR).

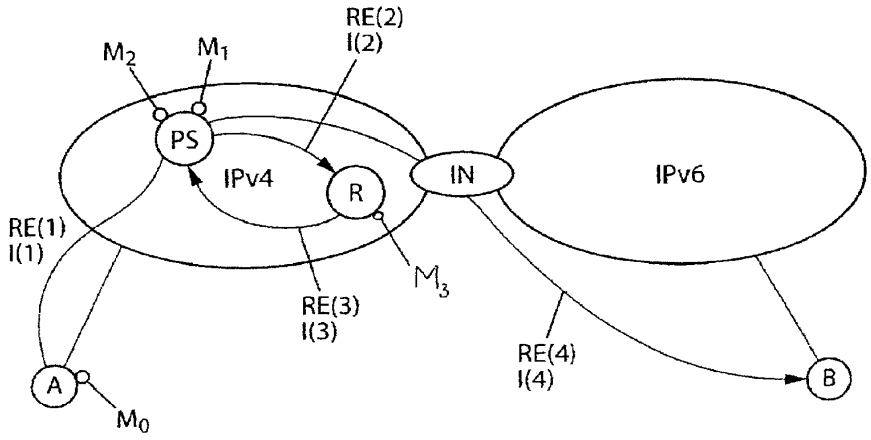
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR,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

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR CHARACTERISING HETEROGENEOUS COMMUNICATION NODES

(54) Titre : PROCEDE ET SYSTEME DE CARACTERISATION DE NOEUDS DE COMMUNICATION HETEROGENES



(57) Abstract: The invention relates to a method for the transmission of data between at least two heterogeneous nodes. Said method comprises at least one step for the insertion of an indicator representing at least one address allocated to a user agent (A) included in one of said nodes, into at least one message transmitted (RE(1), 1(1)) by said user agent (A) before the establishment of a communication session between the nodes. The invention enables the rapid identification of the risk of incompatibility between the types of two user agents (A, B) to be brought into communication with each other, with a view to remedying such an incompatibility if necessary. The invention can be applied to the intercommunication of user agents using type IPv4, IPv6 or dual stack (DS) in an IP network.

[Suite sur la page suivante]

WO 2007/099248 A2

ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, 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).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de transmission de données entre au moins deux nœuds hétérogènes. Le procédé selon l'invention inclut au moins une étape d'insertion, dans au moins un message transmis (RE(1), 1(1)) par un agent utilisateur (A) inclus dans l'un desdits nœuds avant établissement d'une session de communication entre lesdits nœuds, d'un indicateur de type représentatif de type d'au moins une adresse affectée à cet agent utilisateur (A). L'invention permet d'identifier rapidement des risques d'incompatibilité entre les types de deux agents utilisateurs (A, B) devant être mis en communication l'un avec l'autre, en vue de remédier le cas échéant à une telle incompatibilité. Application à l'intercommunication d'agents utilisateurs de type IPv4, IPv6 ou double pile (DS) en réseau IP.

CI

PROCÉDÉ ET SYSTÈME DE CARACTERISATION DE NŒUDS DE COMMUNICATION HÉTÉROGÈNES

L'invention se situe dans le domaine des télécommunications, et plus particulièrement dans celui de la téléphonie sur IP.

Des réseaux conformes à un protocole de communication dit IP (abréviation bien connue de l'homme du métier de l'expression anglaise "Internet Protocol") sont de plus en plus souvent utilisés en tant que supports universels d'une multitude de services et applications. Ce protocole IP a joué un rôle fédérateur auprès de multiples opérateurs qui ont choisi ce protocole pour mutualiser des offres de service jusqu'alors disparates.

IPv4 est une version du protocole de communication IP qui est utilisée depuis des années.

Pour satisfaire des contraintes imposées par de tels services de communication et plus particulièrement pour répondre aux besoins accrus en termes d'adresses, des opérateurs et des constructeurs d'équipements réseau se sont unis pour spécifier un protocole de communication de nouvelle génération, communément référencé IPv6, défini par des spécifications ainsi que des documents d'analyse qui sont à un stade de développement suffisamment avancé pour permettre à présent d'envisager un déploiement opérationnel dans les réseaux des opérateurs.

Néanmoins, l'introduction de cette nouvelle génération de protocole pose des problèmes significatifs liés à un besoin de garantir une interopérabilité et un interfonctionnement du protocole IPv6 et du protocole IPv4 qui est déjà déployé dans les réseaux IP. Dans l'état actuel de la technique des solutions à ces problèmes ont été identifiées, mais elles présentent pour désavantage de ne pas intervenir exclusivement à un niveau "service" (en particulier couche application) mais aussi à un niveau "transport" (couche IP). Dans la couche transport, des mécanismes ont été proposés, voire standardisés à l'IETF (abréviation bien connue de l'homme du métier de l'expression anglaise "Internet Engineering Task Force") tels

qu'une technique dite NAT-PT et diverses techniques connues sous le vocable anglais « tunneling » et consistant à encapsuler des données IPv6 dans des datagrammes IPv4 ou inversement.

En outre, des mises à jour et des adaptations d'architectures et de plateformes de services sont nécessaires pour permettre un interfonctionnement entre clients situés dans des environnements IP de nature différente (IPv4 ou IPv6), et ceci d'une manière aussi transparente que possible pour le client final.

Parmi d'autres activités multimédia, l'IETF a standardisé un protocole appelé SIP (abréviation bien connue de l'homme du métier de l'expression anglaise "Session Initiation Protocol") offrant pour principales fonctions l'initiation, la modification et la terminaison de sessions multimédia. Ce protocole SIP constitue un exemple intéressant d'application de la présente invention. Le protocole SIP s'appuie sur un protocole SDP (abréviation bien connue de l'homme du métier de l'expression anglaise "Service Description Protocol") pour produire une description de paramètres relatifs à la session concernée. Une fois une négociation réussie entre deux parties à un appel, ces dernières peuvent échanger des flux média grâce à une activation d'un protocole RTP (abréviation bien connue de l'homme du métier de l'expression anglaise "Real time Transport Protocol"). Des paramètres de sessions RTP sont pré-négociés *via* des messages de signalisation SIP, notamment dans la partie SDP. Ces paramètres sont principalement des adresses de terminaison et des numéros de port qui seront utilisés de part et d'autre d'une liaison de communication à établir.

Depuis qu'une première version du protocole SIP a été décrite dans un document référencé RFC 2543 (RFC signifiant "requête pour commentaires" ou "Request For Comment" en anglais), ce dernier est compatible avec le protocole IPv6. Une implémentation de ce protocole SIP décode en principe facilement des adresses conformes aux protocoles IPv4 et IPv6. Une telle adresse peut être introduite dans un champ spécifique tel un entête « CONTACT » ou dans des en-têtes de la partie SDP. Cependant, la présence de telles adresses peut empêcher l'établissement des appels

SIP dans le cas où les deux terminaux ne sont pas joignables dans un même environnement IP, à savoir si l'une dispose d'une adresse IPv4 et l'autre d'une adresse IPv6. Ainsi quand un agent utilisateur de type IPv4 A initie une session SIP vers un agent utilisateur de type IPv6 qui s'est enregistré auprès d'un serveur de localisation (noté R ci-après) IPv4, l'échange de messages SIP produit est décrit dans la figure 1a, où un premier agent utilisateur A désireux d'entrer en contact avec un deuxième agent utilisateur B envoie un message « INVITE » vers un serveur de proximité dit serveur proxy (noté PS ci-après) en utilisant une adresse IPv4 propre à ce dernier. Le serveur proxy PS est ici un serveur attaché à un environnement IPv4 exclusivement. Une fois le message reçu par le serveur proxy PS, ce dernier effectue une requête auprès d'un serveur de localisation encore appelé serveur d'enregistrement et récupère ainsi l'adresse du deuxième agent utilisateur B. Cette adresse étant par hypothèse une adresse IPv6, le serveur proxy PS ne connaît pas de route vers cette destination étant donné que ce serveur proxy PS est exclusivement de type IPv4. Un message d'erreur est alors envoyé vers l'agent utilisateur A concluant à une impossibilité d'établir une session SIP entre les premier et deuxième agents utilisateurs A et B. Ce message d'erreur est noté (2) 404 « No Route » sur la figure 1a.

Si l'on suppose maintenant que le serveur proxy PS peut néanmoins joindre l'adresse de localisation du premier agent utilisateur A ainsi que celle du deuxième agent utilisateur B, un autre échange de messages SIP est observé, quand le deuxième agent utilisateur B essaye d'appeler le premier agent utilisateur A, ainsi que représenté en figure 1b.

Dans ce cas de figure, le serveur proxy PS achemine un message « INVITE » reçu du deuxième agent utilisateur B vers l'adresse de localisation du premier agent utilisateur A. Ce message « INVITE » contient une offre SDP décrivant, outre des capacités offertes par le premier agent utilisateur B en termes de CODEC (pour "codeur/décodeur"), un numéro de port RTP et une adresse qu'utilisera le deuxième agent utilisateur B pour émettre/recevoir des flux RTP. Dans le cas de la figure 1b, cette adresse est de type IPv6. Ainsi, lorsque l'agent utilisateur A reçoit ce message

« INVITE », il ne peut que refuser l'ouverture de la session car cet agent utilisateur est un client IPv4. Au mieux pourra-t-il, selon les implémentations, renvoyer un message d'erreur indiquant qu'il ne supporte pas les connexions réseaux vers l'adresse IP de l'agent utilisateur B. Dans les deux exemples précédents, décrits en liaison avec les figures 1a et 1b, les sessions SIP ne peuvent ainsi pas être établies.

Une coexistence d'adresses IP de types différents pourra affecter d'autres appels que ceux ayant fait l'objet de la représentation graphique décrite ci-dessus. Ainsi, des appels destinés à des clients DS (abréviation bien connue de l'homme du métier de l'expression anglaise "Dual Stack"), peuvent aussi ne pas aboutir à des échanges de flux média, les agents utilisateurs de type DS étant en mesure de traiter les deux types d'adresse IPv4 et IPv6. Ceci est dû au fait que le protocole SIP de base ne permet de renseigner qu'une seule adresse IP pour l'émission ou la réception des flux média. Pour pallier ce problème, un document référencé RFC 4092 introduit une nouvelle sémantique consistant, entre autres, à définir un indicateur dénoté « sdp-anat ». Cette nouvelle sémantique permet à un agent utilisateur, d'annoncer et/ou de découvrir un ou plusieurs types d'adresse. Ainsi, des agents utilisateurs de type DS sont en mesure d'indiquer dans leur offre SDP leurs deux adresses IPv4 et IPv6. Grâce à cette technique, tous les appels de/vers un agent utilisateur de type DS vers/de des clients mono version (i.e. compatibles avec le protocole IPv4 seulement ou avec le protocole IPv6 seulement) peuvent donner lieu à des sessions SIP réussies.

Dans un cas où deux nœuds formant des extrémités d'une liaison de communication destinée à véhiculer un appel donné sont mono version, l'opérateur de service de téléphonie SIP concerné peut avoir recours à des applications ALG (abréviation bien connue de l'homme du métier de l'expression anglaise "Application Level Gateway"), pour modifier les offres SDP afin d'assurer une cohérence entre le type d'adresse supporté et celui contenu dans les messages SIP reçus. Pour ce faire les serveurs SIP utilisent des informations relatives à la couche transport, et non propres au protocole SIP, pour router les appels ou pour déterminer le recours à des

applications ALG pour altérer le contenu des offres SDP. Un tel comportement des serveurs SIP n'est pas décrit dans la norme.

D'une manière générale le problème lié aux interconnexions de deux agents utilisateurs hétérogènes (c'est-à-dire de types IP distincts) n'a pas été étudié en détail par la communauté des télécommunications. Excepté une proposition ANAT décrite par (RFC 4091, RFC 4092) qui résout une partie du problème, il n'existe en particulier pas de document de l'IETF décrivant le comportement des serveurs SIP pour acheminer des appels reliant deux agents utilisateurs appartenant à deux environnements IP différents.

En outre, les techniques existantes présentent les inconvénients suivants :

- le recours aux applications ALG et aux fonctions supplémentaires n'est pas documenté. Le serveur proxy PS ne dispose pas de moyens prévus par la RFC 3261 pour faciliter cette tâche ;
- le serveur proxy PS doit avoir recours à des informations de la couche réseau (encore appelée dans ce document couche transport) pour prendre des décisions concernant la couche service. Il est ainsi amené à prendre en compte d'autres considérations telles que l'adresse source des messages, l'adresse utilisée pour contacter le serveur proxy ou examiner la partie SDP. Ceci risque de nuire aux performances du proxy qui est a priori configuré pour ne traiter que les informations du niveau service ;
- l'utilisation des adresses n'est pas optimale : une méthode pour avoir des sessions réussies pourrait être de permettre aux deux agents utilisateurs participant à la communication de disposer de deux types d'adresses pour que la négociation SDP soit réussie dans tous les cas. Cette alternative poserait des problèmes d'optimisation d'utilisation de l'espace d'adresses à la disposition de l'opérateur (notamment en IPv4) ;
- la solution n'est pas générique: la philosophie de routage d'appel et d'intervention du serveur proxy PS dépend de la solution d'interconnexion déployée au niveau transport ;

- le serveur proxy PS ne dispose pas de moyens pour déterminer si un agent utilisateur est de type IPv4, IPv6 ou DS.

Les travaux menés par les inventeurs ont mené ceux-ci à conclure que, nonobstant un besoin qui ressort de l'étude qui précède, il n'existe dans l'état de la technique aucune disposition visant à permettre à un moyen de communication appartenant à un réseau de communication conforme à un protocole IP d'identifier de manière simple le type d'adresse associé à un agent utilisateur donné, une telle carence expliquant pourquoi la plupart des techniques de gestion de communications entre nœuds hétérogènes actuellement à l'étude sont insuffisantes et ne répondent pas aux besoins de service consistant à permettre des communications hétérogènes.

La présente invention offre une solution qui ne présente pas ces inconvénients en proposant un procédé de transmission qui permet une identification aisée du type d'adresse supporté par un agent utilisateur donné.

En effet, un procédé de transmission de données entre au moins deux nœuds hétérogènes conforme à l'invention est caractérisé en ce qu'il inclut au moins une étape d'insertion, dans au moins un message transmis par un agent utilisateur inclus dans l'un desdits nœuds avant établissement d'une session de communication entre lesdits nœuds, d'un indicateur de type représentatif du type d'au moins une adresse associée à cet agent utilisateur.

L'invention permet d'identifier rapidement des risques d'incompatibilité entre les types de deux agents utilisateurs devant être mis en communication l'un avec l'autre, en vue de remédier le cas échéant à une telle incompatibilité.

L'invention permettra ainsi en particulier à un serveur proxy tel celui évoqué plus haut d'identifier rapidement les types de deux agents utilisateurs devant être mis en communication l'un avec l'autre, ce qui permettra audit serveur d'identifier et de mettre en œuvre le cas échéant des ressources nécessaires à un établissement effectif d'une session de

communication entre ces agents, qu'ils soient ou non de même type.

Par type d'un agent utilisateur, on entend ici une ou des versions de protocole IP (par exemple IPv4, IPv6) que cet agent utilisateur est à même de mettre en œuvre par l'intermédiaire de la ou des interfaces réseaux dont dispose le nœud SIP qui l'abrite. Deux nœuds A et B sont dits hétérogènes si le type de l'agent utilisateur abrité par le nœud A est différent du type de l'agent utilisateur abrité par le nœud B.

Ainsi, un protocole conforme à l'invention pourra en outre inclure une étape de classification de l'agent utilisateur émetteur d'un indicateur de type selon l'une des trois catégories de type de protocole IP, IPv4 pur, IPv6 pur ou double pile.

Selon un mode de mise en œuvre particulier de l'invention, l'étape d'insertion est exécutée à l'initiative dudit agent utilisateur.

Ceci permet à l'agent utilisateur de restreindre les communications qu'il reçoit ou émet au type d'interface réseau et de protocole IP correspondant.

L'indicateur de type pourra être avantageusement matérialisé par une valeur numérique codée représentative soit d'un protocole IPv4, soit d'un protocole IPv6, soit encore des deux protocoles IPv4 et IPv6, désigné double pile.

Une telle valeur numérique pourra être très aisément encodée sur un très faible nombre de bits, de sorte que la mise en œuvre de l'invention n'occasionnera pas d'augmentation significative de volume des messages échangés au titre d'une communication.

Selon une première variante avantageuse de l'invention, un procédé tel que décrit plus haut inclura en outre une étape de mémorisation dudit indicateur de type en référence avec un identifiant de l'agent utilisateur associé.

Une telle étape de mémorisation permettra, entre autres, de créer et de tenir à jour au sein d'une base de données une table de référence permettant d'identifier aisément et directement un type d'adresse IP associé à chaque agent utilisateur dont l'indicateur de type aura été enregistré. Cette

base de données pourra être alimentée spontanément par chaque agent utilisateur lors d'une initialisation de connexion de celui-ci ou par des mises à jour régulières, et gérée par un serveur de localisation, auprès duquel les agents utilisateurs s'enregistrent à l'initialisation d'une session de communication ou à l'expiration du délai d'enregistrement.

Selon une deuxième variante avantageuse de l'invention, qui pourra être mise en œuvre alternativement ou cumulativement avec la première variante, un procédé tel que décrit plus haut pourra en outre inclure une étape de transformation d'au moins une adresse incluse dans un message d'invitation à entrer en communication avec un agent utilisateur, ladite étape de transformation étant destinée à être exécutée en cas d'incompatibilité entre un indicateur de type associé à un agent utilisateur ayant émis ledit message d'invitation, d'une part, et un indicateur de type associé à un agent utilisateur destinataire dudit message d'invitation, d'autre part.

Selon cette variante de l'invention, une simple comparaison entre des indicateurs de type associés aux agents utilisateurs appelant et appelé permettra de remédier, avant même toute tentative de connexion entre appelant et appelé, à toute éventuelle incompatibilité entre ceux-ci.

A titre d'exemple, l'invention sera avantageusement mise en œuvre dans une application de téléphonie sur IP désignée couramment par VoIP (abréviation bien connue de l'homme du métier de l'expression anglaise "Voice over IP"), ou généralement groupée sous le thème des services conversationnels.

L'invention s'inscrira alors dans la problématique générale des services de signalisation basés sur le protocole SIP défini par la RFC 3162 et déployés à la fois pour des clients IPv4 et des clients IPv6. Ces services peuvent être des services de voix, de vidéo, de présence, etc.

Ainsi qu'exposé plus haut, l'invention propose un mécanisme simple pour faciliter l'établissement de sessions SIP entre deux clients hétérogènes, un attaché à un domaine IPv4 et l'autre à un domaine IPv6.

Grâce à la mise en œuvre de l'invention, un serveur proxy SIP est

en mesure, d'une part, de router les appels SIP, et, d'autre part, d'intervenir pour altérer ou faire altérer le contenu des offres SDP défini par la RFC 2327 véhiculées dans les messages SIP, afin de permettre l'établissement de sessions entre des nœuds hétérogènes. Au contraire, en l'absence de mise en œuvre de la présente invention, le serveur proxy SIP doit avoir accès à des informations autres que celles de la couche application, en particulier à celles relatives à la couche réseau, pour orienter son choix de routage d'appel et optimiser le recours aux applications ALG, lesquelles se chargent de modifier les messages SIP pour aboutir à des sessions SIP réussies. Sans cette intervention du serveur SIP et de/des applications ALG, certaines sessions SIP ne peuvent pas avoir lieu, faute d'utilisation de piles protocolaires homogènes.

La mise en œuvre de l'invention autorise un interfonctionnement de nœuds SIP hétérogènes et permet de simplifier et ainsi de faciliter le routage des appels dans des systèmes de télécommunication mettant en œuvre le protocole SIP.

En particulier, l'invention permet d'optimiser l'usage d'adresses IP et de ne pas faire reposer le traitement des messages SIP par un serveur proxy SIP sur des informations de la couche transport, pour décider des traitements requis par ces messages SIP reçus par ce serveur.

Selon un mode de réalisation spécifique à l'exemple d'application évoqué ici, l'indicateur de type pourra être inséré dans un champ « CONTACT » inclus dans des messages de requête SIP.

L'introduction de l'indicateur de type dans le message de requête permet d'informer le serveur de localisation et le serveur proxy de la nature des adresses IP supportées par les interfaces réseau disponibles sur un agent utilisateur. En outre, le serveur proxy peut alors traiter un message de requête à partir de cet indicateur de type, pour acheminement vers son destinataire, sans avoir à accéder aux informations contenues dans la couche réseau.

Une transposition au présent exemple d'application de la première variante de l'invention décrite plus haut pourra prévoir de faire

insérer par l'agent utilisateur son indicateur de type dans au moins un message « REGISTER ».

Ainsi, sur réception d'un message « REGISTER », le serveur de localisation procède à la mémorisation au moins de l'adresse d'enregistrement, du délai d'expiration de l'enregistrement et de l'indicateur de type. Le serveur de localisation peut mémoriser également d'autres données.

Une transposition au présent exemple d'application de la deuxième variante de l'invention décrite plus haut pourra prévoir de faire transformer par le serveur proxy au moins une adresse incluse dans un message « INVITE » en cas d'incompatibilité entre un indicateur de type associé à l'agent utilisateur ayant émis ledit message « INVITE », d'une part, et un indicateur de type associé à l'agent utilisateur destinataire dudit message « INVITE », d'autre part.

Une telle incompatibilité survient notamment lorsque les agents utilisateurs émetteur et destinataire du message "INVITE" sont de types différents.

Dans une telle application de l'invention, un serveur proxy qui devra effectuer un traitement de routage d'appel en recourant à une passerelle au niveau application permettant de modifier des messages d'appel entre deux agents utilisateurs, de types distincts, exécutera ce traitement:

- soit à partir d'une classification stockée dans une base d'enregistrement actualisée par le serveur de localisation et contenant la nature du type de l'agent utilisateur appelant et appelé;

- soit à partir d'une classification stockée dans la base d'enregistrement contenant la nature du type de l'agent utilisateur appelé et de l'indicateur de type contenu dans le message « INVITE » transmis par l'agent utilisateur appelant.

Ainsi qu'il ressort de la description qui précède, l'invention concerne également, en tant que produit obtenu directement par sa mise en œuvre dans l'application décrite ci-dessus, tout signal porteur d'un message

de requête comportant un indicateur de type, représentatif de la nature d'au moins une adresse IP associée à un agent utilisateur émetteur de ce message, un tel message pouvant par exemple être matérialisé par un message « REGISTER », « INVITE », ou encore « 200 OK ». L'indicateur de type peut notamment être inséré dans un champ "CONTACT".

L'invention concerne également, selon un aspect matériel, un système de transmission de données entre au moins deux nœuds hétérogènes, caractérisé en ce qu'il inclut des moyens d'insertion, dans au moins un message transmis par un agent utilisateur inclus dans l'un desdits nœuds avant établissement d'une session de communication entre lesdits nœuds, d'un indicateur de type représentatif du type d'au moins une adresse associée à cet agent utilisateur.

L'invention concerne également, selon une variante de cet aspect matériel, un système de transmission tel que décrit ci-dessus incluant en outre des moyens de tri et de classification d'agents utilisateurs émetteurs de messages de requête à partir des indicateurs de type desdits agents, et une base de données destinée à mémoriser ladite classification.

L'invention concerne aussi, selon une autre variante de cet aspect matériel, un système de transmission tel que décrit ci-dessus incluant en outre des moyens de comparaison d'indicateurs de types propres à au moins un agent utilisateur appelant et à au moins un agent utilisateur appelé.

Selon un autre de ses aspect matériels, l'invention concerne en outre, en tant que moyens utiles à sa mise en œuvre, plusieurs programmes d'ordinateur incluant au moins une série d'instructions de code de programme pour l'exécution de certaines des étapes d'un procédé conforme à la description qui précède lorsque ledit programme est exécuté sur un ordinateur.

L'invention sera mieux comprise à l'aide de la description suivante, faite à titre d'exemple non-limitatif et en regard des dessins annexés, dans lesquels, outre les figures 1a et 1b relatives à l'art antérieur,

- la figure 2 représente, à titre illustratif, un organigramme des étapes essentielles de mise en œuvre du procédé objet de l'invention ;

Juniper Exhibit 1002, page 300

- la figure 3 représente, à titre illustratif, un premier exemple d'enregistrement pour des agents utilisateurs de type IPv4 et IPv6 ;
- la figure 4 représente, à titre illustratif, un deuxième exemple d'enregistrement pour un agent utilisateur de type double pile ;
- la figure 5 représente un système d'interfonctionnement de nœuds SIP hétérogènes conforme à l'objet de l'invention, opérant dans le cas de la transmission, par un agent utilisateur, d'un message « REGISTER » destiné à un serveur de localisation et d'un message « INVITE » transitant par un serveur proxy.

Une description plus détaillée du procédé conforme à l'objet de la présente invention sera maintenant donnée en liaison avec la figure 2 et les figures suivantes.

D'une manière générale, on indique que chaque nœud hétérogène formé par exemple par un terminal IP dans la version IPv4, IPv6 ou dans la version hybride désignée double pile DS, comporte un agent utilisateur UA de type déterminé, le type de cet agent utilisateur correspondant à la version du protocole IP que cet agent utilisateur est à même de mettre en œuvre par l'intermédiaire de la ou des interfaces réseaux dont dispose le terminal considéré.

Ainsi que représenté en figure 2, le procédé objet de l'invention consiste au moins, en une étape 10, à insérer dans un message de requête M transmis par l'agent utilisateur UA un indicateur de type, cet indicateur de type étant noté « atypes ». Après insertion, le message de requête transmis est noté M(« atypes »). Un tel message de requête peut être par exemple un message d'enregistrement destiné à un serveur de localisation R. Il peut s'agir également d'un message destiné à un serveur proxy PS, par exemple un message d'invitation à entrer en communication avec un autre agent utilisateur.

Après la transmission 13 du message, dans lequel l'indicateur de type a été inséré, le procédé objet de l'invention consiste en une étape 11 à traiter le message de requête M(« atypes ») à partir de l'indicateur de type « atypes » qu'il contient. Ce traitement est effectué dans un équipement

référencé 12, qui peut être le serveur de localisation dans le cas d'un message d'enregistrement, ou le serveur proxy dans le cas d'un message d'invitation à entrer en communication avec un autre agent.

Dans ce dernier cas, le traitement 11 effectué au niveau du serveur proxy 12 consiste en un acheminement du message, sans qu'il soit nécessaire pour le serveur proxy 12 d'accéder à des informations contenues dans la couche transport.

On comprend en particulier que l'indicateur de type « atypes » contient au moins une donnée numérique codée représentative de la nature des interfaces réseau et du protocole IP disponibles sur l'agent utilisateur émetteur du message dans le but de renseigner le serveur de localisation et le serveur proxy 12 et de leur permettre:

- pour le serveur de localisation 12, de procéder à l'enregistrement 11 de l'indicateur de type, associé à un identifiant de l'agent utilisateur, de façon à maintenir une base de données renseignant sur les types des différents agents utilisateurs susceptibles de vouloir communiquer;

- pour le serveur proxy 12, d'effectuer l'acheminement 11 en l'absence d'accès à toute information contenue dans la couche transport ayant servi à la transmission du message M(« atypes »).

Un exemple de mise en œuvre de l'étape 10 du procédé objet de l'invention représentée en figure 2 sera maintenant décrit en liaison avec les figures 3 et 4.

Dans un mode de mise en œuvre particulier, on insère l'indicateur de type « atypes » dans le champ « CONTACT » des requêtes SIP, en particulier des requêtes « REGISTER » et « INVITE ». Pour illustrer la définition de cet indicateur, la description ABNF du champ « CONTACT », telle que décrite par la RFC 3162, est indiquée ci-après.

Dans la description ABNF ci-après, les éléments connus et décrits par la RFC 3162 sont en écriture droite et les éléments descriptifs supplémentaires sont en écriture droite en caractères gras.

L'ensemble de la nouvelle description ABNF est donné au tableau T1 ci-après :

Tableau T1

Contact	=	(« Contact » / « m ») HCOLON (STAR / (contact-param *(COMMA contact-param))) *COMMA atypes*
contact-param	=	(name-addr / addr-spec) *(SEMI contact-params)
name-addr	=	[display-name] LAQUOT addr-spec RAQUOT
addr-spec	=	SIP-URI / SIPS-URI / absoluteURI
display-name	=	*(token LWS)/ quoted-string
contact-params	=	c-p-q / c-p-expires / contact-extension
c-p-q	=	« q » EQUAL qvalue
c-p-expires	=	« expires » EQUAL delta-seconds
contact-extension	=	generic-param
delta-seconds	=	1*DIGIT
atypes	=	*« atypes » EQUAL 4/6/0*

Un agent utilisateur peut souhaiter restreindre les communications qu'il reçoit ou émet :

- à son interface IPv4,
- à son interface IPv6,
- ou utiliser les deux types d'interface, lorsqu'il est équipé d'une interface double pile DS (i.e. compatible avec les deux versions de protocole IPv4 et IPv6).

Cette opération est notifiée à l'aide de l'indicateur de type « atypes ».

Un agent utilisateur peut choisir par configuration de ne pas annoncer une disponibilité effective en positionnant l'indicateur de type « atypes » à la bonne valeur. A noter que pour l'interface IPv6, l'interface est jugée disponible IPv6 seulement si l'une des adresses configurées est de portée globale (En effet, le protocole IPv6 distingue les adresses de type "Link local" et "global". Les adresses de portée locale ne sont pas routables au delà du réseau local contrairement aux adresses de portée globale qui sont des adresses routables i.e. joignables au-delà du réseau local). Lors de la procédure d'enregistrement, l'agent utilisateur SIP envoie un message « REGISTER » avec un champ «CONTACT» étendu tel que décrit au tableau T1 contenant la rubrique supplémentaire « atypes ». Cette rubrique peut prendre les valeurs suivantes :

- 4 : si l' agent utilisateur supporte IPv4 uniquement,

- 6 : si l' agent utilisateur supporte IPv6 uniquement,
- 0 : si l' agent utilisateur est double pile.

Un agent utilisateur peut indiquer au serveur proxy PS qu'il supporte seulement le protocole IPv4 en positionnant l'indicateur de type « atypes » à 4 (bien que l'agent utilisateur soit de type double pile DS par exemple), ou le protocole IPv6 en positionnant l'indicateur de type « atypes » à 6 ou un protocole double pile DS en positionnant l'indicateur de type « atypes » à 0 dans le message « REGISTER » qu'il envoie au serveur d'enregistrement R.

R et R6 indiquent des serveurs de localisation sur la figure 3, respectivement associés aux agents utilisateurs A et B.

Exemple d'agent utilisateur de type IPv4 :

On suppose que A est un agent utilisateur de type IPv4 dont l'adresse est 192.165.25.2. Ainsi que représenté sur la figure 3, l'agent utilisateur A envoie au serveur de localisation R le message « REGISTER » (1) suivant donné au tableau T2 :

Tableau T2

REGISTER	sip :r.test.evi SIP/2.0
Via :	SIP/2.0/UDP 192.165.25.2:5062;branch=z9hG4bK00e31d6ed
Max-Forwards :	70
Content-Length :	0
To :	A <sip:A@test.evi>
From :	A <sip: A@test.evi >;tag=ed3833bd7363e68
Call-ID :	a8a83b610ae5d242289dfc1c78b7f1d8@test.evi
CSeq :	1830746364 REGISTER
Contact :	A <sip:A@192.165.25.2:5062>;expires=900, atypes=4

Le serveur d'enregistrement R répond à l'agent utilisateur A avec le message "200 OK" (2) donné au tableau T3 :

Tableau T3

	SIP/2.0 200 OK
Call-ID :	a8a83b610ae5d242289dfc1c78b7f1d8@evi.biz
CSeq :	1830746365 REGISTER
From :	A <sip:A@test.evi>;tag=ed3833bd7363e68
To :	A <sip:A@test.evi>;tag=3ab7fe89d998709
Via :	SIP/2.0/UDP 192.165.25.2:5062;branch=z9hG4bK00e31d6ed
Content-Length :	0
Contact :	A <sip:A@192.165.25.2:5062>;expires=900, atypes=4

Exemple d'agent utilisateur IPv6 :

On suppose que B est un agent utilisateur de type IPv6 dont l'adresse est 2001:688:1ffb:ff80::2. Comme représenté sur la figure 3, l'agent utilisateur B envoie au serveur de localisation R6 le message REGISTER (1) donné au tableau T4 :

Tableau T4

REGISTER	sip:r6.test.evi SIP/2.0
Via :	SIP/2.0/UDP [2001:688:1ffb:ff80::2]:5062;branch=z9hG4bK00e31d6ed
Max-Forwards :	70
Content-Length :	0
To :	B <sip:B@test.evi>
From :	B <sip:B@test.evi >;tag=ed3833bd7363e68
Call-ID :	a8a83b610ae5d242289dfc1c78b7f1d8@test.evi
CSeq :	1830746364 REGISTER
Contact :	B <sip:B@[2001:688:1ffb:ff80::2]:5062>;expires=900, atypes=6

Le serveur d'enregistrement R6 répond pour confirmer l'enregistrement avec un message « 200 OK » (2) donné au tableau T5 :

Tableau T5

	SIP/2.0 200 OK
Call-ID :	a8a83b610ae5d242289dfc1c78b7f1d8@evi.biz
CSeq :	1830746365 REGISTER
From :	B <sip:B@test.evi >;tag=ed3833bd7363e68
To :	B <sip:B@test.evi >;tag=3ab7fe89d998709
Via :	SIP/2.0/UDP[2001:688:1ffb:ff80::2]:5062;branch=z9hG4bK00e31d6ed
Content-Length:	0
Contact :	B <sip:B@[2001:688:1ffb:ff80::2]:5062>;expires=900, atypes=6

L'adresse IP contenue dans le champ « CONTACT » peut être unique et de type différent de celui indiqué dans le champ d'indicateur de type « atypes ». En effet, un agent utilisateur instanciant l'indicateur de type « atypes » à 6 peut utiliser une adresse IPv4 dans le champ « CONTACT », ou, un agent utilisateur ayant instancié l'indicateur de type « atypes » à 0 peut ne déclarer qu'une seule adresse et non pas deux, ainsi qu'il sera décrit ci-après. L'adresse contenue dans le champ « CONTACT » est exploitée par le serveur proxy SIP pour acheminer les messages de signalisation. Les messages média seront transmis à l'agent utilisateur par son interface IPv6, car cet agent utilisateur s'est déclaré auprès de son serveur proxy PS comme un agent utilisateur IPv6 (sur la base de l'indicateur de type inséré dans les messages qu'il émet à destination du serveur proxy, ou sur la base

de l'indicateur de type enregistré pour cet agent utilisateur par le serveur de localisation).

Exemple d'agent utilisateur DS avec une seule adresse dans le champ « CONTACT » :

On suppose en liaison avec la figure 4 que l'agent utilisateur DS est un agent utilisateur de type double pile 2001:688:1ffb:ff80::2/192.168.25.5. Comme représenté sur la figure 4 précitée :

L'agent utilisateur DS envoie, lors d'une phase d'enregistrement, à son serveur de localisation R le message « REGISTER » (1) donné au tableau T6 :

Tableau T6

REGISTER	sip :r.test.evi SIP/2.0
Via :	SIP/2.0/UDP 192.168.25.5:5062;branch=z9hG4bK00e31d6ed
Max-Forwards :	70
Content-Length:	0
To :	DS <sip:DS@test.evi>
From :	DS <sip:DS@test.evi >;tag=ed3833bd7363e68
Call-ID :	a8a83b610ae5d242289dfc1c78b7f1d8@test.evi
CSeq :	1830746364 REGISTER
Contact :	DS <sip:DS@192.168.25.5:5062>;expires=900, atypes=0

Le serveur de localisation R6 répond pour confirmer l'enregistrement avec un message « 200 OK » (2) donné au tableau T7 :

Tableau T7

	SIP/2.0 200 OK
Call-ID :	a8a83b610ae5d242289dfc1c78b7f1d8@evi.biz
CSeq :	1830746365 REGISTER
From :	DS <sip:DS@test.evi >;tag=ed3833bd7363e68
To :	DS <sip:DS@test.evi >;tag=3ab7fe89d998709
Via :	SIP/2.0/UDP 192.168.25.5:5062;branch=z9hG4bK00e31d6ed
Content-Length:	0
Contact :	DS <sip:DS@192.168.25.5:5062>;expires=900, atypes=0

Traitement de l'indicateur "atypes"

A la réception du message « REGISTER », le serveur de localisation R stocke en plus de l'adresse d'enregistrement AOR (abréviation anglaise de l'expression "Address Of Record"), et du délai d'expiration de l'enregistrement, la valeur de l'indicateur de type « atypes ». Ces données (ainsi que d'autres éventuellement) sont stockées dans une base

d'enregistrement gérée par le serveur de localisation. Elles peuvent être mises à jour par d'autres messages REGISTER issus du même agent utilisateur. Ce traitement remplace le traitement prévu initialement dans la RFC 3261.

A l'aide de l'information de l'indicateur de type « atypes », le serveur de localisation classifie ses agents utilisateurs en trois catégories:

- "Pure IPv4" en anglais, pour IPv4 pur ;
- "Pure IPv6" en anglais, pour IPv6 pur ;
- DS, double pile.

Cette classification est accessible au serveur proxy par simple consultation de la base d'enregistrement gérée par le serveur de localisation. Cette classification peut également être effectuée directement par le serveur proxy par simple lecture de l'indicateur de type inséré par un agent utilisateur dans un message destiné au proxy, comme détaillé ci-après.

En effet, les agents utilisateurs peuvent aussi positionner l'indicateur de type « atypes » quand ils émettent un message « INVITE ».

Le serveur proxy PS doit se contenter de transmettre les messages SIP sans modifier leur contenu dans les cas suivants, référencés CAS-1 :

- IPv4 vers IPv4,
- IPv6 vers IPv6,
- IPv4 vers DS et DS vers IPv4,
- IPv6 vers DS et DS vers IPv6,
- DS vers DS.

Dans le cas CAS-1 précité, les agents utilisateurs sont dits compatibles, car ils sont de même type (ou, plus généralement dans le cas des agents utilisateurs DS, ont au moins un type commun) et peuvent donc dialoguer en utilisant la même version de protocole IP.

La modification des messages SIP conduisant à disposer des adresses IP de l'agent utilisateur appelé et appelant de même type après modification intervient seulement dans les cas suivants référencés CAS-2 :

- IPv6 vers IPv4,

- IPv4 vers IPv6.

Dans le cas CAS-2 précité, les agents utilisateurs sont dits incompatibles, car ils ne sont pas de même type, et ne peuvent donc pas communiquer.

Pour le routage d'appel et la décision de recourir à une application ALG ou pour modifier les messages SIP pour obtenir des sessions réussies entre deux agents utilisateurs de types distincts, le serveur proxy PS peut agir soit:

- *en examinant la base d'enregistrement maintenue par le serveur de localisation* :

Dans ce cas, le serveur proxy PS interroge le serveur de localisation R sur le type des agents utilisateurs appelant et appelé. Le serveur proxy PS peut alors décider de modifier le contenu SDP du message SIP pour harmoniser ce dernier avec le type d'adresse supporté par l'appelé, s'il s'agit d'un scénario faisant partie du CAS-2. L'exemple représenté en figure 5 illustre ce mode opératoire au travers d'une communication entre un agent utilisateur A de type IPv4 et un agent utilisateur B de type IPv6. Les fonctions d'interconnexion des réseaux IPv4 et IPv6 sont représentées par le nœud IN qui sert de relais et exécute en particulier la translation protocolaire des datagrammes IPv4 en des datagrammes IPv6 et vice versa.

On suppose que l'agent utilisateur B est un agent utilisateur de type IPv6. A l'initialisation du service, l'agent utilisateur B s'est enregistré auprès du serveur de localisation R en positionnant l'indicateur de type « atypes » à 6 et l'agent utilisateur A s'est enregistré auprès du serveur de localisation R en positionnant l'indicateur de type « atypes » à 4. Par souci de simplification, cette phase préalable d'enregistrement n'est pas représentée sur la figure 5.

L'agent utilisateur B est connu dans l'environnement IPv6 par une adresse IPv6 qui est traduite en une adresse IPv4 par les mécanismes d'interconnexion IPv6-IPv4 tels que le NAT-PT. Dans ce cas, l'agent utilisateur B est identifié comme étant un agent utilisateur de type IPv6 et

l'agent utilisateur A comme un agent utilisateur de type IPv4. Lorsque l'agent utilisateur A veut établir une session avec l'agent utilisateur B, les messages SIP échangés sont les suivants:

- RE (1) l'agent utilisateur A envoie un message « INVITE » vers le serveur proxy PS ;
- RE (2) le serveur proxy PS interroge le serveur de localisation R sur l'adresse de localisation de l'agent utilisateur B, et sur les indicateurs de type « atypes » des agents utilisateurs A et B tels qu'indiqués lors de la phase d'enregistrement ;
- RE (3) le serveur de localisation R retourne l'adresse de l'agent utilisateur B, l'indicateur de type « atypes » de l'agent utilisateur B, et celui de l'agent utilisateur A ;
- RE (4) le serveur proxy PS compare les deux indicateurs de type « atypes », des agents utilisateurs A et B. Le serveur proxy PS vérifie, à partir de la classification des types disponible auprès du serveur de localisation R, que A est un agent utilisateur de type IPv4 et B un agent utilisateur de type IPv6. Le serveur proxy PS invoque alors les mécanismes d'adaptation pour modifier l'offre SDP initiale de l'agent utilisateur A pour qu'elle contienne une adresse IPv6. Le serveur proxy PS renvoie alors le message « INVITE » modifié vers l'adresse de l'agent utilisateur B comme indiquée par le serveur de localisation R.

Sans cette procédure, le serveur proxy PS ne disposerait pas de moyens pour router l'appel vers l'agent utilisateur B et pour invoquer les fonctions d'adaptation nécessaires à un acheminement correct du message jusqu'à B. En effet, le serveur proxy PS renverrait la requête vers l'agent utilisateur B sans modifier celle-ci, et, dans ce cas, la session SIP entre les agents utilisateurs A et B ne pourrait pas avoir lieu (confer Figure 1b).

- *En examinant la base d'enregistrement, et l'indicateur de type « atypes » véhiculé dans le message « INVITE » :*

Dans ce cas, le serveur proxy PS questionne le serveur de localisation R sur le type de l'agent utilisateur appelé B. Le type de l'agent utilisateur

appelant A est déduit du message « INVITE » émis par ce dernier. Le serveur proxy PS peut alors décider de modifier le contenu du message SIP pour harmoniser ce dernier avec le type d'adresse supporté par l'agent utilisateur appelé B; il s'agit d'un scénario faisant partie du CAS-2. Pour cette option, un agent utilisateur peut restreindre le type d'adresse à utiliser par session. L'exemple décrit en liaison avec la figure 5 illustre cet autre mode opératoire au travers d'une communication entre un agent utilisateur de type IPv4 et un agent utilisateur de type IPv6.

On suppose que B est un agent utilisateur de type IPv6. Au démarrage du service, l'agent utilisateur B s'est enregistré auprès du serveur de localisation R en positionnant l'indicateur de type « atypes » à 6 et l'agent utilisateur A en positionnant l'indicateur de type « atypes » à 4. Dans ce cas, l'agent utilisateur B est identifié comme étant un agent utilisateur de type IPv6 et l'agent utilisateur A comme un agent utilisateur de type IPv4. Lorsque l'agent utilisateur A veut établir une session avec l'agent utilisateur B, les messages SIP échangés sont les suivants:

- I (1) l'agent utilisateur A envoie un message « INVITE » vers le serveur proxy PS ;
- I (2) le serveur proxy PS interroge le serveur de localisation R sur l'adresse de localisation de l'agent utilisateur B, et sur l'indicateur de type « atypes » de B comme indiqué lors de la phase d'enregistrement ;
- I (3) le serveur de localisation R retourne l'adresse et l'indicateur de type « atypes » de l'agent utilisateur B ;
- I (4) le serveur proxy PS extrait l'indicateur de type « atypes » de l'agent utilisateur A de la requête « INVITE » I (1) et le compare à celui de l'agent utilisateur B. Le serveur proxy PS vérifie, à partir de la classification des types disponible auprès du serveur de localisation R, que A est un agent utilisateur de type IPv4 et B un agent utilisateur de type IPv6. Le serveur proxy PS invoque alors les mécanismes d'adaptation pour modifier l'offre SDP initiale de l'agent utilisateur A pour qu'elle contienne une adresse IPv6. Le serveur proxy PS renvoie

alors le message « INVITE » modifié vers l'adresse de l'agent utilisateur B comme indiquée par le serveur de localisation R.

Pour la mise en œuvre du protocole illustré en figure 5, on indique que le serveur proxy PS comporte avantageusement un module M1 de comparaison d'indicateurs de type associés à un agent utilisateur appelant et à un agent utilisateur appelé. Lorsque le module M1 détermine que les agents utilisateurs appelant et appelé sont de types différents, le serveur proxy active un module M2 d'appel à une ressource de modification de l'adresse IP de l'agent utilisateur appelant. La ressource de modification, externe au serveur proxy PS n'est pas représentée sur la figure 5. Les modules M_1 et M_2 peuvent être implémentés sous forme de programmes d'ordinateur, désignés par souci de simplification par la même référence alphanumérique sur la figure 5.

L'invention couvre en outre un programme d'ordinateur M_0 pour exécution par un ordinateur ou un dispositif dédié tel qu'un agent utilisateur de type IPv4, IPv6 ou double pile d'un terminal IP. Lors de l'exécution du programme d'ordinateur M_0, ses instructions de code permettent l'insertion dans un message de requête transmis par cet agent utilisateur UA, d'un indicateur de type « atypes » représentatif du type d'une ou plusieurs adresses IP supportée(s) par les interfaces réseau disponibles sur cet agent utilisateur UA, ainsi que décrit et représenté en figures 2, 3 et 4 précédemment dans la description.

Comme indiqué ci-dessus, l'invention couvre encore un programme d'ordinateur M_1, M_2 comportant une suite d'instructions pour exécution par un ordinateur ou un dispositif dédié tel qu'un serveur proxy PS. Lors de l'exécution du programme M_1, M_2, ces instructions permettent d'effectuer le traitement d'un message de requête transmis par un agent utilisateur au serveur proxy et contenant un indicateur de type « atypes » représentatif du type d'une ou plusieurs adresses IP supportée(s) par les interfaces réseau disponibles sur cet agent utilisateur, Un tel traitement consiste en l'acheminement de ce message de requête vers son destinataire, en l'absence d'accès à toute information contenue dans la couche de

transport, ainsi que décrit et représenté en figures 2 à 5 précédemment dans la description.

L'invention couvre aussi un programme d'ordinateur M_3, comprenant des instructions de code pour exécution par un ordinateur ou un dispositif dédié tel qu'un serveur de localisation R. Lors de l'exécution du programme M3, ces instructions permettent d'extraire un indicateur de type d'un message d'enregistrement transmis par un agent utilisateur, et de mémoriser cet indicateur de type, en relation avec un identifiant de l'agent utilisateur concerné, dans une base d'enregistrement. Elles permettent également de réaliser une classification de l'agent utilisateur concerné selon l'une des trois catégories de type de protocole IP, à savoir IPv4, IPv6 ou double pile, ainsi que décrit et représenté en figures 2 à 5 précédemment dans la description.

REVENDICATIONS

1. Procédé de transmission de données entre au moins deux nœuds hétérogènes, caractérisé en ce qu'il inclut au moins une étape d'insertion, dans au moins un message transmis par un agent utilisateur inclus dans l'un desdits nœuds avant établissement d'une session de communication entre lesdits nœuds, d'un indicateur de type représentatif du type d'au moins une adresse associée à cet agent utilisateur.

2. Procédé selon la revendication 1, caractérisé en ce que ledit indicateur de type est inséré dans un champ appelé « CONTACT » inclus dans un message de requête SIP.

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que l'étape d'insertion est exécutée à l'initiative dudit agent utilisateur.

4. Procédé selon l'une des revendications 1 à 3, caractérisé en ce que ledit indicateur de type est une valeur numérique codée représentative soit d'un protocole IPv4, soit d'un protocole IPv6, soit encore des deux protocoles IPv4 et IPv6, désigné double pile.

5. Procédé selon l'une des revendications 1 à 4, caractérisé en ce qu'il inclut en outre une étape de mémorisation dudit indicateur de type en référence avec un identifiant de l'agent utilisateur associé.

6. Procédé selon l'une des revendications 4 à 5, caractérisé en ce qu'il inclut en outre une étape de classification de l'agent utilisateur émetteur d'un indicateur de type selon l'une des trois catégories de type de protocole IP, IPv4 pur, IPv6 pur ou double pile.

7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce qu'il inclut en outre une étape de transformation d'au moins une adresse incluse dans un message d'invitation à entrer en communication avec un agent utilisateur, ladite étape de transformation étant destinée à être exécutée en cas d'incompatibilité entre un indicateur de type associé à un agent utilisateur ayant émis ledit message d'invitation, d'une part, et un

indicateur de type associé à un agent utilisateur destinataire dudit message d'invitation, d'autre part.

8. Signal porteur d'un message de requête incluant un indicateur de type représentatif d'un type d'au moins une adresse IP affectée à un agent utilisateur émetteur de ce message.

9. Système de transmission de données entre au moins deux nœuds hétérogènes, caractérisé en ce qu'il inclut des moyens d'insertion, dans au moins un message transmis par un agent utilisateur inclus dans l'un desdits nœuds avant établissement d'une session de communication entre lesdits nœuds, d'un indicateur de type représentatif du type d'au moins une adresse associée à cet agent utilisateur.

10. Système de transmission selon la revendication 9, caractérisé en ce qu'il inclut en outre des moyens de tri et de classification d'agents utilisateurs émetteurs de messages de requête à partir des indicateurs de type desdits agents, et une base de données destinée à mémoriser ladite classification.

11. Système selon la revendication 10, caractérisé en ce qu'il inclut en outre des moyens de comparaison d'indicateurs de types propres à au moins un agent utilisateur appelant et à au moins un agent utilisateur appelé.

12. Programme d'ordinateur incluant au moins une série d'instructions de code de programme pour l'exécution des étapes d'un procédé conforme à l'une des revendications 1 à 4 lorsque ledit programme est exécuté sur un ordinateur.

13. Programme d'ordinateur incluant au moins une série d'instructions de code de programme pour l'exécution des étapes d'un procédé conforme à l'une des revendications 5 et 6 lorsque ledit programme est exécuté sur un ordinateur.

14. Programme d'ordinateur incluant au moins une série d'instructions de code de programme pour l'exécution des étapes d'un procédé conforme à l'une des revendications 6 et 7 lorsque ledit programme est exécuté sur un ordinateur..

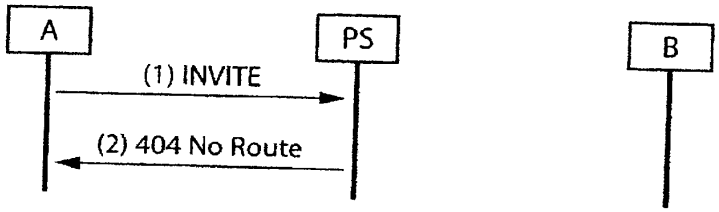


FIG. 1a
(ART ANTÉRIEUR)

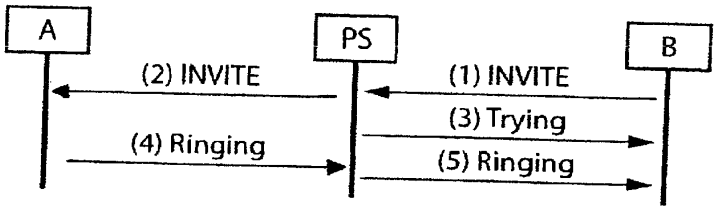


FIG. 1b
(ART ANTÉRIEUR)

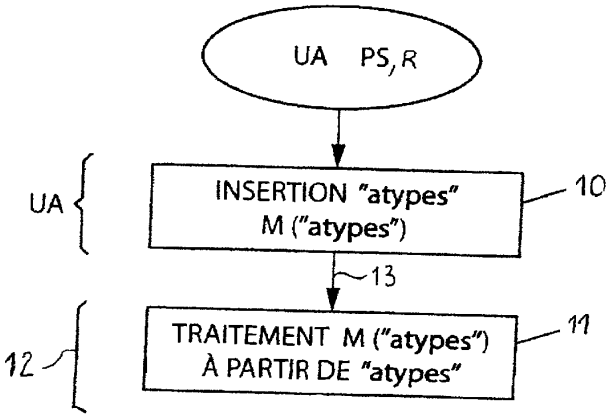


FIG. 2

Juniper Exhibit 1002, page 315

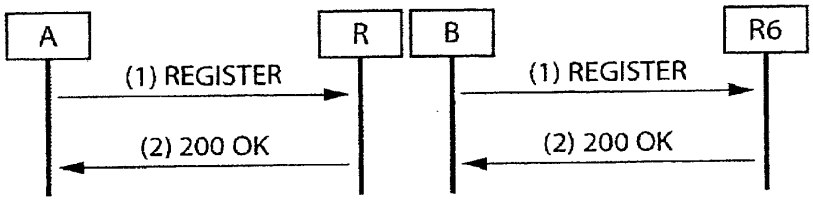


FIG. 3

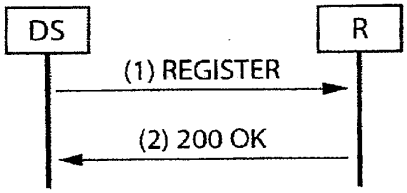


FIG. 4

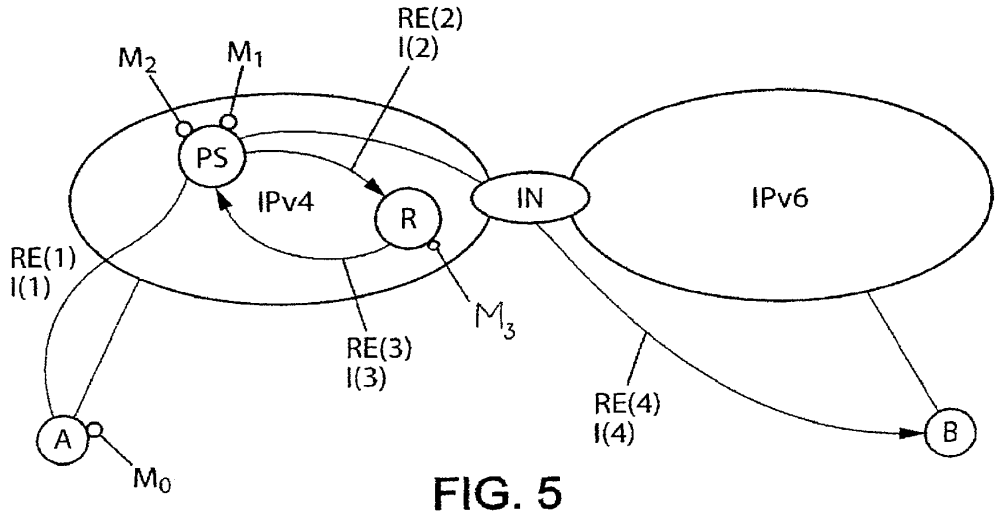


FIG. 5

Juniper Exhibit 1002, page 316

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
7 septembre 2007 (07.09.2007)

PCT

(10) Numéro de publication internationale
WO 2007/099248 A3

(51) Classification internationale des brevets :
H04L 29/12 (2006.01) *H04L 29/06* (2006.01)
H04L 29/08 (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2007/050808

(22) Date de dépôt international :
15 février 2007 (15.02.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0650681 28 février 2006 (28.02.2006) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 Place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BOUCADAIR, Mohamed** [FR/FR]; 124, rue Saint Jean, F-14000 Caen (FR). **NOISETTE, Yoann** [FR/FR]; 2, rue Dom Aubourg, F-14320 May Sur Orne (FR).

(74) Mandataire : **FRANCE TELECOM**; R & D/PIV/Brevets, WINDAL-VERCASSON Gaëlle, 38-40 rue du Général Leclerc, F-92794 Issy Les Moulineaux Cedex 9 (FR).

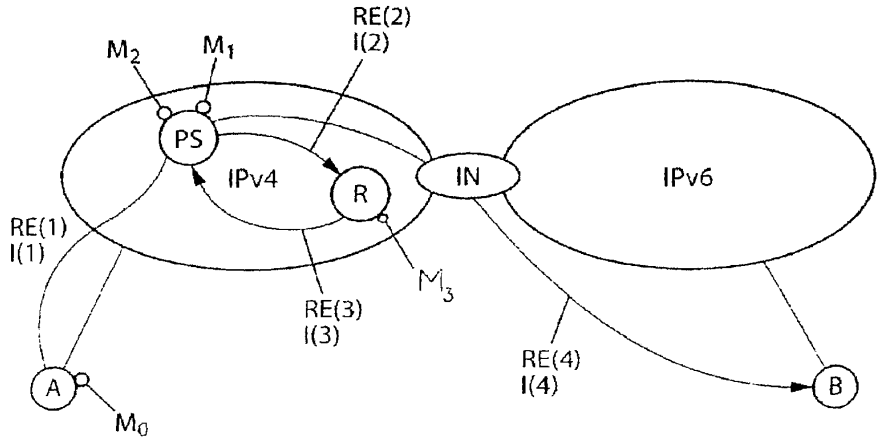
(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR,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

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM FOR CHARACTERISING HETEROGENEOUS COMMUNICATION NODES

(54) Titre : PROCEDE ET SYSTEME DE CARACTERISATION DE NOEUDS DE COMMUNICATION HETEROGENES



(57) Abstract: The invention relates to a method for the transmission of data between at least two heterogeneous nodes. Said method comprises at least one step of inserting an indicator representing at least one address allocated to a user agent (A) included in one of said nodes, into at least one message transmitted (RE(1), I(1)) by said user agent (A) before the establishment of a communication session between the nodes. The invention enables the rapid identification of the risk of incompatibility between the types of two user agents (A, B) to be brought into communication with each other, with a view to remedying any such incompatibility. The invention can be used for the intercommunication of user agents using type IPv4, IPv6 or dual stack (DS) in an IP network.

[Suite sur la page suivante]

WO 2007/099248 A3

BNSDOCID: <WO_____2007099248A3_I_>

ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, 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).

Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

(88) Date de publication du rapport de recherche internationale: 25 octobre 2007

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de transmission de données entre au moins deux nœuds hétérogènes. Le procédé selon l'invention inclut au moins une étape d'insertion, dans au moins un message transmis (RE(1), 1(1)) par un agent utilisateur (A) inclus dans l'un desdits nœuds avant établissement d'une session de communication entre lesdits nœuds, d'un indicateur de type représentatif de type d'au moins une adresse affectée à cet agent utilisateur (A). L'invention permet d'identifier rapidement des risques d'incompatibilité entre les types de deux agents utilisateurs (A, B) devant être mis en communication l'un avec l'autre, en vue de remédier le cas échéant à une telle incompatibilité. Application à l'intercommunication d'agents utilisateurs de type IPv4, IPv6 ou double pile (DS) en réseau IP.

BNSDOCID: <WO_____2007099248A3_I_>

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2007/050808

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/12 H04L29/08 H04L29/06

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 practical, 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.
X	CAMARILLO ERICSSON J ROSENBERG DYNAMICSOFT G: "The Alternative Network Address Types Semantics (ANAT) for the Session Description Protocol (SDP) Grouping Framework; draft-ietf-mmusic-anat-02.txt;" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, vol. mmusic, no. 2, 25 October 2004 (2004-10-25), XP015023068 ISSN: 0000-0004 page 1 page 4, line 33 - page 5, line 17 -/--	1-14

[X] Further documents are listed in the continuation of Box C. [X] 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 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
6 August 2007	14/08/2007

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lebas, Yves

BNSDOCID: <WO_____2007099248A3_I_>

CI

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2007/050808

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KAWARASAKI Y ET AL: "IPv4/IPv6 SIP interworking methods in dual-stack network" COMMUNICATIONS, 2003. APCC 2003. THE 9TH ASIA-PACIFIC CONFERENCE ON 21-24 SEPT. 2003, PISCATAWAY, NJ, USA,IEEE, vol. 3, 21 September 2003 (2003-09-21), pages 1124-1128, XP010687978 ISBN: 0-7803-8114-9 page 1126, left-hand column, line 1 - page 1127, left-hand column, last line ; figures 5-8	1-14
A	BALDI M ET AL: "ALEX: improving SIP support in systems with multiple network addresses" SIGNAL PROCESSING AND INFORMATION TECHNOLOGY, 2005. PROCEEDINGS OF THE FIFTH IEEE INTERNATIONAL SYMPOSIUM ON ATHENS, GREECE DEC. 18 - 21, 2005, PISCATAWAY, NJ, USA,IEEE, 18 December 2005 (2005-12-18), pages 164-169, XP010880999 ISBN: 0-7803-9313-9 page 166, left-hand column, line 13 - page 168, right-hand column, last line ; figures 2-4	1-14
A	EP 1 515 508 A (HITACHI, LTD) 16 March 2005 (2005-03-16) abstract paragraph [0008] - paragraph [0014] paragraph [0021] paragraph [0025] - paragraph [0026] paragraph [0030] paragraph [0044] - paragraph [0048] paragraph [0050]	1-14

BNSDOCID: <WO_____2007099248A3_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2007/050808

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1515508 A	16-03-2005	CN 1595933 A	16-03-2005
		JP 2005086467 A	31-03-2005
		US 2005066038 A1	24-03-2005

BNSDOCID: <WO_____2007099248A3_I_>

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2007/050808

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/12 H04L29/08 H04L29/06

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, COMPENDEX, INSPEC, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	CAMARILLO ERICSSON J ROSENBERG DYNAMICSOFT G: "The Alternative Network Address Types Semantics (ANAT) for the Session Description Protocol (SDP) Grouping Framework; draft-ietf-mmusic-anat-02.txt;" IETF STANDARD-WORKING-DRAFT, INTERNET ENGINEERING TASK FORCE, IETF, CH, vol. mmusic, no. 2, 25 octobre 2004 (2004-10-25), XP015023068 ISSN: 0000-0004 page 1 page 4, ligne 33 - page 5, ligne 17 -/--	1-14

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
6 août 2007	14/08/2007

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx 31 651 epo nl, Fax: (+31–70) 340–3016	Lebas, Yves

BNSDOCID: <WO_____2007099248A3_I_>

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2007/050808

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	KAWARASAKI Y ET AL: "IPv4/IPv6 SIP interworking methods in dual-stack network" COMMUNICATIONS, 2003. APCC 2003. THE 9TH ASIA-PACIFIC CONFERENCE ON 21-24 SEPT. 2003, PISCATAWAY, NJ, USA,IEEE, vol. 3, 21 septembre 2003 (2003-09-21), pages 1124-1128, XP010687978 ISBN: 0-7803-8114-9 page 1126, colonne de gauche, ligne 1 - page 1127, colonne de gauche, dernière ligne ; figures 5-8	1-14
A	BALDI M ET AL: "ALEX: improving SIP support in systems with multiple network addresses" SIGNAL PROCESSING AND INFORMATION TECHNOLOGY, 2005. PROCEEDINGS OF THE FIFTH IEEE INTERNATIONAL SYMPOSIUM ON ATHENS, GREECE DEC. 18 - 21, 2005, PISCATAWAY, NJ, USA,IEEE, 18 décembre 2005 (2005-12-18), pages 164-169, XP010880999 ISBN: 0-7803-9313-9 page 166, colonne de gauche, ligne 13 - page 168, colonne de droite, dernière ligne ; figures 2-4	1-14
A	EP 1 515 508 A (HITACHI, LTD) 16 mars 2005 (2005-03-16) abrégé alinéa [0008] - alinéa [0014] alinéa [0021] alinéa [0025] - alinéa [0026] alinéa [0030] alinéa [0044] - alinéa [0048] alinéa [0050]	1-14

BNSDOCID: <WO_____2007099248A3_I_>

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2007/050808

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1515508 A	16-03-2005	CN 1595933 A	16-03-2005
		JP 2005086467 A	31-03-2005
		US 2005066038 A1	24-03-2005

BNSDOCID: <WO_____2007099248A3_I_>

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
3 janvier 2008 (03.01.2008)

PCT

(10) Numéro de publication internationale
WO 2008/001007 A2

(51) Classification internationale des brevets : Non classée

(21) Numéro de la demande internationale :
PCT/FR2007/051531

(22) Date de dépôt international : 26 juin 2007 (26.06.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0605945 30 juin 2006 (30.06.2006) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BOUCADAIR, Mohamed** [FR/FR]; 124, rue Saint Jean, F-14000 Caen (FR). **NOISETTE, Yoann** [FR/FR]; 2, rue Dom Aubourg, F-14320 May sur Orne (FR).

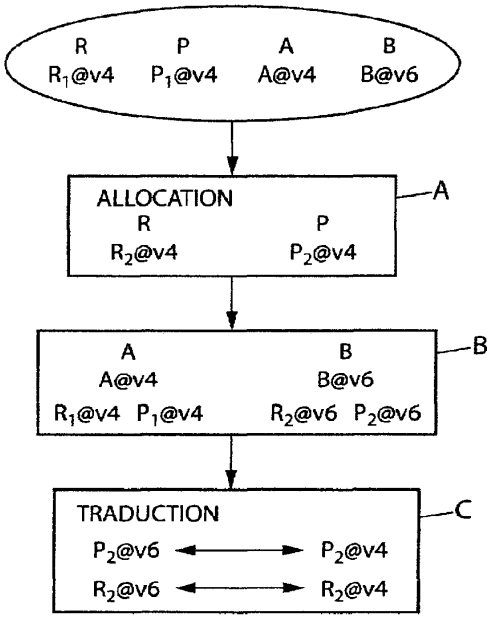
(74) Mandataire : **FRANCE TELECOM/FTR & D/PIV/BREVETS**; Gaëlle WINDAL-VERCASSON, 38-40, rue du Général Leclerc, F-92794 Issy les Moulineaux Cédex (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR,

[Suite sur la page suivante]

(54) Title: METHOD FOR ADDRESSING CALL TRANSMISSION AND SERVICE ELEMENTS BETWEEN HETEROGENEOUS NODES

(54) Titre : PROCEDE D'ADRESSAGE DES ELEMENTS DE SERVICE ET DE TRANSMISSION D'APPEL ENTRE NOEUDS HETEROGENES



(57) Abstract: A SIP server addressing method for the inter-operation of SIP nodes (A, B) of a determined IP type in which each SIP server (P, R) is attributed (A) an auxiliary address (R_2@v4, P_2@v4) of the same IP type as their original address (R_1@v4, P_1@v4), wherein the auxiliary address corresponds to a distinct IP type communication address, all SIP nodes of the same IP type as this SIP server are supplied (B) with the original address, and to all SIP nodes with an IP type distinct from the IP type of this SIP server, this communication address and the communication address of one of the IP types is translated (C) into the auxiliary address, of the same IP type as the IP type of the original address.

(57) Abrégé : Un procédé d'adressage de serveurs SIP pour l'inter-fonctionnement de nœuds SIP (A, B) d'un type IP déterminé dans lequel on alloue (A) à tout serveur SIP (P, R) une adresse auxiliaire (R_2@v4, P_2@v4) de même type IP que leur adresse d'origine (R_1@v4, P_1@v4), l'adresse auxiliaire correspondant à une adresse de communication de type IP distinct, on fournit (B) à tout nœud SIP du même type IP que ce serveur SIP l'adresse d'origine et à tout nœud SIP de type IP distinct du type IP de ce serveur SIP cette adresse de communication et on traduit (C) l'adresse de communication de l'un ou l'autre type IP en l'adresse auxiliaire, de même type IP que le type IP de l'adresse d'origine.

WO 2008/001007 A2

CI

LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :

— *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

Juniper Exhibit 1002, page 326

PROCÉDÉ D'ADRESSAGE DES ELEMENTS DE SERVICE ET DE TRANSMISSION D'APPEL ENTRE NŒUDS HÉTÉROGÈNES

L'invention se situe dans le domaine des télécommunications, et plus particulièrement dans celui de la téléphonie sur IP.

Des réseaux conformes à un protocole de communication dit IP (abréviation bien connue de l'homme du métier de l'expression anglaise "Internet Protocol") sont de plus en plus souvent utilisés en tant que supports universels d'une multitude de services et applications. Ce protocole IP a joué un rôle fédérateur auprès de multiples opérateurs qui ont choisi ce protocole pour mutualiser des offres de service jusqu'alors disparates.

IPv4 est une version du protocole de communication IP qui est utilisée depuis des années.

Pour satisfaire des contraintes imposées par de tels services de communication et plus particulièrement pour répondre aux besoins accrus en termes d'adresses, des opérateurs et des constructeurs d'équipements réseau se sont unis pour spécifier un protocole de communication de nouvelle génération, communément référencé IPv6, défini par des spécifications ainsi que des documents d'analyse qui sont à un stade de développement suffisamment avancé pour permettre à présent d'envisager un déploiement opérationnel dans les réseaux des opérateurs.

Néanmoins, l'introduction de cette nouvelle génération de protocole pose des problèmes significatifs liés à un besoin de garantir une interopérabilité et un interfonctionnement du protocole IPv6 et du protocole IPv4 qui est déjà déployé dans les réseaux IP.

Dans la couche transport, des mécanismes ont été proposés, voire standardisés à l'IETF (abréviation bien connue de l'homme du métier de l'expression anglaise "Internet Engineering Task Force") tels qu'une technique dite NAT-PT et diverses techniques connues sous le vocable anglais « tunneling » et consistant à encapsuler des données IPv6 dans des datagrammes IPv4 ou inversement.

En outre, des mises à jour et des adaptations d'architectures et

de plateformes de services sont nécessaires pour permettre un interfonctionnement entre clients situés dans des environnements IP de nature différente (IPv4 ou IPv6), et ceci d'une manière aussi transparente que possible pour le client final.

Parmi ses activités multimédia, l'IETF a standardisé un protocole appelé SIP (abréviation bien connue de l'homme du métier de l'expression anglaise "Session Initiation Protocol") offrant pour principales fonctions l'initiation, la modification et la terminaison de sessions multimédia. Le protocole SIP constitue un exemple intéressant d'application de la présente invention. Le protocole SIP s'appuie sur un protocole SDP (abréviation bien connue de l'homme du métier de l'expression anglaise "Session Description Protocol") pour produire une description de paramètres associés à la session concernée. Une fois une négociation réussie entre deux parties participant à un appel, ces dernières peuvent échanger des flux média grâce à une activation d'un protocole RTP (abréviation bien connue de l'homme du métier de l'expression anglaise "Real time Transport Protocol"). Des paramètres de sessions RTP sont pré-négociés *via* des messages de signalisation SIP, notamment dans la partie SDP. Ces paramètres sont principalement des adresses de terminaison et des numéros de port qui seront utilisés de part et d'autre.

Depuis la première version du protocole SIP, décrite dans un document référencé RFC 2543 (RFC signifiant "requête pour commentaires" ou "Request For Comment" en anglais), ce dernier supporte le protocole IPv6. Une implémentation conforme à la RFC2543, ou à sa mise à jour RFC3261, décode en principe facilement des adresses conformes aux protocoles IPv4 et IPv6. Une telle adresse peut être introduite dans un champ spécifique tel un entête « CONTACT » ou dans des en-têtes de la partie SDP. Cependant, la présence de telles adresses peut empêcher l'établissement des appels SIP dans le cas où les deux terminaux ne sont pas joignables dans un même environnement IP, à savoir si l'une dispose d'une adresse IPv4 et l'autre d'une adresse IPv6. Ainsi quand un agent utilisateur de type IPv4 A initie une session SIP vers un agent utilisateur de

type IPv6 qui s'est enregistré auprès d'un serveur de localisation (noté R ci-après) IPv4, l'échange de messages SIP produit est décrit dans la figure 1a, où un premier agent utilisateur A désireux d'entrer en contact avec un deuxième agent utilisateur B envoie un message « INVITE » vers un serveur de proximité dit serveur proxy (noté PS ci-après) en utilisant une adresse IPv4 propre à ce dernier. Le serveur proxy PS est ici un serveur attaché à un environnement IPv4 exclusivement. Une fois le message reçu par le serveur proxy PS, ce dernier effectue une requête auprès d'un serveur de localisation encore appelé serveur d'enregistrement et récupère ainsi l'adresse du deuxième agent utilisateur B. Cette adresse étant par hypothèse une adresse IPv6, le serveur proxy PS ne connaît pas de route vers cette destination étant donné que ce serveur proxy PS est exclusivement de type IPv4. Un message d'erreur est alors envoyé vers l'agent utilisateur A concluant à une impossibilité d'établir une session SIP entre les premier et deuxième agents utilisateurs A et B. Ce message d'erreur est noté (2) 404 « No Route » sur la figure 1a.

Si l'on suppose maintenant que le serveur proxy PS peut néanmoins joindre l'adresse de localisation du premier agent utilisateur A ainsi que celle du deuxième agent utilisateur B, un autre échange de messages SIP est observé, quand le deuxième agent utilisateur B essaye d'appeler le premier agent utilisateur A, ainsi que représenté en figure 1b.

Dans ce cas de figure, le serveur proxy PS achemine un message « INVITE » reçu du deuxième agent utilisateur B vers l'adresse de localisation du premier agent utilisateur A. Ce message « INVITE » contient une offre SDP décrivant, outre des capacités offertes par le premier agent utilisateur B en termes de CODEC (pour "codeur/décodeur"), un numéro de port RTP et une adresse qu'utilisera le deuxième agent utilisateur B pour émettre/recevoir des flux RTP. Dans le cas de la figure 1b, cette adresse est de type IPv6. Ainsi, lorsque l'agent utilisateur A reçoit ce message « INVITE », il ne peut que refuser l'ouverture de la session car cet agent utilisateur est un client IPv4. Au mieux pourra-t-il, selon les implémentations, renvoyer un message d'erreur indiquant qu'il ne supporte pas les connexions

réseaux vers l'adresse IP de l'agent utilisateur B. Dans les deux exemples précédents, décrits en liaison avec les figures 1a et 1b, les sessions SIP ne peuvent ainsi pas être établies.

Une coexistence d'adresses IP de types différents pourra affecter d'autres appels que ceux ayant fait l'objet de la représentation graphique décrite ci-dessus. Ainsi, des appels destinés à des clients de type IP double pile, DS, (abréviation bien connue de l'homme du métier de l'expression anglaise "Dual Stack"), peuvent aussi ne pas aboutir à des échanges de flux média, les agents utilisateurs de type DS étant en mesure de traiter les deux types d'adresse IPv4 et IPv6. Ceci est dû au fait que le protocole SIP de base ne permet de renseigner qu'une seule adresse IP pour l'émission ou la réception des flux média. Pour pallier ce problème, des documents référencés RFC 4092 et RFC 4091 introduisent une nouvelle sémantique consistant, entre autres, à définir un indicateur dénoté « sdp-anat ». Cette nouvelle sémantique permet à un agent utilisateur, d'annoncer et/ou de découvrir un ou plusieurs types d'adresse. Ainsi, des agents utilisateurs de type double pile sont en mesure d'indiquer dans leur offre SDP leurs deux adresses IPv4 et IPv6. Grâce à cette technique, tous les appels de/vers un agent utilisateur de type DS vers des/de clients mono version (i.e. compatibles avec le protocole IPv4 seulement ou avec le protocole IPv6 seulement) peuvent donner lieu à des sessions SIP réussies.

Dans un cas où deux nœuds formant des extrémités d'une liaison de communication destinée à véhiculer un appel donné sont mono version, l'opérateur de service de téléphonie SIP concerné peut avoir recours à des applications ALG (abréviation bien connue de l'homme du métier de l'expression anglaise "Application Layer Gateway"), pour modifier les offres SDP afin d'assurer une cohérence entre le type d'adresse supporté et celui contenu dans les messages SIP reçus. Pour ce faire les serveurs SIP utilisent des informations relatives à la couche transport, et non propres au protocole SIP, pour router les appels ou pour déterminer le recours à des applications ALG pour altérer le contenu des offres SDP. Un tel comportement des serveurs SIP n'est pas décrit dans la norme.

D'une manière générale le problème lié aux interconnexions de deux agents utilisateurs hétérogènes (c'est-à-dire de types IP distincts) n'a pas été étudié en détail par la communauté des télécommunications. Excepté une proposition ANAT décrite par (RFC 4091, RFC 4092) qui résout une partie du problème, il n'existe en particulier pas de document de l'IETF décrivant le comportement des serveurs SIP pour acheminer des appels reliant deux agents utilisateurs appartenant à deux environnements IP différents.

En outre, les techniques existantes présentent les inconvénients suivants :

- le recours aux applications ALG et aux fonctions supplémentaires n'est pas documenté. Le serveur proxy PS ne dispose pas de moyens prévus par la RFC 3261 pour faciliter cette tâche ;
- la solution n'est pas générique: la philosophie de routage d'appel et d'intervention du serveur proxy PS dépend de la solution d'interconnexion déployée au niveau transport ;
- le serveur proxy PS ne dispose pas de moyens pour déterminer si un agent utilisateur est de type IPv4, IPv6 ou double pile.

Les travaux conduits par les inventeurs ont mené ceux-ci à conclure que, nonobstant un besoin qui ressort de l'étude qui précède, il n'existe dans l'état de la technique aucune disposition visant à permettre à un moyen de communication appartenant à un réseau de communication conforme à un protocole IP d'identifier de manière simple et générique le type IP d'adresse associé à un agent utilisateur donné, une telle carence expliquant pourquoi la plupart des techniques de gestion de communications entre nœuds hétérogènes actuellement à l'étude sont insuffisantes et ne répondent pas aux besoins de service consistant à permettre des communications hétérogènes.

La présente invention a pour objet de remédier aux inconvénients et limitations des techniques actuelles, compte tenu de la présence conjointe des protocoles de communication IPv4, IPv6 ou IP ISO défini par la norme ISO 8473 dans les réseaux IP.

Plus précisément, un objet de l'invention est de permettre aux serveurs SIP, de connaître le type IP d'agents utilisateurs cherchant à communiquer, afin de permettre l'établissement réussi de sessions entre ces agents, qu'ils soient ou non de même type, de faciliter le routage des appels et d'optimiser l'usage d'adresses IP.

Conformément à l'invention exposée dans la présente demande de brevet, on considère à titre de seul exemple, la téléphonie sur IP désignée couramment par VoIP pour Voice over IP en anglais, ou généralement groupée sous le thème des services conversationnels.

L'invention s'inscrit dans la problématique générale des services de transmission basés sur le protocole SIP défini par la RFC 3261 et déployés à la fois pour des clients IPv4 et des clients IPv6. Ces services peuvent être des services de voix, de vidéo, de présence, etc.

L'invention propose un mécanisme simple pour faciliter l'établissement de sessions SIP entre deux clients ou nœuds SIP hétérogènes, un attaché à un domaine IPv4 et l'autre à un domaine IPv6 par exemple.

La présente invention a, notamment, en conséquence pour objet la mise en œuvre d'un procédé d'adressage de serveurs SIP pour l'inter-fonctionnement de nœuds SIP hétérogènes permettant d'allouer aux serveurs SIP des ressources pour reconnaître le type IP des agents utilisateurs UA. Par type IP d'un agent utilisateur, on entend la ou les versions de protocole IP (par exemple IPv4, IPv6) que cet agent utilisateur est à même de mettre en œuvre par l'intermédiaire de la ou des interfaces réseaux dont dispose le nœud SIP qui l'abrite. Des nœuds SIP hétérogènes sont donc des nœuds SIP qui comprennent des agents utilisateurs de types IP différents.

Un autre objet de la présente invention est en outre la mise en œuvre d'un procédé d'adressage de serveurs SIP pour l'inter-fonctionnement de nœuds SIP hétérogènes permettant de simplifier et ainsi de faciliter le routage des appels.

Un autre objet de la présente invention est, enfin, la mise en

œuvre d'un procédé d'adressage de serveurs SIP permettant d'optimiser l'usage d'adresses IP.

Le procédé d'adressage de serveurs SIP pour l'inter-fonctionnement de nœuds SIP hétérogènes d'un premier respectivement d'un deuxième type IP, objet de l'invention, est remarquable en ce qu'il inclut au moins l'allocation à tout serveur SIP, opérant dans un environnement IP de l'un ou l'autre type IP et muni d'une adresse d'origine d'un type IP déterminé, d'une adresse auxiliaire de même type IP que le type de l'adresse d'origine et correspondant à une adresse de communication de type IP distinct, la fourniture comme adresse d'appel, à tout nœud SIP du même type IP que ce serveur SIP de cette adresse d'origine dans cet environnement IP et à tout nœud SIP, de type IP autre que le type IP de ce serveur SIP, de cette adresse de communication, la traduction de cette adresse de communication de l'un ou l'autre type IP en cette adresse auxiliaire de même type IP que le type IP de cette adresse d'origine.

Le mode opératoire du procédé d'adressage objet de l'invention permet d'assurer l'intercommunication de tout nœud SIP à partir d'un environnement IP d'un type IP correspondant à celui des serveurs SIP ou d'un type IP distinct.

Le procédé d'adressage objet de l'invention est en outre remarquable en ce que cette adresse de communication est configurée comme entrée DNS de l'environnement IP de type IP distinct de celui de ce serveur SIP.

Le procédé d'adressage objet de l'invention est enfin remarquable en ce que les serveurs SIP incluent tout serveur d'enregistrement respectivement tout serveur proxy de l'un ou l'autre des environnements IP.

L'invention couvre également un procédé de communication entre au moins un serveur opérant dans un environnement de type IP déterminé et au moins un nœud du réseau, ce nœud étant de même type IP ou de type IP distinct du type IP déterminé.

Ce procédé de communication est remarquable en ce qu'il

comprend les étapes suivantes, allocation au serveur d'au moins deux adresses dans l'environnement de type IP déterminé, comprenant une adresse dite d'origine et une adresse dite auxiliaire, à laquelle est associée par traduction une adresse de communication dans un environnement de type IP distinct du type IP déterminé, la fourniture à ce nœud, comme adresse d'appel du serveur de cette adresse d'origine, si le nœud est de même type IP que le type IP déterminé, respectivement de cette adresse de communication, si le nœud est de type IP distinct du type IP déterminé, et, sur appel de ce serveur par ce nœud, la discrimination du type IP de ce nœud en fonction de l'adresse d'origine ou auxiliaire du serveur sur laquelle est reçu cet appel.

Le procédé de communication, objet de l'invention, est en outre remarquable en ce que, le serveur étant un serveur d'enregistrement, ce procédé comprend également une étape d'enregistrement du nœud en fonction du type IP discriminé dans au moins une base de données.

Le procédé objet de l'invention est en outre remarquable en ce que ce serveur d'enregistrement maintient au moins deux bases de données comprenant respectivement les nœuds de même type IP que le type IP déterminé et les nœuds de type IP distincts du type IP déterminé. Les adresses stockées dans ces bases de données sont de même type que celui du serveur proxy.

Le procédé de communication, objet de l'invention, est également remarquable en ce que le nœud présentant au moins deux types IP, à savoir le type IP déterminé et au moins un type IP distinct de ce type IP déterminé, ce procédé comprend une étape de transmission par ce nœud d'une requête d'enregistrement vers l'adresse d'origine du serveur d'enregistrement, et une étape de transmission par ce nœud d'au moins une requête d'enregistrement vers l'adresse de communication du serveur, destinée à être reçue après traduction sur l'adresse auxiliaire du serveur.

Le procédé de communication objet de l'invention est également remarquable en ce que le serveur étant un serveur proxy et l'appel du serveur proxy par le nœud mettant en œuvre une transmission au serveur

proxy d'une requête d'appel du nœud appelant vers un nœud appelé, ce procédé comprend également une première étape de transmission du serveur proxy vers le serveur d'enregistrement d'une requête de type IP du nœud appelé, une deuxième étape de transmission du serveur d'enregistrement vers le serveur proxy du type IP du nœud appelé enregistré dans la base de données et d'une adresse du nœud appelé et une étape de routage de cet appel du nœud appelant vers le nœud appelé, en fonction du type IP du nœud appelant discriminé par le serveur proxy et du type IP du nœud appelé transmis par le serveur d'enregistrement.

Le procédé objet de l'invention est enfin remarquable en ce que lors de la deuxième étape de transmission, l'adresse du nœud appelé transmise par le serveur d'enregistrement est une adresse dans l'environnement de type IP déterminé dans lequel opère le serveur proxy.

Le procédé de communication objet de l'invention est également remarquable en ce que au cours de l'exécution de l'étape d'enregistrement,, pour tout nœud SIP de type IP déterminé, l'adresse IP enregistrée pour ledit nœud dans la base de données par le serveur d'enregistrement est systématiquement du même type IP que le serveur proxy utilisé par le service, ceci afin d'assurer l'exploitation ultérieure de ladite adresse par ledit serveur proxy et en particulier pour le routage de l'appel.

L'invention couvre également un serveur SIP d'enregistrement opérant dans un environnement IP de type IP déterminé en présence d'un autre environnement IP de type IP distinct et comportant des organes d'entrée sortie reliés à une unité centrale de traitement et à une mémoire de travail, remarquable en ce qu'il comporte, outre une adresse IP d'origine, une adresse IP auxiliaire de type IP correspondant à cet environnement IP, des moyens de discrimination du type IP de tout nœud SIP opérant un enregistrement en fonction de l'adresse d'appel d'origine respectivement de communication correspondant à cette adresse auxiliaire utilisée par ce nœud SIP, dans une requête d'enregistrement transmise à ce serveur SIP d'enregistrement, des moyens de première et de deuxième base de données d'enregistrement de chaque nœud SIP candidat, correspondant à un nœud

SIP de même type IP que le type IP de ce serveur SIP d'enregistrement, dont l'adresse d'appel est l'adresse d'origine de ce dernier, respectivement de type IP distinct du type IP de ce serveur SIP d'enregistrement, dont l'adresse d'appel est l'adresse auxiliaire de ce serveur SIP d'enregistrement par l'intermédiaire de cette adresse de communication.

L'invention couvre enfin un serveur proxy SIP opérant en transmission d'une requête d'appel d'un nœud SIP appelé par un nœud SIP appelant, de type IP déterminé identique ou distinct, dans un environnement IP de type IP déterminé en présence d'un autre environnement IP de type IP distinct, ce serveur proxy SIP comportant des organes d'entrée – sortie reliés à une unité centrale de traitement et à une mémoire de travail.

Il est remarquable en ce qu'il inclut, outre une adresse IP d'origine correspondant à cet environnement IP de type IP déterminé, une adresse auxiliaire de même type IP que le type IP de l'adresse d'origine, des moyens de discrimination, à partir de la requête d'appel du type IP de tout nœud SIP appelant, en fonction de l'adresse d'appel qui peut être soit l'adresse d'origine, soit une adresse auxiliaire de ce serveur proxy SIP qui correspond à l'adresse d'appel initiale, des moyens de discrimination, par un serveur SIP d'enregistrement objet de l'invention précité, du type IP du nœud SIP appelé, et des moyens de transmission et de routage de cette requête d'appel, compte tenu du type IP du nœud SIP appelé.

Ils seront mieux compris à la lecture de la description et à l'observation des dessins ci-après dans lesquels, outre les figures 1a et 1b relatives à l'art antérieur :

- la figure 2a représente à titre purement illustratif un organigramme des étapes essentielles du procédé d'adressage de serveur SIP, objet de la présente invention ;
- la figure 2b représente, à titre illustratif, une configuration réseau IP en présence d'un premier environnement IP de type IPv4 et d'un deuxième environnement IP de type IP distinct, IPv6, interconnectés par un nœud intermédiaire ;
- la figure 3a représente, à titre illustratif, un organigramme des étapes

essentielles d'un processus d'enregistrement de nœud SIP auprès d'un serveur d'enregistrement SIP, grâce à la mise en œuvre du procédé d'adressage conforme à l'objet de la présente invention ;

- la figure 3b représente, à titre illustratif, un organigramme spécifique de mise en œuvre du processus d'enregistrement illustré en figure 3a, dans le cas où le nœud SIP est un nœud SIP de type IP double pile ;
- la figure 4a représente, à titre illustratif, un organigramme des étapes essentielles d'un procédé de transmission d'un appel entre un nœud SIP appelant et un nœud SIP appelé par l'intermédiaire d'un proxy SIP grâce au procédé d'adressage et au processus d'enregistrement objets de la présente invention ;
- la figure 4b représente, à titre illustratif, un organigramme des étapes essentielles d'un procédé de communication conforme à l'objet de la présente invention, entre un serveur opérant dans un environnement de type IP déterminé et au moins un nœud d'un réseau ;
- la figure 4c représente à titre illustratif une variante de mise en œuvre du procédé de communication illustré en figure 4b, dans lequel le type IP du nœud appelant et du nœud appelé est établi par un serveur d'enregistrement sur requête d'un serveur proxy ;
- les figures 5a à 5c représentent, à titre illustratif, un protocole de transmission d'appel entre nœud SIP de même type IP, IPv4 figure 5a, IPv6 figure 5b et de type IP distinct, IPv4 - IPv6 figure 5c ;
- la figure 6a représente, à titre illustratif, un schéma fonctionnel d'un serveur d'enregistrement SIP conforme à l'objet de la présente invention ;
- la figure 6b représente, à titre illustratif, un schéma fonctionnel d'un serveur proxy SIP conforme à l'objet de la présente invention.

Une description plus détaillée du procédé d'adressage de serveur SIP pour l'inter-fonctionnement de nœuds SIP d'un premier respectivement d'un deuxième type IP sera maintenant donnée en liaison avec la figure 2a et la figure 2b.

En référence aux figures précitées, on considère à titre d'exemple un premier environnement IP de type IPv4 et un deuxième environnement IP

de type IPv6.

Ainsi que représenté en figure 2b, on indique que, de manière non limitative, la présente description est établie dans le contexte où l'ensemble des éléments constituant la plateforme de service SIP réside dans l'environnement IPv4 et en conséquence, les éléments précités, c'est-à-dire le serveur d'enregistrement R et le serveur proxy SIP P sont représentés dans l'environnement IPv4.

On indique toutefois que le procédé objet de la présente invention est tout à fait applicable en inversant les rôles entre l'environnement IPv4 et l'environnement IPv6, les éléments serveur d'enregistrement R et serveur proxy SIP P étant alors placés dans l'environnement IPv6 dans cette hypothèse.

En outre, on considère à titre d'exemple non limitatif et afin de faciliter la compréhension de l'ensemble, l'existence d'un nœud intermédiaire IN représenté en figure 2b pour « Intermediate Node » en anglais situé à la frontière des environnements IPv4 et IPv6. Ce nœud intermédiaire représente fonctionnellement les éléments requis pour l'interconnexion des domaines IPv6 et IPv4 tels que les éléments NAT-PT précédemment cités dans la description. Toutefois, on indique que les fonctions / traitements / opérations exécutés par le nœud intermédiaire IN peuvent être répartis dans le réseau en fonction de l'implémentation du service mis en place par un opérateur de ce dernier.

En référence aux figures 2a et 2b, on dispose donc d'un serveur d'enregistrement R d'adresse d'origine R_1@v4, d'un serveur proxy SIP P d'adresse d'origine P_1@v4, d'un nœud SIP A d'adresse A@v4 dans l'environnement IPv4 et d'un nœud SIP B d'adresse B@v6 dans l'environnement IPv6.

Ainsi que représenté en figure 2a, le procédé objet de l'invention consiste à allouer en une étape A, à tout serveur SIP, i.e. serveur d'enregistrement R et serveur proxy SIP P, opérant dans un environnement IP de l'un ou l'autre type IP, une adresse auxiliaire de même type IP que le type de l'adresse d'origine.

Ainsi à l'étape A de la figure 2a, au serveur d'enregistrement R est allouée l'adresse auxiliaire R_2@v4 et au serveur proxy SIP P est allouée l'adresse auxiliaire P_2@v4. A l'adresse auxiliaire précitée on associe une adresse de communication de type IP distinct du type de l'adresse auxiliaire.

L'étape A est alors suivie d'une étape B consistant à fournir à tout nœud SIP, du même type IP que le serveur SIP, l'adresse d'origine de chaque serveur SIP dans l'environnement IP correspondant, et à tout nœud SIP,de type IP autre que le type IP du serveur proxy SIP, une adresse de communication correspondant à l'adresse auxiliaire allouée à chaque serveur SIP.

Ainsi que représenté à l'étape B de la figure 2a, on dispose après la fourniture des adresses précitées, afin de mettre en communication les nœuds SIP A et B :

Nœud SIP A :

- A@v4, adresse du nœud SIP A dans l'environnement IPv4 ;
- R_1@v4, adresse d'origine du serveur d'enregistrement R dans l'environnement IPv4 ;
- P_1@v4, adresse d'origine du serveur proxy SIP P dans l'environnement IPv4 ;

Nœud SIP B :

- B@v6, adresse du nœud SIP B dans l'environnement IPv6 ;
- R_2@v6, adresse de communication du serveur d'enregistrement R ;
- P_2@v6, adresse de communication du serveur proxy SIP P.

L'étape de fourniture d'adresses précitées est alors suivie d'une étape C consistant à traduire l'adresse de communication de l'un ou l'autre type IP en l'adresse auxiliaire de même type IP que le type IP de l'adresse d'origine des serveurs SIP.

A l'étape C de la figure 2a, l'opération de traduction est notée selon les relations :

$$P_2@v6 \leftrightarrow P_2@v4$$

$$R_2@v6 \leftrightarrow R_2@v4.$$

On comprend ainsi que, grâce au processus d'allocation

d'adresses auxiliaires et en fait de double adressage de chaque serveur SIP mis en jeu, l'intercommunication entre tout nœud SIP de l'un et/ou de l'autre environnement IP, IPv4 ou IPv6, peut ainsi être exécutée.

D'une manière générale, on indique que les adresses d'origine R_1@v4 et P_1@v4 des serveurs SIP sont configurées dans les entrées DNS désignées entrées de nommage de noms de domaines dans un environnement IP correspondant, IPv4.

Il en est de même en ce qui concerne les adresses de communication R_2@v6 et P_2@v6 lesquelles peuvent être configurées comme entrée DNS pour l'environnement IPv6.

Enfin, on indique que les serveurs SIP objets du double adressage, conformément au procédé d'adressage objet de l'invention, incluent tout serveur d'enregistrement respectivement tout serveur proxy SIP de l'un ou l'autre des environnements IP.

Un processus d'enregistrement d'un nœud SIP de type IP déterminé auprès d'un serveur d'enregistrement, tel que le serveur R représenté en figure 2b, sera maintenant décrit en liaison avec les figures 3a et 3b.

En référence à la figure 3a précitée, on indique que le nœud SIP précité peut être constitué par un nœud SIP de type IPv4 ou IPv6, le serveur d'enregistrement R opérant dans un environnement IP d'un même type IP ou d'un autre type IP que celui du nœud SIP considéré.

Ainsi que représenté en figure 3a, le serveur d'enregistrement R comporte bien entendu une adresse d'origine R_1@v4 dans l'exemple non limitatif de la figure 2b, et une adresse auxiliaire de type IP correspondant à cet environnement IP, c'est-à-dire l'adresse R_2@v4 allouée conformément au procédé d'adressage tel que décrit précédemment dans la description avec la figure 2a et la figure 2b.

En référence à la figure 3a, on considère un nœud ou terminal A de l'un des types IPv4 ou IPv6, à ce terminal A étant ainsi allouée une adresse A@vx, x désignant soit le type IPv4, soit le type IPv6 ou encore le type double pile tel que décrit précédemment dans la description.

En référence à la figure 3a, le procédé objet de l'invention consiste au moins, sur transmission d'une requête d'enregistrement notée RR(R@vx), à discriminer le type IP du nœud SIP A, en fonction de l'adresse d'appel d'origine respectivement auxiliaire correspondant à l'adresse de communication utilisée initialement par le nœud SIP A pour transmettre la requête d'enregistrement.

On comprend en particulier que, dans la requête d'enregistrement, R@vx désigne soit l'adresse d'origine R_1@v4 du serveur d'enregistrement soit au contraire une adresse de communication telle que l'adresse R_2@v6 mentionnée précédemment dans la description en liaison avec la figure 2a.

L'adresse de communication précitée correspond bien entendu à l'adresse auxiliaire R_2@v4 allouée au serveur d'enregistrement R ainsi que mentionné précédemment dans la description.

A l'étape D de la figure 3a, l'opération de transmission est notée par la relation symbolique :

$$A \xrightarrow{RR(R@vx)} R.$$

L'étape D est alors suivie d'une étape E consistant à discriminer le type IP du nœud SIP A en fonction de l'adresse d'appel d'origine respectivement de communication correspondant à l'adresse auxiliaire utilisée par le nœud SIP dans la requête d'enregistrement précitée.

A l'étape E de la figure 3a, l'opération de discrimination est donnée par les relations :

$$vx=v4 \text{ si } R@vx=R_1@v4,$$

$$vx=v6 \text{ si } R@vx \equiv R_2@v4.$$

Dans les relations précédentes et dans la suite de la description, le signe = représente l'identité directe des adresses et le signe $\equiv$ représente l'identité des adresses après traduction, par le nœud intermédiaire IN.

En effet, on comprend que lorsque l'adresse d'appel est une adresse de communication, celle-ci est transformée en adresse auxiliaire ce qui permet bien entendu de discriminer le type IP du nœud SIP à l'enregistrement.

Dans les relations précédentes, vx désigne en fait le type IP discriminé du terminal SIP.

L'étape E est alors suivie d'une étape F consistant à établir et maintenir une première $DB_1(v4)$ et une deuxième $DB_2(v6)$ bases de données de l'enregistrement de chaque nœud SIP.

On comprend en effet, que suite à la discrimination réalisée à l'étape E, chaque nœud SIP correspond à un nœud SIP de même type IP que le type IP du serveur proxy, de type v4 dans l'exemple donné, en liaison avec la figure 2b et pour lequel l'adresse d'appel est l'adresse d'origine de ce dernier.

Au contraire, un nœud SIP est de type IP distinct du type IP du serveur proxy, lorsque l'adresse d'appel correspond à l'adresse auxiliaire de ce serveur d'enregistrement par l'intermédiaire de l'adresse de communication.

L'établissement des bases de données d'enregistrement précitées peut correspondre à l'insertion d'une référence à l'adresse de chaque nœud SIP correspondant, notée pour cette raison A@vx=A@v4 lorsque le terminal candidat A est inscrit dans la première base de données d'enregistrement $DB_1(v4)$, et A@vx=A'@v4, l'adresse A@v6 ayant été traduite en cours de route en cette adresse A'@v4, lorsque l'adresse du nœud SIP correspondant, correspond à un nœud SIP de type v6, l'adresse correspondante A'@v4 étant inscrite dans la deuxième base de données d'enregistrement $DB_2(v6)$.

On comprend, en particulier, que le processus d'enregistrement objet de l'invention est mis en œuvre en raison du fait que tous les nœuds SIP de type IPv4, par configuration, contactent le serveur d'enregistrement R sur son adresse d'origine exclusivement, alors que tous les nœuds SIP de type IPv6 prennent contact avec le serveur d'enregistrement R uniquement par l'adresse de communication R_2@v6, laquelle est bien entendu transformée en adresse auxiliaire R_2@v4. Le serveur d'enregistrement reçoit donc toute requête émise par un terminal SIP de type IPv6 exclusivement sur son adresse auxiliaire.

Dans le cas d'un terminal SIP double pile A_{DS}, c'est, de préférence, l'adresse utilisée par ce dernier pour s'enregistrer auprès du serveur d'enregistrement R qui permet de déterminer la base dans laquelle il apparaît.

En outre, et dans un mode de réalisation préférentiel non limitatif, on indique que pour une procédure d'enregistrement optimisée et dans le cas d'un nœud SIP de type IP double pile, le processus peut consister en outre, ainsi que représenté en figure 3b, à transmettre en une étape D' une requête d'enregistrement de type IP correspondant au type IP du serveur proxy et à transmettre une requête d'enregistrement de type IP distinct du type IP du serveur proxy.

Cette opération à l'étape D' de la figure 3b est notée par la relation :

$$A_{DS} \xrightarrow{RR_1((R@vx),\ RR_2(R@vy))} R.$$

Dans la relation précédente, on comprend que $RR_1(R@vx)$ désigne la requête d'enregistrement de type IP correspondant au type IP du serveur proxy par exemple et que $RR_2(R@vy)$ désigne une requête d'enregistrement de type IP distinct du type IP du serveur proxy par exemple.

Les types IP des deux requêtes peuvent bien entendu être intervertis.

L'étape D' est alors suivie d'une étape E' consistant à discriminer le type IP du nœud SIP à partir de chacune des deux requêtes d'enregistrement émises précitée.

A l'étape E' présentée en figure 3b, la discrimination des types vx et vy, est représentée par la relation symbolique :

$vx=v4$ si $R@vx=R_1@v4$,

$vy=v6$ si $R@vy \equiv R_2@v4$.

De même que dans le cas de la figure 3a, le signe Ξ représente l'identité des adresses après traduction, par le nœud intermédiaire IN.

Dans les relations précédentes, l'identité de l'adresse d'appel du serveur d'enregistrement et de l'adresse auxiliaire du serveur

d'enregistrement s'entend de l'identité après transformation de l'adresse de communication formant l'adresse d'appel.

L'étape E' est alors suivie d'une étape F' consistant à établir et maintenir conjointement la première et la deuxième bases de données d'enregistrement $DB_1(v4)$ et $DB_2(v6)$ pour le nœud SIP de type double pile, à partir des deux types IP discriminés.

On comprend ainsi que, par la mise en œuvre du processus d'enregistrement selon l'invention représentée en figure 3b et pour un nœud SIP double pile, ce dernier est alors présent dans les deux bases de données d'enregistrement.

En outre, on indique que tout nœud SIP de type IPv6, est représenté dans l'environnement IPv4 par une adresse IPv4 pour laquelle une correspondance est réalisée avec l'adresse IPv6 du nœud SIP de type IPv6 dans son environnement IP d'origine. La requête d'enregistrement d'un nœud SIP de type IPv6 arrive donc sur l'adresse auxiliaire $R_2@v4$ du serveur d'enregistrement R et l'adresse IPv4 représentant le nœud SIP de type IPv6 dans l'environnement IPv4 est alors disponible pour l'opération d'enregistrement puisque fournie par les fonctions d'adaptation mises en œuvre par ailleurs par l'opérateur du réseau IPv4.

De ce fait, les bases d'enregistrement maintenues par le serveur d'enregistrement R peuvent alors ne contenir que des adresses IPv4 ce qui bien entendu assure une cohérence totale du service de transmission réseau.

Un procédé de communication entre au moins un serveur S opérant dans un environnement de type IP déterminé, pris à titre d'exemple non limitatif comme le type IPv4, et au moins un nœud A du réseau, ce nœud A pouvant être de même type IP, IPv4, ou de type IP distinct, IPv6, que le type IP déterminé, IPv4, du serveur S sera maintenant décrit en liaison avec la figure 4a.

En référence à la figure 4a précitée, on alloue, à l'étape G, au moins deux adresses au serveur S, dans l'environnement de type IP déterminé IPv4. Ces adresses comprennent une adresse d'origine, notée

S_1@v4 et une adresse auxiliaire, notée S_2@v4. A cette adresse auxiliaire est associée par traduction une adresse de communication dans un environnement de type IP, IPv6, distinct du type IP déterminé, IPv4. L'adresse de communication à l'étape G est notée S_2@v6.

On fournit ensuite au nœud A, comme adresse d'appel du serveur S, soit l'adresse d'origine, S_1@v4, si le nœud A est du même type IP déterminé, IPv4, soit l'adresse de communication, S_2@v6, si le nœud A est de type IP, IPv6, distinct du type IP déterminé, IPv4.

L'opération correspondante est représentée en figure 4a, pour un nœud A d'adresse A@vx a priori de l'un ou l'autre type IP, IPv4 ou IPv6, par un test H de vérification du type IP de l'adresse du nœud A, par la comparaison :

$$Vx = V4 \ ?$$

Sur réponse positive au test H, on fournit à l'étape I l'adresse d'origine S_1@v4 comme adresse d'appel du serveur S au nœud A, selon la relation :

$$\begin{matrix} A \leftarrow S_1@v4 \\ A@vx \end{matrix}$$

Sinon, sur réponse négative au test H, on fournit à l'étape J l'adresse de communication, S_2@v6, distinct du type IP déterminé, IPv4.

Sur appel à l'étape K du serveur S par le nœud A, par transmission d'une requête d'appel représentée par la relation

$$A \xrightarrow{CR(S_y@v4)} S,$$

où CR(Sy@v4) désigne la requête d'appel, Sy@v4 désigne soit l'adresse d'origine S_1@v4, soit l'adresse de communication S_2@v6 qui est traduite en cours de route par IN en adresse auxiliaire S_2@v4 du serveur S, on procède à la discrimination, à l'étape L, du type IP du nœud A, en fonction de l'adresse d'origine S_1@v4 ou auxiliaire S_2@v4 du serveur sur laquelle ce appel a été reçu.

Sur la figure 4a, l'étape de test L est représentée par la relation :

$$S_y@v4 = S_1@v4.$$

Sur réponse positive au test L, le nœud A est discriminé, à l'étape

M, comme appartenant au type IP déterminé IPv4, A | A@vx = A@v4. Sinon, sur réponse négative au test L, le nœud A est discriminé à l'étape N comme appartenant au type IP distinct, IPv6, du type IP déterminé A | A@vx = A'@v4 qui est la traduction de A@v6 par IN, car S_y@v4 = S_2@v4 lorsque l'appel est reçu par P.

Lorsque le serveur S est un serveur d'enregistrement, le procédé de communication comprend également une étape d'enregistrement, ainsi que décrit en liaison avec les figures 3a et 3b.

Une description plus détaillée d'un procédé de transmission d'appel d'un nœud SIP appelé par un nœud SIP appelant est maintenant donnée en liaison avec la figure 4b.

En référence à la figure 4b précitée, on indique que le nœud SIP appelant, tel que le nœud A, est d'un type IP déterminé, l'adresse de ce nœud étant désignée A@vx et le nœud SIP appelé B est un nœud SIP de type IP également déterminé, identique ou distinct du type du nœud SIP appelant. L'adresse du nœud SIP appelé est notée B@vy.

La transmission de l'appel est effectuée par l'intermédiaire d'un serveur proxy SIP noté P opérant dans un environnement IP de même type IP ou de type IP distinct du type IP du nœud SIP appelant.

A titre d'exemple, on considère le serveur proxy SIP P lequel comporte alors une adresse d'origine P_1@v4 et une adresse auxiliaire P_2@v4 de type IP correspondant à cet environnement IP et allouées conformément au procédé d'adressage objet de l'invention, tel que décrit précédemment dans la description en liaison avec les figures 2a et 2b.

En outre, on considère que le nœud SIP appelant A et le nœud SIP appelé B ont satisfait au processus d'enregistrement auprès du serveur R lequel dispose lui-même de son adresse d'origine R_1@v4 et de son adresse auxiliaire R_2@v4 ainsi que décrit précédemment dans la description, en liaison avec les figures 3a et 3b.

Le procédé de transmission d'appel objet de l'invention comprend au moins, ainsi que représenté sur la figure 4b, suite à la transmission à l'étape T d'une requête d'appel du nœud SIP appelant au serveur proxy SIP,

Juniper Exhibit 1002, page 346

cette requête d'appel étant notée :

$$CR(P@v4, B@vy),$$

la discrimination, au niveau du serveur proxy SIP, du type du nœud SIP appelant à partir de l'adresse d'appel d'origine respectivement de l'adresse de communication correspondant à l'adresse auxiliaire allouée au serveur proxy SIP.

On comprend, en particulier, qu'à l'étape U la discrimination peut être directement effectuée par le serveur proxy SIP P sur la base de l'appel dans la requête d'appel, soit de l'adresse d'origine du serveur proxy SIP, auquel cas le nœud SIP appelant A correspond à un nœud de type IP identique à celui du proxy SIP P, ou au contraire, à un nœud SIP de type IP distinct de celui du serveur proxy SIP P, lorsque l'adresse d'appel de ce dernier correspond, après traduction, à l'adresse auxiliaire $P_2@v4$.

L'étape U peut alors être suivie d'une étape W consistant à discriminer au niveau du serveur d'enregistrement R, le type IP du nœud SIP appelé à partir des bases d'enregistrement $DB_1(v4)$ et $DB_2(v6)$. Cette opération est exécutée par un appel V du serveur d'enregistrement R par le serveur proxy SIP P ainsi qu'il sera décrit ultérieurement dans la description.

A l'étape W de la figure 4b, l'opération de discrimination de type du terminal appelé est donnée par la relation symbolique :

$$vy=v4 \text{ si } B@vy \in DB_1(v4),$$

$$vy=v6 \text{ si } B@vy \in DB_2(v6).$$

L'étape W précitée est alors suivie d'une étape X de transmission du serveur d'enregistrement au serveur proxy SIP du type IP discriminé pour le terminal appelé B et de l'adresse de communication du nœud SIP appelé pour qualification et routage de la requête d'appel à l'étape Y représentée en figure 4b.

A l'étape X de transmission, l'opération de transmission est représentée par un message de service selon la relation :

$$R \xrightarrow{SM(vy,\, B@vx)} P.$$

Enfin, l'opération de routage à l'étape Y est représentée par la relation :

$$P \xrightarrow{CR(P@v4,\ B@vy,\ A@vx,\ ALG(SDP))} B.$$

Le mode opératoire de la transmission d'appel selon le procédé objet de l'invention tel que représenté en figure 4b, peut alors être explicité de la manière ci-après.

Lors de l'établissement d'un appel, le procédé objet de l'invention permet à tout serveur proxy SIP de déterminer, simplement dans le contexte de l'appel, notamment le type IP du nœud SIP appelant respectivement appelé afin d'optimiser les choix de routage et notamment le recours aux fonctions d'adaptation précitées.

A l'étape U, le serveur proxy SIP détermine le type IP du nœud SIP appelant A. Dans ce but, il s'appuie sur la connaissance des adresses utilisées par les nœuds SIP pour le contacter.

En effet, par configuration, tous les nœuds SIP de type IPv4 contactent le serveur proxy SIP P sur son adresse d'origine exclusivement. Par ailleurs, les nœuds SIP de type IP distincts, soit de type IPv6 dans l'exemple donné, contactent le serveur proxy précité sur son adresse de communication P_2@v6. Cette dernière adresse correspond ainsi que décrit précédemment à l'adresse auxiliaire P_2@v4 du serveur proxy P considéré puisqu'une correspondance est assurée entre ces deux adresses par le service mis en œuvre par ailleurs par l'opérateur du réseau IP.

Le serveur proxy SIP P considéré reçoit donc toute requête émise par un nœud SIP de type distinct du type IP de ce serveur SIP exclusivement sur son adresse auxiliaire. Le serveur proxy SIP P peut donc déduire qu'un nœud SIP est de type double pile lorsque ce nœud SIP a été référencé dans chacune des bases de données d'enregistrement précédemment décrites.

De plus, tout nœud SIP double pile utilise l'attribut « ANAT » pour renseigner ces deux adresses.

A l'étape W, le serveur d'enregistrement R détermine le type IP du nœud SIP appelé P.

Lors d'un traitement classique d'un appel SIP, le serveur proxy intermédiaire contacte le serveur d'enregistrement pour que ce dernier

Juniper Exhibit 1002, page 348

fournisse l'adresse avec laquelle le nœud SIP appelé B s'est au préalable enregistré. Le serveur d'enregistrement R retourne au serveur proxy SIP P l'adresse requise après avoir consulté sa base d'enregistrement.

Au contraire, le procédé objet de l'invention introduit un élément supplémentaire dans ces échanges. En effet, le serveur proxy SIP P requiert en plus le type IP du nœud SIP appelé à l'étape V. Pour répondre, le serveur d'enregistrement R s'appuie sur ses bases de données d'enregistrement, puisque le type IP de la référence du nœud SIP enregistré est le critère d'enregistrement dans la base de données d'enregistrement en laquelle, ce dernier a été enregistré.

Lorsque cette information a été déterminée, le serveur d'enregistrement R transmet cette dernière à l'étape X, typiquement en même temps que la fourniture de l'adresse du nœud SIP appelé B.

Lorsque cette opération a été exécutée, c'est-à-dire après l'étape W de la figure 4b, le serveur proxy SIP P dispose donc des éléments nécessaires pour qualifier l'appel, ce qui à l'étape Y permet à ce dernier de router l'appel de façon optimale.

En particulier, pour un nœud SIP appelant et un nœud SIP appelé de type IP distinct, le serveur proxy SIP route l'appel par l'intermédiaire de fonctions d'adaptation ALG permettant de modifier le contenu du champ SDP de la requête d'appel et d'y intégrer des informations destinées au nœud SIP appelé.

Ainsi, en référence aux figures 4a et 4b, lorsque le serveur S est un serveur proxy P et lorsque l'appel du serveur proxy P par le nœud A met en œuvre une transmission T au serveur proxy d'une requête d'appel CR(P@v4, B@vy) du nœud appelant A vers le nœud appelé B, le procédé de communication objet de l'invention peut comprendre en outre au moins l'étape V de transmission, du serveur proxy P vers le serveur d'enregistrement R, d'une requête de type IP du nœud appelé B selon la relation :

$$P \xrightarrow{TYPR(B@vy)} R,$$

suite à l'étape U de discrimination du type IP du nœud appelé par le serveur

d'enregistrement R, puis l'étape X de transmission, du serveur d'enregistrement R vers le serveur proxy P, du type IP, vy, du nœud appelé B, enregistré dans la base de données et d'une adresse B@vy du nœud appelé. L'étape X est suivie de l'étape de routage Y de l'appel du nœud appelant A vers le nœud appelé B, en fonction du type IP, vx, du nœud appelant discriminé par le serveur proxy P à l'étape U et du type IP, vy, du nœud appelé B transmis par le serveur d'enregistrement R à l'étape X.

En variante, ainsi que représenté en figure 4c, les étapes U et V de la figure 4b sont remplacées par une étape U' de transmission par le proxy P d'une requête de type du nœud appelant A et du nœud appelé B notée :

$$P \xrightarrow{TYPR(A@vx,\ B@vy)} R.$$

Les étapes U et V de la figure 4b sont supprimées. L'étape U' est suivie d'une W' de discrimination des types IP, vx, vy du terminal appelant A@vx et du terminal appelé B@vy par le serveur d'enregistrement R selon la relation :

$$vx/y = v4 \text{ si } A/B@vx/y \in DB_1(v4)$$
$$vx/y = v6 \text{ si } A/B@vx/y \in DB_2(v6).$$

L'étape W' est suivie d'une étape X' de transmission du serveur d'enregistrement R au serveur proxy P d'un message de service comportant les types IP respectifs vx, vy du terminal appelant A et du terminal appelé B, accompagnés de l'adresse de communication du terminal appelé B@vx selon la relation :

$$R \xrightarrow{SM(vx,vy,B@vx)} P.$$

L'étape X' est suivie de l'étape Y de routage décrite en liaison avec la figure 4b. Dans la variante de mise en œuvre de la figure 4c, le type du nœud appelant A et du nœud appelé B est déterminé par le serveur d'enregistrement R, sur requête du proxy P.

Une représentation des différents cas de transmission d'appel est maintenant décrite en liaison avec les figures 5a à 5c.

Figure 5a : cas où les nœuds SIP appelant et appelé sont de même type IP, ou l'un des deux est de type double pile.

Dans cette situation, le serveur proxy SIP P n'a pas recours aux fonctions d'adaptation ALG, puisque les informations contenues dans le champ SDP de la requête d'appel vont être pertinentes pour les deux nœuds SIP considérés appelant et appelé.

La figure 5a illustre le cas de l'appel entre deux nœuds SIP de même type IPv4 entre le nœud SIP A et l'agent utilisateur UA de même type d'un nœud SIP C.

Les messages SIP successifs sont les suivants :

- 1) transmission de la requête d'appel du nœud SIP A au serveur proxy SIP P ;
- 2) transmission d'un message de service entre le serveur proxy SIP P et le serveur d'enregistrement R pour interrogation des types selon les étapes U et V ;
- 3) transmission d'un message de service entre le serveur d'enregistrement R et le serveur proxy SIP P selon l'étape W ;
- 4) transmission d'un message « INVITE » par le serveur proxy SIP vers l'agent utilisateur UA du nœud SIP C, puis échange des flux RTP.

Figure 5b : transmission d'un appel entre nœuds SIP de même type IPv6.

Dans cette situation, la mise en œuvre des fonctions d'adaptation ALG n'est également pas requise. En effet, les informations IPv6 contenues dans le champ SDP des messages SIP sont pertinentes pour les deux nœuds SIP qui sont de même type SIP IPv6.

Ne pas router l'appel vers des fonctions d'adaptation mettant typiquement en œuvre une application ALG permet en outre de maintenir l'établissement des flux RTP au sein de l'environnement IPv6, sans passer par un nœud intermédiaire. Toutefois, les éléments de service et en particulier ceux représentés au nœud intermédiaire IN, sont en principe situés en environnement IP IPv4. En conséquence, la signalisation de l'appel traverse une simple fonction relais du point de vue du transport entre l'environnement IPv4 et l'environnement IPv6.

L'échange des messages SIP successifs 1 à 4 est représenté au

dessin de la figure 5b.

Figure 5c : cas d'un appel entre clients hétérogènes de type IP distinct.

Dans le cas où les nœuds SIP appelant et appelé A et B représentés en figure 5c sont de type IP distinct, le proxy IP route l'appel vers les fonctions d'adaptation, lesquelles mettent typiquement en œuvre une application ALG SIP. De telles applications permettent, entre autre, de modifier le contenu du champ SDP des messages pour y intégrer des éléments d'informations pertinents pour le nœud SIP destinataire du message.

L'échange des messages SIP successifs 1 à 4 est également représenté en figure 5c dans cette situation.

Le procédé et le protocole utilisés pour les échanges entre serveur proxy SIP et serveur d'enregistrement conformes à l'objet de l'invention, dépendent de l'implémentation. En particulier, de nombreuses implémentations ont la particularité de faire résider le serveur d'enregistrement R et le proxy SIP au sein de la même entité physique, ce qui permet d'alléger la réalisation globale de la fonction supplémentaire de détermination des types IP du terminal appelant et du terminal appelé, conformément à l'objet de la présente invention.

Une description plus détaillée d'un serveur SIP d'enregistrement opérant dans un environnement IP de type IP déterminé, en présence d'un autre environnement IP de type IP distinct, conforme à l'objet de l'invention, sera maintenant donnée en liaison avec la figure 6a.

De manière classique, un tel serveur comporte des organes d'entrée – sortie, notés I/O, reliés à une unité centrale de traitement CPU et à une mémoire de travail RAM.

Il est remarquable en ce qu'il comporte, en outre, une adresse IP d'origine notée R_1@v4 sur la figure 6a et une adresse auxiliaire de type IP correspondant à cet environnement IP et notée R_2@v4. Ces deux adresses peuvent avantageusement être mémorisées dans une mémoire programmable par exemple.

En outre, ainsi que représenté en figure 6a, le serveur d'enregistrement objet de l'invention comprend un module M_0 de discrimination de type IP de tout nœud SIP candidat à un enregistrement, en fonction de l'adresse d'appel d'origine respectivement de l'adresse de communication correspondant à l'adresse auxiliaire précitée, utilisée par le nœud SIP dans une requête d'enregistrement auprès de ce serveur d'enregistrement.

Enfin, ainsi que représenté en outre sur la figure 6a, le serveur SIP d'enregistrement objet de l'invention comprend des ressources de première et deuxième bases de données d'enregistrement $DB_1(v4)$ et $DB_2(v6)$, de chaque nœud SIP candidat à l'enregistrement correspondant à un nœud SIP d'un même type IP que le type IP du serveur proxy dont l'adresse d'appel est l'adresse d'origine de ce dernier $R_1@v4$, respectivement de type IP distinct du type IP du serveur SIP d'enregistrement, dont l'adresse d'appel est l'adresse auxiliaire de ce serveur SIP d'enregistrement, adresse $R_2@v4$, par l'intermédiaire de l'adresse de communication.

En outre, et selon une caractéristique remarquable du serveur SIP d'enregistrement objet de l'invention, on indique que pour tout nœud SIP de type IP double pile, la première base de données d'enregistrement $DB_1(v4)$ comprend une référence à l'adresse IP du nœud SIP de type IP correspondant au type IP du serveur proxy de type IP et la deuxième base de données d'enregistrement $DB_2(v6)$ comprend une référence à l'adresse IP du nœud SIP de type IP distinct du type IP du serveur proxy de type IP.

La figure 6b représente un serveur proxy SIP conforme à l'objet de la présente invention et opérant en transmission d'une requête d'appel d'un nœud SIP appelé par un nœud SIP appelant.

Il comporte des organes d'entrée – sortie I/O reliés à une unité centrale de traitement CPU et à une mémoire de travail RAM.

Il est en outre remarquable en ce qu'il inclut une adresse IP d'origine $P_1@v4$ correspondant à l'environnement IP de type IP déterminé, dans lequel est implanté le serveur proxy, et une adresse auxiliaire de même

type IP que le type IP de l'adresse d'origine, adresse notée P_2@v4. Ces adresses peuvent être mémorisées dans une mémoire programmable.

Il comprend enfin un module M_1 de discrimination, à partir de la requête d'appel, du type IP de tout nœud SIP appelant à partir de l'adresse d'appel d'origine respectivement de communication correspondant à l'adresse auxiliaire du serveur proxy SIP, ainsi que décrit précédemment dans la description.

Il comporte, en outre, un module M_2 de discrimination par interrogation d'un serveur SIP d'enregistrement du type IP du nœud SIP appelé ainsi que décrit précédemment dans la description.

Il comprend enfin un module M_3 de transmission et de routage de la requête d'appel compte tenu du type IP et de l'adresse de communication du nœud SIP appelé.

En particulier, lorsque le nœud SIP appelant et le nœud SIP appelé sont de type IP distinct, le module M_3 précité exécute le routage de la requête d'appel par l'intermédiaire de fonctions d'adaptations permettant de modifier le contenu du champ SDP de la requête d'appel et d'y intégrer des informations destinées au nœud SIP appelé.

L'invention couvre également un programme d'ordinateur comportant une suite d'instructions mémorisées sur un support de mémorisation et exécutables par un ordinateur ou un dispositif dédié, tel qu'un serveur SIP d'enregistrement. Le serveur SIP d'enregistrement opère l'enregistrement d'un nœud SIP de type IP déterminé dans un environnement IP de même type ou d'un autre type IP.

Ce serveur SIP d'enregistrement comporte une adresse d'origine et une adresse auxiliaire de type IP et une adresse auxiliaire de type IP correspondant à l'environnement IP, cette adresse auxiliaire étant allouée ainsi que décrit précédemment dans la description en liaison avec les figures 2a et 2b. Il est remarquable en ce que lors de son exécution, ce programme exécute le processus d'enregistrement d'un nœud SIP ainsi que décrit précédemment dans la description en liaison avec les figures 3a et 3b. Ce programme d'ordinateur peut consister en un module logiciel, tel que le

module M_0 décrit précédemment en liaison avec la figure 6a.

L'invention couvre enfin un programme d'ordinateur comportant une suite d'instructions mémorisées sur un support de mémorisation et exécutables par un ordinateur ou un dispositif dédié, tel qu'un serveur proxy SIP, opérant en transmission d'une requête d'appel d'un nœud SIP appelé par un nœud SIP appelant de type IP déterminé identique ou distinct.

Le serveur proxy SIP comporte une adresse d'origine et une adresse auxiliaire de type IP correspondant à l'environnement IP et allouées conformément au procédé d'adressage tel que décrit précédemment dans la description en liaison avec les figures 2a et 2b. Les nœuds SIP appelant et appelé ont satisfait au processus d'enregistrement de nœuds SIP, tel que décrit précédemment dans la description en liaison avec les figures 3a et 3b.

Il est remarquable en ce que, lors de son exécution ce programme exécute le procédé de transmission d'appel ainsi que décrit précédemment dans la description en liaison avec la figure 4b. Ce programme peut être mis en œuvre sous forme de modules logiciels distincts tels que les modules M_1 à M_3 décrits en liaison avec la figure 6b.

REVENDICATIONS

1. Procédé d'adressage de serveurs pour l'inter-fonctionnement de nœuds d'un premier respectivement d'un deuxième type IP, caractérisé en ce qu'il inclut au moins :

- l'allocation à tout serveur, opérant dans un environnement IP de l'un ou l'autre type IP et muni d'une adresse d'origine d'un type IP déterminé, d'une adresse auxiliaire de même type IP que le type IP de l'adresse d'origine, à ladite adresse auxiliaire correspondant une adresse de communication de type IP distinct de ce type IP déterminé ;
- la fourniture, comme adresse d'appel, à tout nœud du même type IP que ledit serveur, de ladite adresse d'origine et à tout nœud hétérogène, de type IP autre que le type IP dudit serveur, de ladite adresse de communication ;
- la traduction de ladite adresse de communication de l'un ou l'autre type IP en ladite adresse auxiliaire, de même type IP que le type IP de l'adresse d'origine.

2. Procédé selon la revendication 1, caractérisé en ce que ladite adresse de communication est configurée comme entrée DNS de l'environnement IP de type IP distinct de celui dudit serveur.

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que lesdits serveurs incluent tout serveur d'enregistrement respectivement tout serveur proxy de l'un ou l'autre des environnements IP.

4. Procédé de communication entre au moins un serveur opérant dans un environnement de type IP déterminé et au moins un nœud d'un réseau, ledit nœud étant de même type IP ou de type IP distinct dudit type IP déterminé, caractérisé en ce qu'il comprend les étapes suivantes :

- allocation audit serveur d'au moins deux adresses dans ledit environnement de type IP déterminé, comprenant une adresse dite d'origine et une adresse dite auxiliaire, à laquelle est associée par

traduction une adresse de communication dans un environnement de type IP distinct du type IP déterminé ;

- fourniture audit nœud, comme adresse d'appel dudit serveur :
  - de ladite adresse d'origine si ledit nœud est de même type IP que ledit type IP déterminé ;
  - de ladite adresse de communication si ledit nœud est de type IP distinct dudit type IP déterminé ;
- sur appel dudit serveur par ledit nœud, discrimination du type IP dudit nœud en fonction de l'adresse d'origine ou auxiliaire dudit serveur sur laquelle est reçu ledit appel.

5. Procédé de communication selon la revendication 4, caractérisé en ce que, ledit serveur étant un serveur d'enregistrement, le procédé comprend également une étape d'enregistrement dudit nœud en fonction dudit type IP discriminé dans au moins une base de données.

6. Procédé de communication selon la revendication 4, caractérisé en ce que ledit serveur d'enregistrement maintient au moins deux bases de données comprenant respectivement lesdits nœuds de même type IP que ledit type IP déterminé et lesdits nœuds de type IP distinct dudit type IP déterminé.

7. Procédé de communication selon l'une quelconque des revendications 5 et 6, caractérisé en ce que ledit nœud présentant au moins deux types IP, à savoir ledit type IP déterminé et au moins un type IP distinct dudit type IP déterminé, ledit procédé comprend :

- une étape de transmission par ledit nœud d'une requête d'enregistrement vers ladite adresse d'origine dudit serveur d'enregistrement ;
- une étape de transmission par ledit nœud d'au moins une requête d'enregistrement vers ladite adresse de communication dudit serveur, destinée à être reçue après traduction sur ladite adresse auxiliaire dudit serveur.

8. Procédé de communication selon l'une quelconque des revendications 5 à 7, caractérisé en ce que, ledit serveur étant un serveur proxy, et ledit appel dudit serveur proxy par ledit nœud mettant en œuvre

Juniper Exhibit 1002, page 357

une transmission audit serveur proxy d'une requête d'appel dudit nœud appelant vers un nœud appelé, le procédé comprend également :

- une première étape de transmission dudit serveur proxy vers ledit serveur d'enregistrement d'une requête de type IP dudit nœud appelé ;
- une deuxième étape de transmission dudit serveur d'enregistrement vers ledit serveur proxy du type IP dudit nœud appelé enregistré dans ladite base de données et d'une adresse dudit nœud appelé ;
- une étape de routage dudit appel dudit nœud appelant vers ledit nœud appelé, en fonction du type IP dudit nœud appelé transmis par ledit serveur d'enregistrement.

9. Procédé de communication selon la revendication 8, caractérisé en ce que, lors de ladite deuxième étape de transmission, l'adresse dudit nœud appelé transmise par ledit serveur d'enregistrement est une adresse dans ledit environnement de type IP déterminé dans lequel opère ledit serveur proxy.

10. Serveur d'enregistrement opérant dans un environnement de type IP déterminé, dans un réseau comprenant un autre environnement de type IP distinct du type IP déterminé, ledit serveur comportant des organes d'entrée – sortie reliés à une unité centrale de traitement et à une mémoire de travail, caractérisé en ce qu'il comporte au moins deux adresses dans ledit environnement de type IP déterminé, comprenant une adresse dite d'origine et une adresse dite auxiliaire, à laquelle est associée par traduction une adresse de communication dans ledit environnement de type IP distinct, et :

- des moyens de discrimination du type IP d'un nœud candidat à un enregistrement, en fonction de l'adresse d'appel d'origine ou auxiliaire dudit serveur sur laquelle est reçue une requête d'enregistrement transmise à ce serveur d'enregistrement par ledit nœud candidat ;
- des moyens d'enregistrement dudit nœud en fonction dudit type IP discriminé dans au moins une base de données.

11. Serveur d'enregistrement selon la revendication 10, caractérisé en ce qu'il comprend des moyens d'enregistrement dudit nœud

dans au moins une première et une deuxième bases de données comprenant respectivement lesdits nœuds de même type IP que ledit type IP déterminé et lesdits nœuds de type IP distinct dudit type IP déterminé.

12. Serveur d'enregistrement selon la revendication 11, caractérisé en ce que pour un nœud de type IP double pile, ladite première base de données d'enregistrement comprend :

- une référence à l'adresse IP dudit nœud de type IP correspondant au type IP déterminé dudit serveur d'enregistrement ; et, en ce que ladite deuxième base de données d'enregistrement comprend :
- une référence à l'adresse IP dudit nœud de type IP distinct du type IP déterminé dudit serveur d'enregistrement.

13. Serveur proxy opérant dans un environnement de type IP déterminé, dans un réseau comprenant un autre environnement de type IP distinct du type IP déterminé, ledit serveur opérant en transmission d'une requête d'appel d'un nœud appelé par un nœud appelant, de types IP identique ou distinct dudit type IP déterminé, et comportant des organes d'entrée – sortie reliés à une unité centrale de traitement et à une mémoire de travail, caractérisé en ce qu'il comporte au moins deux adresses dans ledit environnement de type IP déterminé, comprenant une adresse dite d'origine et une adresse dite auxiliaire, à laquelle est associée par traduction une adresse de communication dans ledit environnement de type IP distinct et :

- des moyens de discrimination du type IP dudit nœud appelant, en fonction de l'adresse d'appel d'origine ou auxiliaire dudit serveur sur laquelle est reçue ladite requête d'appel ;
- des moyens de discrimination, par interrogation d'un serveur d'enregistrement selon l'une des revendications 10 à 12, du type IP dudit nœud appelé ;
- des moyens de transmission et de routage de ladite requête d'appel, compte tenu du type IP et de l'adresse de communication dudit nœud appelé.

14. Serveur proxy selon la revendication 13, caractérisé en ce

Juniper Exhibit 1002, page 359

que, pour un nœud appelant et un nœud appelé de type IP distinct, ledit serveur proxy exécute le routage de ladite requête d'appel par l'intermédiaire de fonctions d'adaptation permettant de modifier le contenu du champ SDP de ladite requête d'appel et d'y intégrer des informations destinées audit nœud appelé.

15. Programme d'ordinateur comportant une suite d'instructions mémorisées sur un support de mémorisation et exécutable par un ordinateur ou un dispositif dédié tel qu'un serveur d'enregistrement, ledit serveur d'enregistrement opérant l'enregistrement d'un nœud de type IP déterminé dans un environnement IP de même type ou d'un autre type IP, ce serveur d'enregistrement comportant une adresse d'origine et une adresse auxiliaire de type IP correspondant à cet environnement IP allouée conformément au procédé selon les revendications 1 à 3, caractérisé en ce que lors de son exécution ledit programme exécute une étape d'enregistrement d'un nœud en fonction du type IP de ce dernier discriminé dans au moins une base de données.

16. Programme d'ordinateur comportant une suite d'instructions mémorisées sur un support de mémorisation et exécutables par un ordinateur ou un dispositif dédié tel qu'un serveur proxy opérant en transmission d'une requête d'appel d'un nœud appelé par un nœud appelant, de type IP déterminé identique ou distinct, dans un environnement IP de type IP déterminé en présence d'un autre environnement IP de type IP distinct, ce serveur proxy comportant une adresse d'origine et une adresse auxiliaire de type IP correspondant à cet environnement IP allouée conformément au procédé d'adressage selon l'une des revendications 1 à 3, ledit nœud appelant et ledit nœud appelé ayant satisfait à un processus d'enregistrement, caractérisé en ce que lors de son exécution ledit programme exécute le procédé de communication entre au moins un serveur opérant dans un environnement de type IP déterminé et au moins un nœud du réseau selon l'une des revendications 4 à 9.

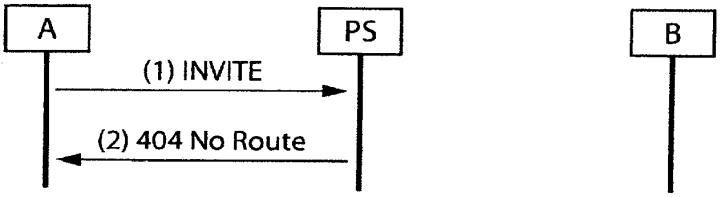

A
PS
B
(1) INVITE
(2) 404 No Route

FIG. 1a

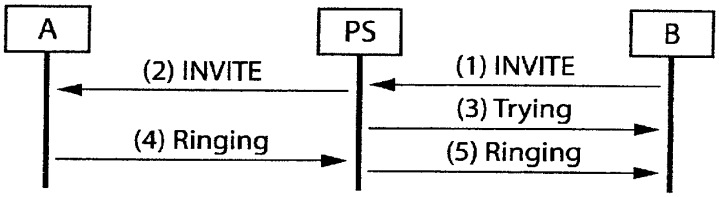

A
PS
B
(2) INVITE
(1) INVITE
(3) Trying
(4) Ringing
(5) Ringing

FIG. 1b

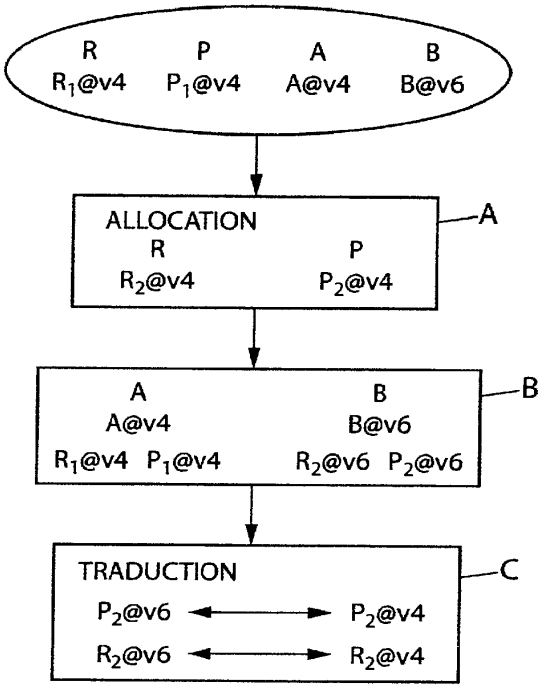

R
R_1@v4
P
P_1@v4
A
A@v4
B
B@v6
ALLOCATION
R
R_2@v4
P
P_2@v4
A
B
A
A@v4
R_1@v4 P_1@v4
B
B@v6
R_2@v6 P_2@v6
TRADUCTION
P_2@v6 ⟷ P_2@v4
R_2@v6 ⟷ R_2@v4
A
B
C

FIG. 2a

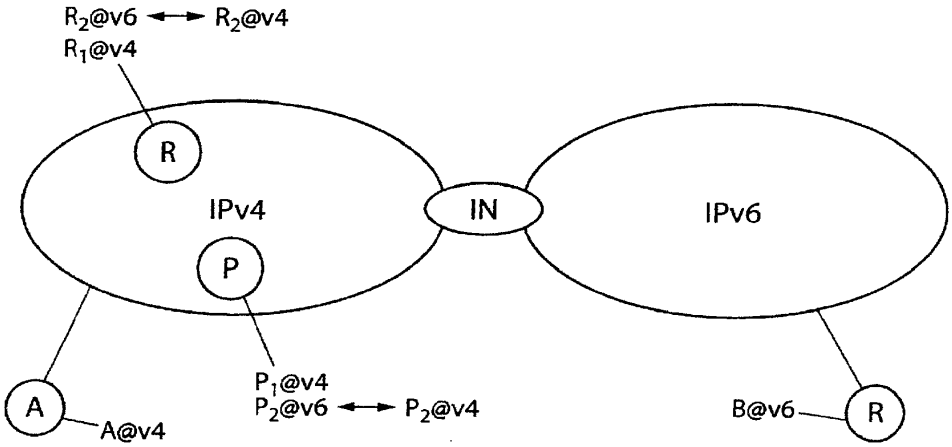

R_2@v6 ⟷ R_2@v4
R_1@v4
R
IPv4
IN
IPv6
P
A
A@v4
P_1@v4
P_2@v6 ⟷ P_2@v4
B@v6
R

FIG. 2b

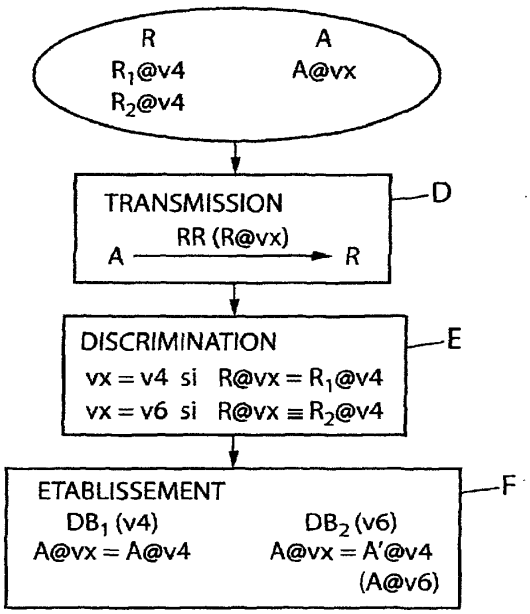


FIG. 3a

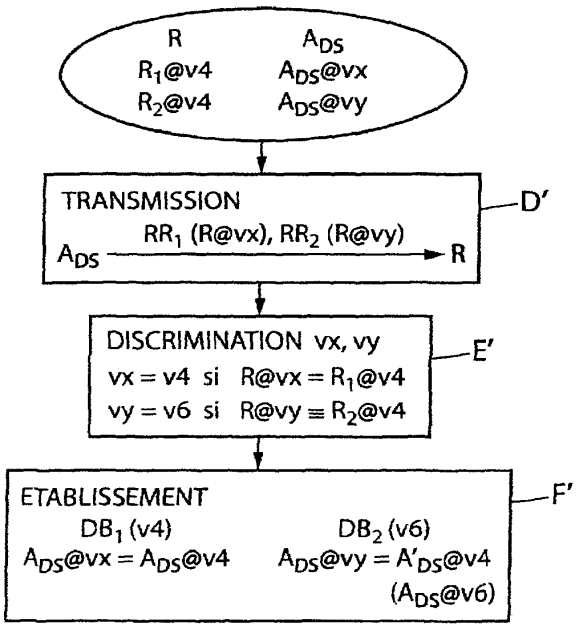


FIG. 3b

Juniper Exhibit 1002, page 363

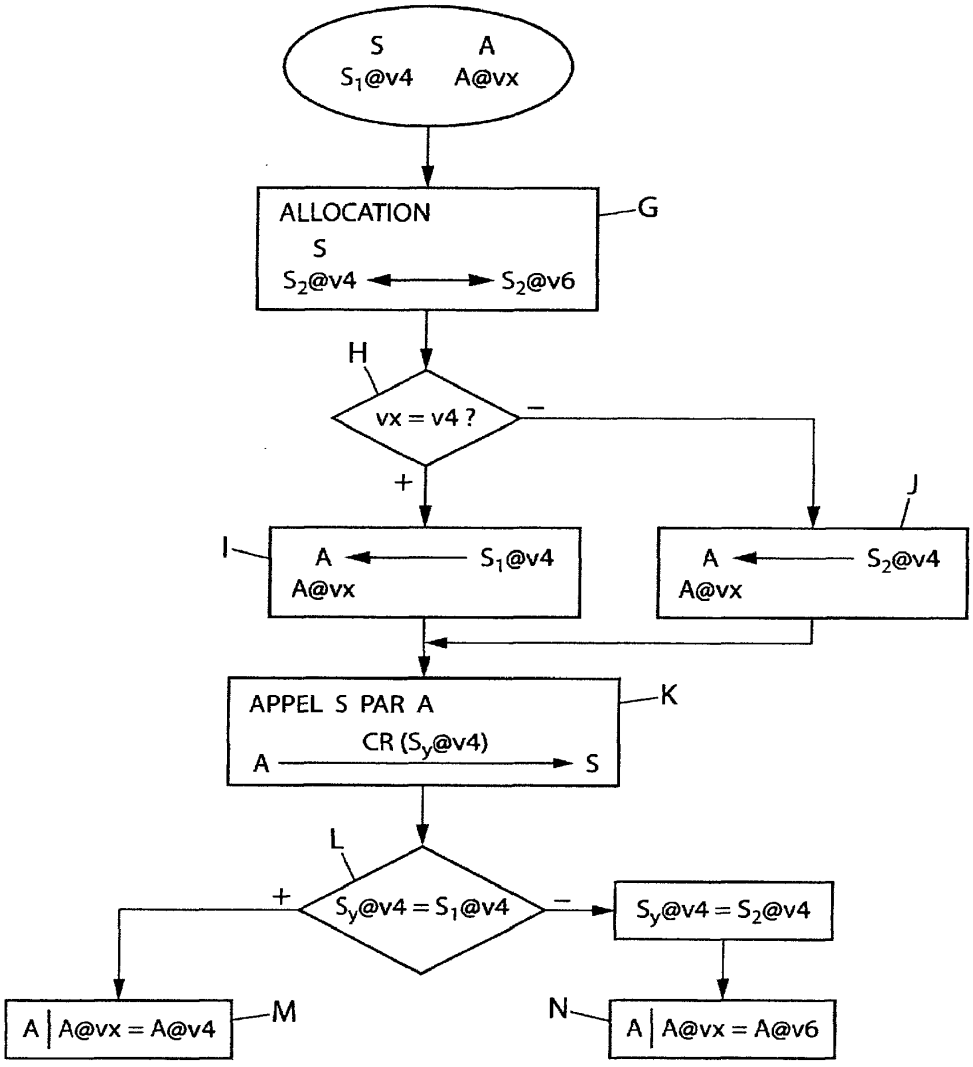

S A
S1@v4 A@vx
ALLOCATION
S
S2@v4 S2@v6
G
H
vx = v4 ?
+
–
I
A S1@v4
A@vx
J
A S2@v4
A@vx
APPEL S PAR A
CR (Sy@v4)
A S
K
L
+
Sy@v4 = S1@v4
–
Sy@v4 = S2@v4
A | A@vx = A@v4
M
N
A | A@vx = A@v6

FIG. 4a

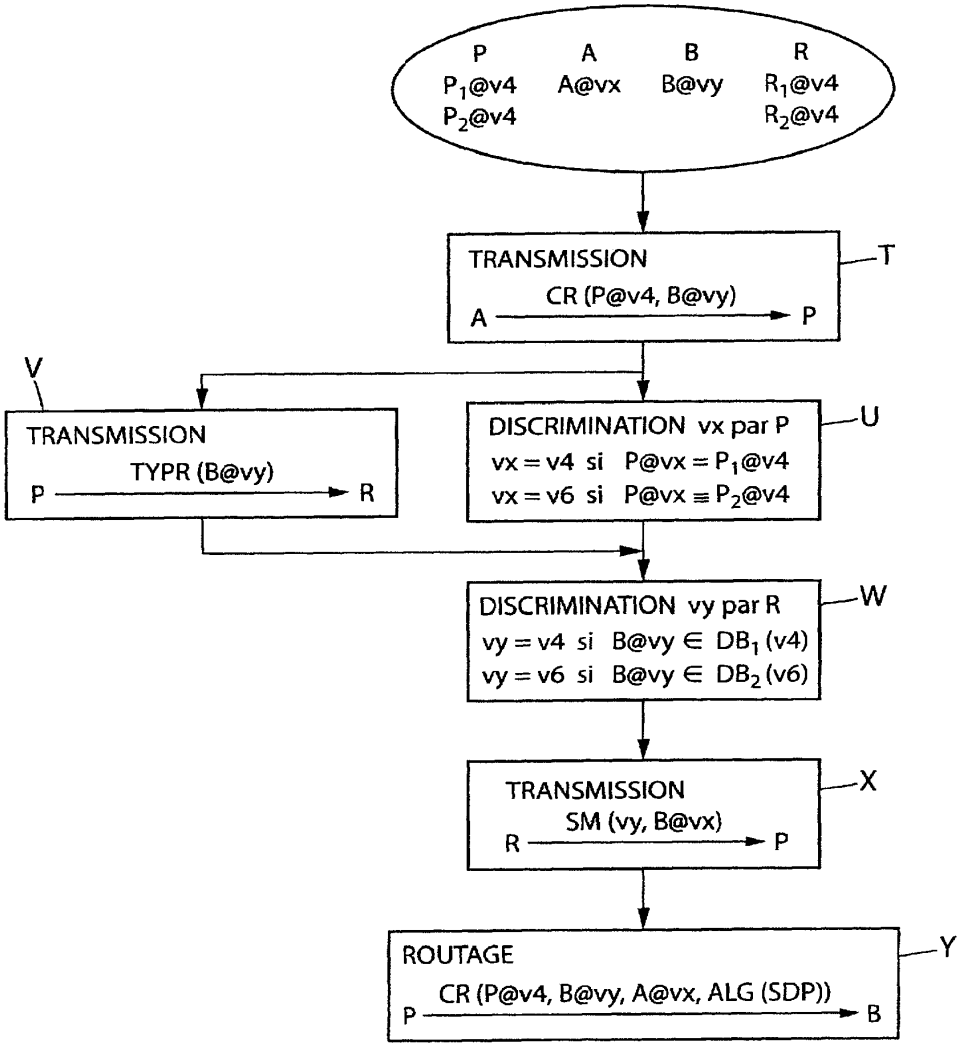

P
A
B
R
P1@v4
P2@v4
A@vx
B@vy
R1@v4
R2@v4
TRANSMISSION
CR (P@v4, B@vy)
A
P
T
V
TRANSMISSION
TYPR (B@vy)
P
R
DISCRIMINATION vx par P
vx = v4 si P@vx = P1@v4
vx = v6 si P@vx = P2@v4
U
DISCRIMINATION vy par R
vy = v4 si B@vy ∈ DB1 (v4)
vy = v6 si B@vy ∈ DB2 (v6)
W
TRANSMISSION
SM (vy, B@vx)
R
P
X
ROUTAGE
CR (P@v4, B@vy, A@vx, ALG (SDP))
P
B
Y

FIG. 4b

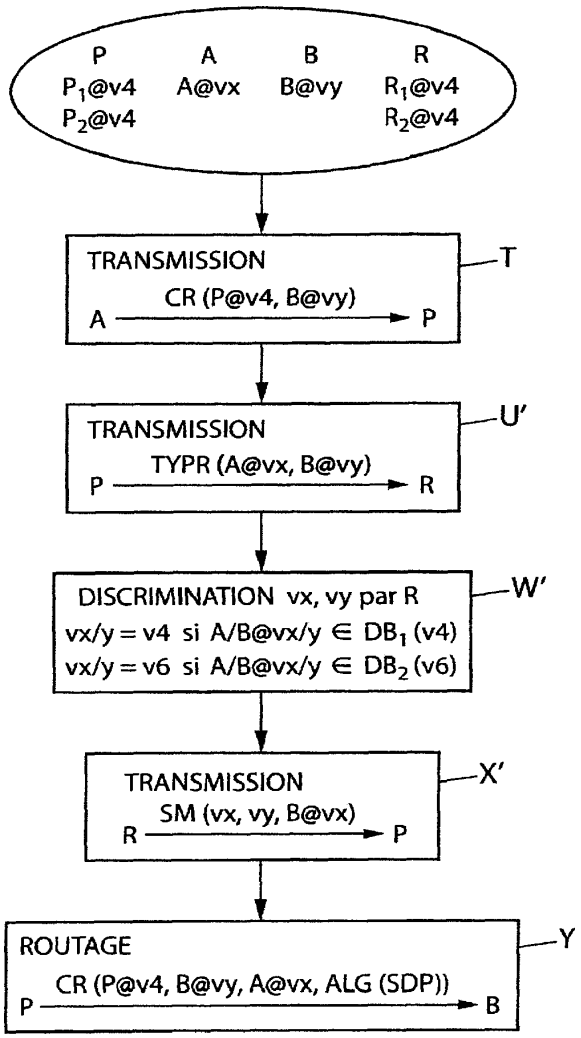

P
A
B
R
P1@v4
A@vx
B@vy
R1@v4
P2@v4
R2@v4
TRANSMISSION
CR (P@v4, B@vy)
A
P
T
TRANSMISSION
TYPR (A@vx, B@vy)
P
R
U'
DISCRIMINATION vx, vy par R
vx/y = v4 si A/B@vx/y ∈ DB1 (v4)
vx/y = v6 si A/B@vx/y ∈ DB2 (v6)
W'
TRANSMISSION
SM (vx, vy, B@vx)
R
P
X'
ROUTAGE
CR (P@v4, B@vy, A@vx, ALG (SDP))
P
B
Y

FIG. 4c

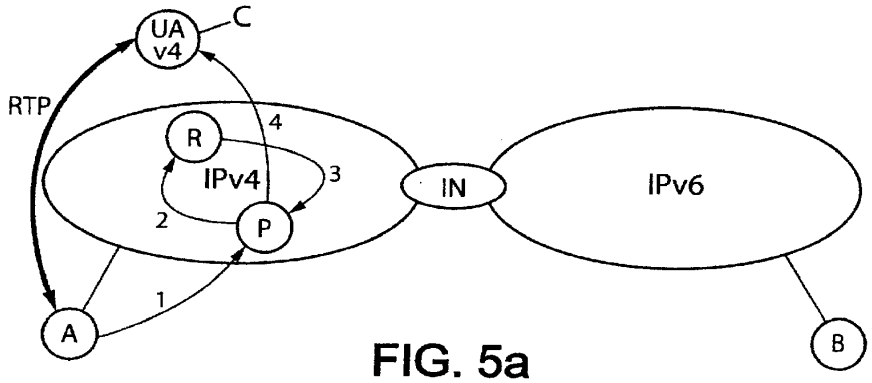


FIG. 5a

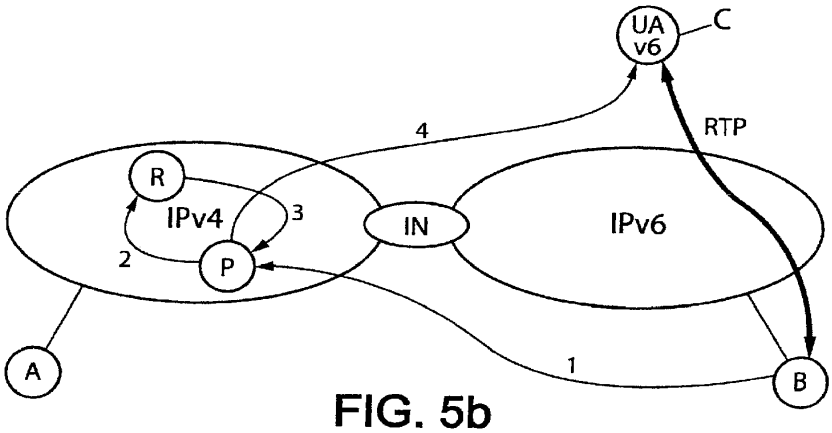


FIG. 5b

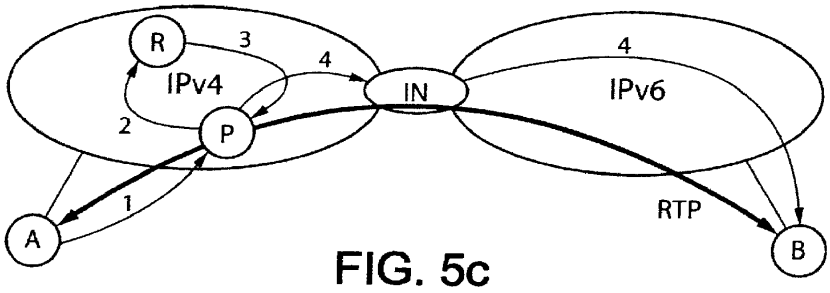


FIG. 5c

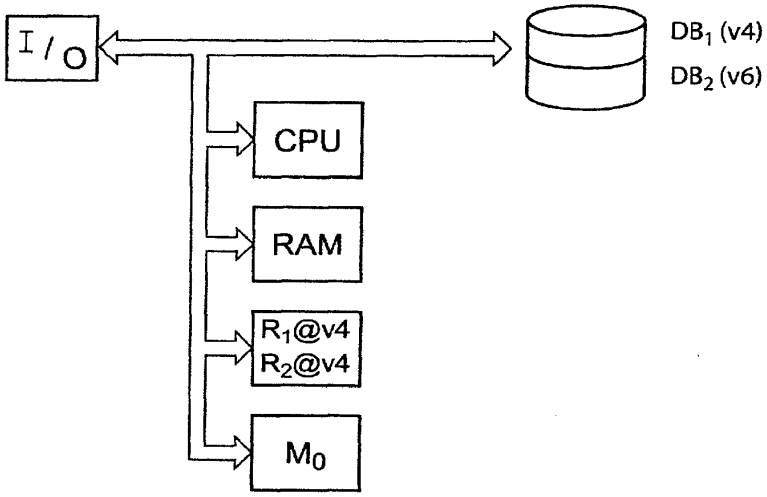

I / O
DB1 (v4)
DB2 (v6)
CPU
RAM
R1@v4
R2@v4
M0

FIG. 6a

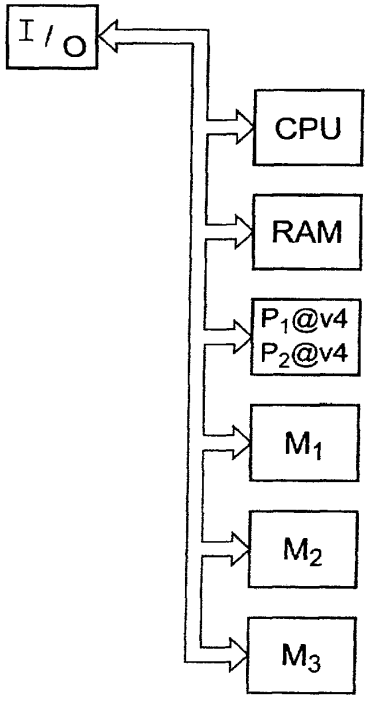

I / O
CPU
RAM
P1@v4
P2@v4
M1
M2
M3

FIG. 6b

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
3 janvier 2008 (03.01.2008)

PCT

(10) Numéro de publication internationale
WO 2008/001007 A3

(51) Classification internationale des brevets :
H04L 29/06 (2006.01) *H04L 29/12* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2007/051531

(22) Date de dépôt international : 26 juin 2007 (26.06.2007)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0605945 30 juin 2006 (30.06.2006) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **BOUCADAIR, Mohamed** [FR/FR]; 124, rue Saint Jean, F-14000 Caen (FR). **NOISETTE, Yoann** [FR/FR]; 2, rue Dom Aubourg, F-14320 May sur Orne (FR).

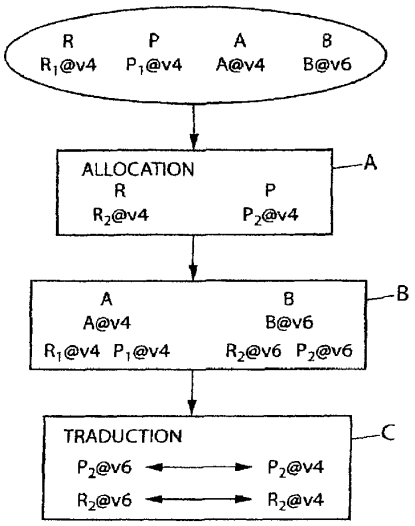
(74) Mandataire : **FRANCE TELECOM/FTR & D/PIV/BREVETS**; Gaëlle WINDAL-VERCASSON, 38-40, rue du Général Leclerc, F-92794 Issy les Moulineaux Cédex (FR).

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

[Suite sur la page suivante]

(54) Title: METHOD FOR ADDRESSING CALL TRANSMISSION AND SERVICE ELEMENTS BETWEEN HETEROGENEOUS NODES

(54) Titre : PROCEDE D'ADRESSAGE DES ELEMENTS DE SERVICE ET DE TRANSMISSION D'APPEL ENTRE NOEUDS HETEROGENES



C... TRANSLATION

(57) Abstract: A SIP server addressing method for the inter-operation of SIP nodes (A, B) of a determined IP type in which each SIP server (P, R) is attributed (A) an auxiliary address (R_2@v4, P_2@v4) of the same IP type as their original address (R_1@v4, P_1@v4), wherein the auxiliary address corresponds to a distinct IP type communication address, all SIP nodes of the same IP type as this SIP server are supplied (B) with the original address, and to all SIP nodes with an IP type distinct from the IP type of this SIP server, this communication address and the communication address of one of the IP types is translated (C) into the auxiliary address, of the same IP type as the IP type of the original address.

(57) Abrégé : Un procédé d'adressage de serveurs SIP pour l'inter-fonctionnement de nœuds SIP (A, B) d'un type IP déterminé dans lequel on alloue (A) à tout serveur SIP (P, R) une adresse auxiliaire (R_2@v4, P_2@v4) de même type IP que leur adresse d'origine (R_1@v4, P_1@v4), l'adresse auxiliaire correspondant à une adresse de communication de type IP distinct, on fournit (B) à tout nœud SIP du même type IP que ce serveur SIP l'adresse d'origine et à tout nœud SIP de type IP distinct du type IP de ce serveur SIP cette adresse de communication et on traduit (C) l'adresse de communication de l'un ou l'autre type IP en l'adresse auxiliaire, de même type IP que le type IP de l'adresse d'origine.

WO 2008/001007 A3

BNSDOCID: <WO_____2008001007A3_I_>

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :
— *relative à la qualité d'inventeur (règle 4.17.iv))*

Publiée :
— *avec rapport de recherche internationale*
— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

(88) Date de publication du rapport de recherche internationale: 13 mars 2008

BNSDOCID: <WO_____2008001007A3_I_>

CI

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2007/051531

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 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)
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, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 1 515 508 A (HITACHI LTD [JP]) 16 March 2005 (2005-03-16) paragraph [0025] - paragraph [0030] paragraph [0042] - paragraph [0056]	1-16
A	US 2006/015647 A1 (KANG SEONG-MIN [KR] ET AL) 19 January 2006 (2006-01-19) paragraph [0049] - paragraph [0068]	1-16

-/--

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

[X] 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 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
2 janvier 2008	09/01/2008

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lebas, Yves

Form PCT/ISA/210 (second sheet) (April 2005)

BNSDOCID: <WO_____2008001007A3_I_>

CI

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2007/051531

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KAWARASAKI Y ET AL: "IPv4/IPv6 SIP interworking methods in dual-stack network" COMMUNICATIONS, 2003. APCC 2003. THE 9TH ASIA-PACIFIC CONFERENCE ON 21-24 SEPT. 2003, PISCATAWAY, NJ, USA,IEEE, vol. 3, 21 September 2003 (2003-09-21), pages 1124-1128, XP010687978 ISBN: 0-7803-8114-9 page 1124, right-hand column, line 1 - page 1127, left-hand column, last line	1-16

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

BNSDOCID: <WO____2008001007A3_I_>

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2007/051531

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1515508 A	16-03-2005	CN 1595933 A	16-03-2005
		JP 2005086467 A	31-03-2005
		US 2005066038 A1	24-03-2005
US 2006015647 A1	19-01-2006	CN 1722729 A	18-01-2006
		KR 20060006440 A	19-01-2006

Form PCT/ISA/210 (patent family annex) (April 2005)

BNSDOCID: <WO_____2008001007A3_I_>

CI

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2007/051531

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. H04L29/06 H04L29/12

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela estréalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, COMPENDEX, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 1 515 508 A (HITACHI LTD [JP]) 16 mars 2005 (2005-03-16) alinéa [0025] - alinéa [0030] alinéa [0042] - alinéa [0056]	1-16
A	US 2006/015647 A1 (KANG SEONG-MIN [KR] ET AL) 19 janvier 2006 (2006-01-19) alinéa [0049] - alinéa [0068]	1-16

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
2 janvier 2008	09/01/2008

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lebas, Yves

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

BNSDOCID: <WO_____2008001007A3_I_>

CI

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2007/051531

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	KAWARASAKI Y ET AL: "IPv4/IPv6 SIP interworking methods in dual-stack network" COMMUNICATIONS, 2003. APCC 2003. THE 9TH ASIA-PACIFIC CONFERENCE ON 21-24 SEPT. 2003, PISCATAWAY, NJ, USA,IEEE, vol. 3, 21 septembre 2003 (2003-09-21), pages 1124-1128, XP010687978 ISBN: 0-7803-8114-9 page 1124, colonne de droite, ligne 1 - page 1127, colonne de gauche, dernière ligne ----	1-16

Formulaire PCT/ISA/210 (suite de la deuxième feuille) (avril 2005)

BNSDOCID: <WO_____2008001007A3_I_>

CI

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2007/051531

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 1515508 A	16-03-2005	CN 1595933 A	16-03-2005
		JP 2005086467 A	31-03-2005
		US 2005066038 A1	24-03-2005
US 2006015647 A1	19-01-2006	CN 1722729 A	18-01-2006
		KR 20060006440 A	19-01-2006

Formulaire PCT/ISA/210 (annexe familles de brevets) (avril 2005)

BNSDOCID: <WO_____2008001007A3_I_>

CI

Electronic Acknowledgement Receipt	
EFS ID:	9499531
Application Number:	13001907
International Application Number:	
Confirmation Number:	5439
Title of Invention:	METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY
First Named Inventor/Applicant Name:	Mohamed Boucadair
Customer Number:	08968
Filer:	Brian Charles Rupp/Irina Mikitiouk
Filer Authorized By:	Brian Charles Rupp
Attorney Docket Number:	P3714US
Receipt Date:	23-FEB-2011
Filing Date:	29-DEC-2010
Time Stamp:	10:08:53
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	P3714US_Communication.pdf	63156 2d4841ab6ceabe66c46c33aaf5f0786dbf654560	no	2
Warnings:					
Information:					

CI

2	Oath or Declaration filed	P3714US_Combined_Declaration_and_Power_of_Attorney.pdf	112961 f8e7bc71534e06b26b98bf8bb20a7b81ec9bd448	no	4
Warnings:					
Information:					
3	Transmittal Letter	P3714US_Information_Disclosure_Statement.pdf	87383 116632e74fc9f01e2fc9975320c898c9d323af5f	no	4
Warnings:					
Information:					
4	Information Disclosure Statement (IDS) Filed (SB/08)	P3714US_1449_Form.pdf	34577 4e523e0753b3948fe279ab3c9c54a99015f5a373	no	1
Warnings:					
Information:					
This is not an USPTO supplied IDS fillable form					
5	Foreign Reference	P3714US_WO2004039014.pdf	1306834 93ee530151e6b2bd2918dfa88873acb336365817	no	35
Warnings:					
Information:					
6	Foreign Reference	P3714US_EP1420559.pdf	469611 2aafee1e3c1ae0ccde4180b319dac63fb48e26b2	no	10
Warnings:					
Information:					
7	Foreign Reference	P3714US_WO20070099248.pdf	1572729 100d79f045b0a18d95f8e3d57a676e6463542bad	no	37
Warnings:					
Information:					
8	Foreign Reference	P3714US_WO2008001007.pdf	2196674 6444b408e9524385bf8e4614ab7d68a437db790c	no	52
Warnings:					
Information:					
9	NPL Documents	P3714US_Afifi.pdf	408477 2fe077b88335a5402f623ce204cbce98564448d7	no	7
Warnings:					
Information:					
10	NPL Documents	P3714US_Kawarasaki.pdf	283285 c7b041938582531 8c10e8ca8d9292a5f640da59b	no	5

Warnings:					
Information:					
11	NPL Documents	P3714US_Park.pdf	922405 1990341d6339b625a2b1a5459e1e8bedfd80bc15	no	21
Warnings:					
Information:					
12	NPL Documents	P3714US_Shin.pdf	300276 07bbd42592e8efc752bf794714425ab687fb6771	no	4
Warnings:					
Information:					
13	NPL Documents	P3714US_Srisuresh.pdf	1400880 c0036f067b3d2ce41dc02520cb7571cdee3f4f8c	no	30
Warnings:					
Information:					
		Total Files Size (in bytes):	9159248		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PATENT
Attorney Docket No. P3714US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Boucadair et al.

Group Art Unit: Unassigned

Application No. 13/001,907
(U.S. National Phase of PCT/FR2009/051228)

Examiner: Unassigned

Filed: December 29, 2010

For: A METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

COMMUNICATION

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Sir:

Applicants hereby submit an executed Combined Declaration and Power of Attorney. A Declaration of Inventorship in accordance with PCT Rule 4.17.iv was submitted in PCT Application No. PCT/FR2009/051228.

The items checked below are appropriate:

1. Status of Applicant

This application is on behalf of ☒ other than a small entity or ☐ a small entity.

2. Documents Submitted Herewith

a. ☒ Executed Combined Declaration and Power of Attorney
b. ☐ Other:

3. Fees

No fees are believed to be due in connection with this submission.

CI

4. Extension of Time

☐ Applicants petition for a extension of time under 37 CFR 1.136, the fee for which is .

☒ Applicants believe that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicants have inadvertently overlooked the need for a petition and fee for extension of time.

Fee Due $0.00

5. Total Fee Due

The total fee due is:

Late Filing of Declaration Surcharge	$ 0.00
Extension of Time Fee	$ 0.00

Total Fee Due: $0.00

6. Fee Payment

☐ Attached is a check in the sum of $.
☐ Charge Account No. 07-0181 the sum of $.

7. Fee Deficiency

☒ If any additional fee is required in connection with this communication, charge Account No. 07-0181.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
One of the Attorneys for Applicant(s)
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 telephone
(312) 569-3000 facsimile
Customer No.: 08968

Date: February 23, 2011

CH01/ 25685882.1

CI

Juniper Exhibit 1002, page 381

PATENT
Attorney Docket No. P3714US

COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

This declaration is of the following type:

☐ original ☐ design ☐ supplemental
☒ national stage of PCT/FR2009/051228, filed on June 26, 2009
☐ divisional ☐ continuation ☐ continuation-in-part

My residence, post office address, and citizenship are as stated below next to my name. I believe I am the original, first, and sole inventor *(if only one name is listed below)* or an original, first, and joint inventor *(if plural names are listed below)* of the subject matter which is claimed and for which a patent is sought on the invention entitled:

A METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

the specification of which:

☐ is attached hereto.
☒ was filed on December 29, 2010, as Application No. 13/001,907, and was amended on December 29, 2010 *(if applicable)*.
☐ was filed on , by Express Mail No. *as Application No. not known yet*, and was amended on *(if applicable)*.
☐ was filed on , as PCT International Application No. , and was amended on *(if any)*.

I state that I have reviewed and understand the contents of the specification identified above, including the claim(s), as amended by any amendment referred to above.

I acknowledge the duty to disclose information that is material to the patentability of the application identified above as defined in 37 CFR 1.56.

I claim foreign priority benefits under 35 USC 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate or 365(a) of any PCT international application(s) designating at least one country other than the United States of America listed below and have also identified below any foreign application(s) for patent, utility model, design registration, or inventor's certificate or any PCT international application(s) designating at least one country other than the United States of America filed by me on the same subject matter and having a filing date before that of the application(s) from which the benefit of priority is claimed.

PRIOR FOREIGN PATENT, UTILITY MODEL, AND DESIGN REGISTRATION APPLICATIONS						
COUNTRY	PRIOR FOREIGN APPLICATION NO.	DATE OF FILING (day,month,year)	PRIORITY CLAIMED			
France	08 54405	30 June 2008	X	YES		NO
				YES		NO
				YES		NO

CI

I claim the benefit pursuant to 35 USC 119(e) of the following United States provisional patent application(s):

PRIOR U.S. PROVISIONAL PATENT APPLICATIONS, BENEFIT CLAIMED UNDER 35 USC 119(e)	
APPLICATION NO.	DATE OF FILING (day,month,year)

I claim the benefit pursuant to 35 USC 120 of any United States patent application(s) or PCT international application(s) designating the United States of America listed below and, insofar as the subject matter of each of the claims of this patent application is not disclosed in the prior patent application(s) in the manner provided by the first paragraph of 35 USC 112, I acknowledge the duty to disclose material information as defined in 37 CFR 1.56 effective between the filing date of the prior patent application(s) and the national or PCT international filing date of this patent application.

PRIOR U.S. PATENT APPLICATIONS OR PCT INTERNATIONAL APPLICATIONS DESIGNATING THE U.S., BENEFIT CLAIMED UNDER 35 USC 120					
U.S. PATENT APPLICATIONS			Status *(check one)*		
U.S. APPLICATION NO.	U.S. FILING DATE		PATENTED	PENDING	ABANDONED
1.					
2.					
3.					
PCT APPLICATIONS DESIGNATING THE U.S.			Status *(check one)*		
PCT APPLICATION NO.	PCT FILING DATE (day,month,year)	U.S. APPLICATION NOS. ASSIGNED (if any)	PATENTED	PENDING	ABANDONED
4.					
5.					
6.					

DETAILS OF FOREIGN APPLICATIONS FROM WHICH PRIORITY CLAIMED UNDER 35 USC 119 FOR ABOVE LISTED U.S./PCT APPLICATIONS				
ABOVE APPLICATION. NO.	COUNTRY	APPLICATION NO.	DATE OF FILING (day,month,year)	DATE OF ISSUE (day,month,year)
1.				
2.				
3.				
4.				
5.				
6.				

Juniper Exhibit 1002, page 383

In re Appln. of Boucadair et al.
Attorney Docket No. P3714US

As a named inventor, I hereby appoint Drinker Biddle & Reath LLP to prosecute this application and transact all business in the Patent and Trademark Office connected therewith: Customer Number 08968.

08968
08968
PATENT TRADEMARK OFFICE

I further direct that correspondence concerning this application be directed to Drinker Biddle & Reath LLP: Customer Number 08968.

08968
08968
PATENT TRADEMARK OFFICE

I declare that all statements made herein of my own knowledge are true, that all statements made on information and belief are believed to be true, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full name of **sole or first inventor:** Mohamed BOUCADAIR

Inventor's signature _____

Date 25/01/2011

Country of Citizenship: France

Residence: Rennes, France
(city/state or country)

Post Office Address: 1, Square Louis Harel de la Nöe, 35000 Rennes, France
(complete mailing address)

CI

Full name of **second joint inventor,** if any: Jean-Luc GRIMAULT

Inventor's signature _____

Date 04/01/2011

Country of Citizenship: France

Residence: Mondeville, France
(city/state or country)

Post Office Address: 7, Impasse de l'Europe, 14120 Mondeville, France
(complete mailing address)

CH01/ 25646400.1

CI

Juniper Exhibit 1002, page 385

PATENT
Attorney Docket No. P3714US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Boucadair et al.

Group Art Unit: Unassigned

Application No. 13/001,907

Examiner: Unassigned

Filed: December 29, 2010

For: A METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

INFORMATION DISCLOSURE STATEMENT

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Pursuant to 37 CFR 1.97 and 1.98, the references listed on the enclosed Form PTO-1449 and/or Substitute Form PTO-1449 ("Form 1449") are submitted for consideration by the Examiner in the examination of the above-identified patent application.

The full consideration of the references in their entirety by the Examiner is respectfully requested and encouraged. Also, it is respectfully requested that the references be entered into the record of the present application and that the Examiner place his or her initials in the appropriate area on the enclosed Form 1449, thereby indicating the Examiner's consideration of each of the references.

The submission of the references listed on the Form 1449 is for the purpose of providing a complete record and is not a concession that the references listed thereon are prior art to the invention claimed in the patent application. The right is expressly reserved to establish an invention date earlier than the above-identified filing date in order to remove any reference submitted herewith as prior art should it be deemed appropriate to do so.

Further, the submission of the references is not to be taken as a concession that any reference represents art that is material, relevant or analogous to the claimed invention. Accordingly, the right to argue that any reference is not properly within the scope of prior art relevant to an examination of the claims in the above-identified application is also expressly reserved.

The Information Disclosure Statement is being filed:

☒ **within** any one of the following time periods: (a) within three months of the filing date of a national application other than a continued prosecution application under 37 CFR 1.53(d); (b) within three months of the date of entry of the national stage as set forth in 37 CFR 1.491 of an international application; (c) before the mailing date

of a first Office Action on the merits; or (d) before the mailing of a first Office Action after the filing of a request for continued examination under 37 CFR 1.114.

☐ **after** (a), (b), (c) or (d) above, but before the mailing date of a final action under 37 CFR 1.113, a Notice of Allowance under 37 CFR 1.311, or an action that otherwise closes prosecution in the application, and includes *one* of:

☐ the Statement under 37 CFR 1.97(e) (see "Statement under 37 CFR 1.97(e)" below).

or

☐ the fee of $180 set forth in 37 CFR 1.17(p) (see "Fees" below).

☐ **after** the mailing date of a final action under 37 CFR 1.113 or a Notice of Allowance under 37 CFR 1.311, or an action that otherwise closes prosecution in the application, and on or before payment of the issue fee, and includes the Statement under 37 CFR 1.97(e) (see "Statement under 37 CFR 1.97(e)" below), and the fee of $180 as set forth in 37 CFR 1.17(p) (see "Fees" below).

☐ **after** the mailing date of a Notice of Allowance under 37 CFR 1.311, and on or before payment of the issue fee, and **within** thirty days of receiving each item of information contained in the Information Disclosure Statement, and includes the Statement under 37 CFR 1.704(d) (see "Statement under 37 CFR 1.704(d)" below), and the fee of $180 as set forth in 37 CFR 1.17(p) (see "Fees" below).

NOTE: This is for original applications except applications for a design patent, filed on or after May 29, 2000, wherein a paper containing only an Information Disclosure Statement in compliance with 37 CFR 1.97 and 1.98 is being filed.

Copies of the References

☒ Copies of the references listed on the enclosed Form 1449 are enclosed herewith. Attached to each reference not in the English language is a concise explanation of the relevance pursuant to 37 CFR 1.98(a)(3).

☐ The filing date of the subject application is after June 30, 2003. Therefore, copies of U.S. patents and patent applications that are listed on the accompanying Form 1449 are not enclosed herewith in accordance with the U.S. Patent and Trademark Office's waiver of the requirement under 37 CFR 1.98 (see Official Gazette Notice of August 5, 2003). Copies of other references identified on the accompanying Form 1449 are enclosed herewith.

☐ Copy of the foreign search report is enclosed herewith.

☐ The references listed on the enclosed Form 1449 were previously identified in the parent application(s) of the present application, and copies of the references were furnished at that time. Accordingly, additional copies of the references are not submitted herewith, so as not to burden the file with duplicate copies of references. The Examiner is respectfully requested to carefully review the references in accordance with the requirements set out in the Manual of Patent Examining Procedure. In accordance with 37 CFR 1.98(d), the details of the parent application(s)

relied upon for an earlier filing date under 35 USC 120 in which copies of the references were previously furnished are set out below:

U.S. APPLICATIONS		Status *(check one)*		
U.S. APPLICATIONS	U.S. FILING DATE	PATENTED	PENDING	ABANDONED
1.				
2.				
3.				

Statement under 37 CFR 1.97(e)

☐ The **undersigned** hereby states that each item of information contained in the Information Disclosure Statement was first cited in any communication from a foreign patent office in a counterpart foreign patent application not more than three months prior to the filing of the Information Disclosure Statement.

☐ The **undersigned** hereby states that no item of information contained in the Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign patent application, and, to the knowledge of the undersigned after making reasonable inquiry, no item of information contained in the Information Disclosure Statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the Information Disclosure Statement.

Statement under 37 CFR 1.704(d)

☐ The **undersigned** hereby states that each item of information contained in the Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart application and that this communication was not received by any individual designated in 37 CFR 1.56(c) more than thirty days prior to the filing of the Information Disclosure Statement.

Fees

☒ **No fee** is owed by the applicant(s).
☐ The **IDS Fee of $180** under 37 CFR 1.17(p) is enclosed herewith.

Method of Payment of Fees

☐ Attached is a check in the amount of $.
☐ Charge Deposit Account No. 07-0181 in the amount of $.

Authorization to Charge Additional Fees

☒ If any additional fees are owed in connection with this communication, please charge Deposit Account No. 07-0181.

CI

In re Appln. of Boucadair et al.
Application No. 13/001,907

Instructions as to Overpayment

☒ Credit Account No. 07-0181.
☐ Refund

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: February 23, 2011

CH01/ 25685883.1

CI

Juniper Exhibit 1002, page 389

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
13/001,907	12/29/2010	Mohamed Boucadair	P3714US

CONFIRMATION NO. 5439

8968
DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

PUBLICATION NOTICE



Title:METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

Publication No.US-2011-0110375-A1
Publication Date:05/12/2011

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publically available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently http://www.uspto.gov/patft/.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently http://pair.uspto.gov/. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Office of Data Managment, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

CI

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/001,907	12/29/2010	Mohamed Boucadair	P3714US	5439

8968 7590 11/30/2012

DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

EXAMINER	
CHO, HONG SOL	

ART UNIT	PAPER NUMBER
2467	

NOTIFICATION DATE	DELIVERY MODE
11/30/2012	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

DBRIPDocket@dbr.com
IPDockets@dbr.com

Office Action Summary	Application No.	Applicant(s)	
	13/001,907	BOUCADAIR ET AL.	
	Examiner	Art Unit	
	HONG CHO	2467	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-10* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-10* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☒ The specification is objected to by the Examiner.

11)☒ The drawing(s) filed on *29 December 2010* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Specification

1. The abstract is objected to because it contains legal words, "said".

Claim Objections

2. Claims 1 and 7 are objected to because of the following informality:

Re claims 1 and 7, "said address" should read - - said IPv6 destination address- -.

Claim Rejections - 35 USC § 112, First paragraph

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-10 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

Juniper Exhibit 1002, page 393

Re claims 1, 2, 7 and 8, the specification fails to describe how the concatenation is carried out to construct an IPv6 destination address.

Claims 3-6, 9 and 10 depend on claims 1 and 7 are therefore similarly rejected.

Claim Rejections - 35 USC § 112, Second paragraph

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Re claims 1, 2, 7 and 8, it is not clear what an operator prefix is.

Claims 3-6, 9 and 10 depend on claims 1 and 7 are therefore similarly rejected.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hong Cho whose telephone number is 571-272-3087. The examiner can normally be reached on Mon-Fri during 7 am to 4 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Phillips can be reached on 571-272-3940. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Juniper Exhibit 1002, page 394

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Hong Cho/

Primary Examiner, Art Unit 2467

Notice of References Cited	Application/Control No. 13/001,907	Applicant(s)/Patent Under Reexamination BOUCADAIR ET AL.	
	Examiner HONG CHO	Art Unit 2467	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-2005/0286553 A1	12-2005	Wetterwald et al.	370/466
*	B	US-7,245,622 B2	07-2007	Huitema, Christian	370/392
*	C	US-7,551,632 B2	06-2009	Thubert et al.	370/401
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13001907	BOUCADAIR ET AL.
	Examiner	Art Unit
	HONG CHO	2467

SEARCHED			
Class	Subclass	Date	Examiner
370	389,392,393,401,466	11/26/2012	hc

SEARCH NOTES		
Search Notes	Date	Examiner
EAST text search	11/26/2012	hc

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13001907	BOUCADAIR ET AL.
	Examiner	**Art Unit**
	HONG CHO	2467

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	11/26/2012								
	1	✓								
	2	✓								
	3	✓								
	4	✓								
	5	✓								
	6	✓								
	7	✓								
	8	✓								
	9	✓								
	10	✓								

Please type a plus sign (+) inside this box →

Substitute for form 1449A/B/PTO				Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT				Application Number	13/001,907
				Filing Date	December 29, 2010
				First Named Inventor	Mohamed BOUCADAIR
				Group Art Unit	Unassigned
(Use as many sheets as necessary)				Examiner Name	Unassigned
Sheet	1	of	1	Attorney Docket Number	P3714US

U.S. PATENT DOCUMENTS

Examiner Initials	Doc. No.	U.S. Patent Document: Application or Patent Number	U.S. Patent Document: Kind Code	Name of Patentee or Applicant	Date of Publication	Filing Date If Appropriate

FOREIGN PATENT DOCUMENTS

Examiner Initials	Doc. No.	Foreign Patent Document: Office	Foreign Patent Document: Application or Patent Number	Foreign Patent Document: Kind Code	Name of Patentee or Applicant	Date of Publication	Translation: Yes	Translation: No*+
	A A	WO	2004/039014	A1	Cisco Technology, Inc.	May 6, 2004		
	A B	EP	1 420 559	A1	Thomson Licensing S.A.	May 19, 2004		
	A C	WO	2007/099248	A2	France Telecom	September 7, 2007		X+
	A D	WO	2008/001007	A2	France Telecom	January 3, 2008		X+

OTHER - NON PATENT LITERATURE DOCUMENTS

Examiner Initials	Doc. No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number (s), publisher, city and/or country where published.	Translation: Yes	Translation: No*+
	A E	AFIFI et al., "Methods for IPv4-IPv6 Transition," IEEE International Symposium on Computers and Communications, Red Sea, Egypt 6-8 July 1999, Proceedings, Los Alamitos, CA, USA, IEEE Comput. Soc., US, pp. 478-484 (July 6, 1999)		
	A F	KAWARASAKI et al., "IPv4/IPv6 SIP interworking methods in dual-stack network," The 9th Asia-Pacific Conference on Communications, 2003, APCC 2003, 21-24 September 2003, Piscataway, NJ, USA, IEEE, vol. 3, pp. 1124-1128 (September 21, 2003)		
	A G	PARK et al., "Network Address Translation – Protocol Translation (NAT-PT); draft-daniel-natpt-bis-01.txt," Internet Engineering Task Force, IETF, pp. 1-21 (October 22, 2005)		
	A H	SHIN et al., "Ports Option Support in Dual Stack Transition Mechanism (DSTM)," The 6th International Conference on Advanced Communication Technology, Phoenix Park, Korea, February 9-11, 2004, Piscataway, NJ, USA, IEEE, vol. 1, pp. 225-228 (February 9, 2004)		
	A I	SRISURESH et al., "RFC 2663 – IP Network Address Translator (NAT) Terminology and Considerations, " Network Working Group, retrieved from internet website: http://www.ietf.org/rfc/rfc2663.txt, pp. 1-30 (1999)		

Examiner Signature	/Hong Cho/	Date Considered	11/26/2012

* A concise statement of relevance is being submitted in lieu of a translation. 37 CFR 1.98(a)(3).

\+ An English-language equivalent/patent, or an English-language abstract, or an English-language version of the search report or action by a foreign patent office in a counterpart foreign application indicating the degree of relevance found by the foreign office is being submitted in lieu of a concise explanation of relevance under 37 CFR 1.98(a)(3).

CH01/ 25685885.1

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /H.C./

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S5	30434	370/389,392,393,401,466.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/11/19 10:49
S9	17	S5 and ipv4 with ipv6 same port near destination near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/11/19 10:50
S10	15	((MOHAMED) near2 (BOUCADAIR)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/19 10:51
S11	12	((JEAN-LUC) near2 (GRIMAULT)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2012/11/19 10:56
S14	134	ipv4 near destination adj address with port same ipv6 near destination adj address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/11/19 11:11
S15	7	(extract$3 or generat$3 or construct$3) with ipv6 near destination adj address same port with ipv4 near destination adj address with port	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/11/19 11:49
S18	7	(creat$3 or generat$3 or construct$3) with ipv6 near destination same ipv4 near destination with port	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/11/20 08:50
S20	20	(creat$3 or generat$3 or construct$3 or extract$3) with ipv4 near address with port same ipv6 near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2012/11/20 10:34

11/26/2012 8:26:23 AM
C:\Users\hcho\Documents\EAST\Workspaces\13001850.wsp

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 5439

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/001,907	12/29/2010	370	2467	P3714US

APPLICANTS

Mohamed Boucadair, Rennes, FRANCE;
Jean-Luc Grimault, Mondeville, FRANCE;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/FR2009/051228 06/26/2009

**** FOREIGN APPLICATIONS ***************************

FRANCE 0854405 06/30/2008

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

01/31/2011

Foreign Priority claimed ☑ Yes ☐ No 35 USC 119(a-d) conditions met ☑ Yes ☐ No Verified and Acknowledged /HONG SOL CHO/ Examiner's Signature	☐ Met after Allowance Initials	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
		FRANCE	9	10	2

ADDRESS

DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606
UNITED STATES

TITLE

METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

FILING FEE RECEIVED		
980	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

CI

PATENT
Attorney Docket No. P3714US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Boucadair et al.

Application No. 13/001,907

Filed: December 29, 2010

Group Art Unit: 2467

Examiner: Hong Sol Cho

For: A METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

RESPONSE TO OFFICE ACTION OF NOVEMBER 30, 2012

Mail Stop Amendment
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

In response to the Office Action of November 30, 2012, please enter the following amendments and consider the following remarks:

Amendments to the Specification begin on page 2 of this paper.

Amendments to the Abstract begin on page 3 of this paper.

Amendments to the Claims are provided in a listing of claims, which begins on page 4 of this paper.

Remarks begin on page 7 of this paper.

Amendments to the Specification

Please amend the paragraph at page 8, lines 20-24, as follows:

According to one aspect of the invention, when the data packet comes from the IPv4 domain and goes to a user terminal connected to the ~~IUPv6~~ IPv6 domain by said home gateway, the step of regularizing the ~~source~~ destination address comprises the following steps:

Please amend the paragraph at page 14, lines 20-27, as follows:

There is described below with reference to Figure 1 an IPv6 domain 1 and an IPv4 ~~domain 2~~ domain 3 or IPv6/IPv4 access node 40 to an IPv4 ~~domain 2~~ domain 3 and an access router 30 adapted to route data packets going to or coming from a home gateway 20 connected to the IPv6 domain 1. This kind of gateway administers a home network 2 to which the terminals 21 and 22 are connected.

Amendments to the Abstract

Please amend the abstract as follows:

A method of receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, ~~said~~ the packet comprising an IPv6 destination address and an IPv6 source address. The method comprises the following steps: identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address and a destination port number; if necessary, regularizing at least one address of the data packet and modifying the data packet; and routing the modified data packet to its destination.

The replacement Abstract is attached hereto on a separate sheet in accordance with 37 CFR 1.72.

Listing of the Claims

This Listing of Claims will replace all prior version, and listings, of claims in the application.

Claim 1 (currently amended): A method for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet comprising an IPv6 destination address and an IPv6 source address, said method being executed in a home gateway adapted to connect a user terminal to said IPv6 domain, and comprising the following steps:

identifying an IPv6 destination address constructed by concatenating an ~~operator~~ IPv6 prefix, an IPv4 destination address and a destination port number;

if necessary, regularizing at least one of the IPv6 source address and the IPv6 destination address of the data packet by replacing said at least one IPv6 address, the replacement process belonging to a group comprising replacement of a constructed address with a native address and replacement of a native address with a constructed address, and modifying the data packet using the regularized address; and

routing the modified data packet to its destination.

Claim 2 (currently amended): The method according to claim 1, wherein when the data packet comes from said user terminal and goes to the IPv4 domain, the step of regularizing the source address further comprises the following steps:

identifying an IPv6 native source address;

creating an entry in an address translation table, said entry associating said native source address with a source address constructed by concatenating an ~~operator~~ IPv6 prefix, an IPv4 address assigned to the gateway, and a source port number belonging to a range of port numbers authorized for said gateway; and

replacing the native source address of the data packet with the constructed source address.

Claim 3 (previously presented): The method according to claim 2, wherein address identification uses an identifier contained in the destination address.

Juniper Exhibit 1002, page 405

Claim 4 (previously presented): The method according to claim 2, further comprising a step of verifying that the source port number of the data packet and the source port number of the constructed source address match.

Claim 5 (currently amended): The method according to claim 1, wherein when the data packet comes from the IPv4 domain and goes to said user terminal, the step of regularizing the ~~source~~ destination address comprises the following steps:

searching an address translation table of the gateway for an entry associating with said constructed destination address a native destination address;

if an entry is found, replacing the constructed destination address of the data packet with the native destination address from that entry.

Claim 6 (previously presented): The method according to claim 5, further comprising a step of verifying that the destination port number of the data packet and the destination port number contained in the constructed destination address match.

Claim 7 (currently amended): A device for receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, said packet comprising an IPv6 destination address and an IPv6 source address, said device for use in a home gateway adapted to connect a user terminal to said IPv6 domain, comprising:

means for identifying an IPv6 destination address constructed by concatenating an ~~operator~~ IPv6 prefix, an IPv4 destination address, and a destination port number;

means for regularizing, if necessary, at least one of the IPv6 source address and the IPv6 destination address of the data packet by replacing said at least one IPv6 address, the replacement process belonging to a group comprising replacement of a constructed address with a native address and replacement of a native address with a constructed address, and modifying the data packet using the regularized address; and

means for routing the modified data packet to its destination.

Claim 8 (currently amended): A home gateway adapted to connect user terminals of a home network to an IPv6 domain connected to an IPv4 domain, comprising:

means for obtaining an IPv4 address, a range of port numbers authorized for said gateway, and a range of IPv6 addresses authorized for said gateway, said range of IPv6 addresses being constructed by concatenating an ~~operator~~ IPv6 prefix, said IPv4 address, and the range of authorized IPv4 port numbers; and

a device according to claim 7 for receiving an IPv6 data packet in the IPv6 domain connected to the IPv4 domain.

Claim 9 (previously presented): A home gateway according to claim 8, comprising an address translation table containing entries associating at least one source address for a communications session involving a user terminal of its home network, wherein said gateway is adapted to store in said entry an IPv6 constructed source address and an IPv6 native source address.

Claim 10 (previously presented): A non-transitory computer program product that is at least one of downloadable from a communications network and stored on a computer-readable medium and executable by a microprocessor, comprising program code instructions for executing the method according to claim 1 of receiving a data packet in an IPv6 domain.

REMARKS

The following remarks are responsive to the Office Action of November 30, 2012.

At the time of the Office Action, claims 1-10 were pending in the application. The status of the claims is as follows:

- All claims are rejected under 35 U.S.C. §112, first and second paragraphs.
- The abstract of the application was objected to.
- Claims 1 and 7 were objected to.

Claims 1, 2, 5, 7, and 8, and a paragraph in the specification corresponding to part of claim 5, are now amended as discussed in more detail below. Some typing mistakes are also corrected. The abstract is corrected as requested by the Examiner. No new matter is added by this amendment.

Specification.

The abstract was objected to as containing the word "said." That has now been corrected. The opportunity has also been taken to correct some typing mistakes on page 14.

Claim objections.

Claims 1 and 7 were objected to on the ground that "said address" at line 8 should apparently specify the IPv6 destination address. It is respectfully pointed out that the "said address" at line 8 is the "at least one IPv6 address" at line 7. The words "at least" make clear that it can be either the IPv6 destination address or the IPv6 source address. The claims have been amended to spell that out explicitly.

The opportunity has been taken to correct claim 5, and the corresponding paragraph on page 8, where "source address" should clearly read "destination address," in view of the four subsequent references to the destination address in question. The opportunity has also been taken to correct some typing mistakes in the paragraph being amended on page 8.

35 U.S.C. ¶ 112, first paragraph rejections.

Claims 1-10 stand rejected on the ground that there is allegedly no enabling disclosure of the "concatenation" recited in claims 1, 2, 7, and 8. The rejection is traversed.

It is respectfully pointed out that to "concatenate" is "to link together in a series or chain." An example of how the parts of the IPv6 address are concatenated is shown in Fig. 7

and described beginning at page 28, line 35 – page 29, line 6 (¶[0178] of the printed text US 2011/0110375). The IPv6 prefix used at page 29, line 3 is further described at page 18, line 5 – page 19, line 12 (¶[0115]-[0120] of the printed text). Concatenating a specified series of digital data is so well known in the digital arts that no further explanation should be necessary to enable the skilled person to put the claimed concatenation into effect.

35 U.S.C. ¶ 112, second paragraph rejections.

Claims 1-10 stand rejected on the ground that the expression "operator prefix" in claims 1, 2, 7, and 8 is allegedly unclear.

It is respectfully pointed out that the expression "operator prefix" is explicitly defined at page 18, lines 18-22 as the prefix assigned to an Internet Service Provider by its Regional Internet Registry. However, the expression "operator prefix" has been replaced by "IPv6 prefix." The rejection is therefore moot. Support for the amendment is found, for example, at page 14 lines 3-6 (explaining the function of the IPv6 prefix), page 15, line 34 to page 16, line 5, page 18, lines 1-22 and Fig. 2. See also Figs. 6 and 7 and their associated description.

Conclusion

For the foregoing reasons, this application is considered in good and proper form for allowance, and the Examiner is respectfully requested to pass this application to issue. If, in the opinion of the Examiner, a telephone conference would expedite the prosecution of the subject application, the Examiner is invited to call the undersigned attorney.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer Number: 08968

Date: February 25, 2013

CH01/ 26094890.1

ABSTRACT

A method of receiving an IPv6 data packet in an IPv6 domain connected to an IPv4 domain, the packet comprising an IPv6 destination address and an IPv6 source address. The method comprises the following steps: identifying an IPv6 destination address constructed by concatenating an operator prefix, an IPv4 destination address and a destination port number; if necessary, regularizing at least one address of the data packet and modifying the data packet; and routing the modified data packet to its destination.

Juniper Exhibit 1002, page 410

Electronic Acknowledgement Receipt	
EFS ID:	15037805
Application Number:	13001907
International Application Number:	
Confirmation Number:	5439
Title of Invention:	METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY
First Named Inventor/Applicant Name:	Mohamed Boucadair
Customer Number:	8968
Filer:	Brian Charles Rupp/Irina Mikitiouk
Filer Authorized By:	Brian Charles Rupp
Attorney Docket Number:	P3714US
Receipt Date:	25-FEB-2013
Filing Date:	29-DEC-2010
Time Stamp:	13:26:24
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		P3714US_Response_to_Office_Action.pdf	98434 1bc0dd40f74c2e485ce5b0a73e08b2e278c284ec	yes	8

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Amendment/Req. Reconsideration-After Non-Final Reject	1	1
	Specification	2	2
	Abstract	3	3
	Claims	4	6
	Applicant Arguments/Remarks Made in an Amendment	7	8

Warnings:					
Information:					
2	Abstract	P3714US_Replacement_Abstract.pdf	27701 13fd9c0ce1b948a2d6ecd1dbdf226d28fbc04819	no	1
Warnings:					
Information:					
		Total Files Size (in bytes):	126135		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 13/001,907	Filing Date 12/29/2010	☐ To be Mailed

APPLICATION AS FILED – PART I

	(Column 1)	(Column 2)	SMALL ENTITY ☐		OR	OTHER THAN SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE ($)	FEE ($)		RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		(Column 1)		(Column 2)	(Column 3)	SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
AMENDMENT	02/25/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	* 10	Minus	** 20	= 0	X $ =		OR	X $62=	0
	Independent (37 CFR 1.16(h))	* 2	Minus	***3	= 0	X $ =		OR	X $250=	0
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	**0**

		(Column 1)		(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)		RATE ($)	ADDITIONAL FEE ($)
	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/MARY HOLMES/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

8968 7590 03/21/2013

DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

EXAMINER
CHO, HONG SOL

ART UNIT	PAPER NUMBER
2467	

DATE MAILED: 03/21/2013

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/001,907	12/29/2010	INV001Mohamed Boucadair	P3714US	5439

TITLE OF INVENTION: METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1780	$300	$0	$2080	06/21/2013

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 02/11)

CI

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

8968 7590 03/21/2013
DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/001,907	12/29/2010	INV001Mohamed Boucadair	P3714US	5439

TITLE OF INVENTION: METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1780	$300	$0	$2080	06/21/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHO, HONG SOL	2467	370-393000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

PTOL-85 (Rev. 02/11)

CI

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29	NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
❑ Applicant asserting small entity status. See 37 CFR 1.27	NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
❑ Applicant changing to regular undiscounted fee status.	NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/001,907	12/29/2010	INV001Mohamed Boucadair	P3714US	5439

EXAMINER
CHO, HONG SOL

ART UNIT	PAPER NUMBER
2467	

8968 7590 03/21/2013

DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

DATE MAILED: 03/21/2013

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 275 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 275 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No.	Applicant(s)	
	13/001,907	BOUCADAIR ET AL.	
	Examiner	Art Unit	
	HONG CHO	2467	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *02/25/13*.
2. ☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. ☒ The allowed claim(s) is/are *1-10*. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov .
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
3. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
4. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
5. ☐ Examiner's Amendment/Comment
6. ☒ Examiner's Statement of Reasons for Allowance
7. ☐ Other _____.

/HONG CHO/
Primary Examiner, Art Unit 2467

Reasons for Allowance

1. Claims 1-10 are allowed.

2. The following is an examiner's statement of reasons for allowance:

Claims 1 and 7 are allowable over the prior art of record since the cited reference taken individually or in combination fails to particularly disclose identifying an IPv6 destination address constructed by concatenating an operator IPv6 prefix, an IPv4 destination address and a destination port number; if necessary, regularizing at least one of the IPv6 source address and the IPv6 destination address of the data packet by replacing at least one IPv6 address, the replacement process belonging to a group comprising replacement of a constructed address with a native address and replacement of a native address with a constructed address, and modifying the data packet using the regularized address.

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hong Cho whose telephone number is 571-272-3087. The examiner can normally be reached on Mon-Fri during 7 am to 4 pm.

Juniper Exhibit 1002, page 420

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Phillips can be reached on 571-272-3940. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Hong Cho/

Primary Examiner, Art Unit 2467

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	15	((MOHAMED) near2 (BOUCADAIR)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/12 08:04
L2	13	((JEAN-LUC) near2 (GRIMAULT)).INV.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/03/12 08:04
L4	31251	370/389,392,393,401,466.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/03/12 08:18
L5	19	L4 and ipv4 with ipv6 same port near destination near address	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/03/12 08:18
L10	44	(ipv4 with destination with (port or interface) same ipv6 with destination).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/03/12 08:42
L12	5	(ipv4 near destination with port same ipv6 near destination).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/03/12 09:03
L13	4	(ipv4 near destination with (port or interface) with ipv6 near destination).clm.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2013/03/12 09:03

3/12/2013 10:07:50 AM
C:\Users\hcho\Documents\EAST\Workspaces\13001850.wsp

Search Notes	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13001907	BOUCADAIR ET AL.
	Examiner	Art Unit
	HONG CHO	2467

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
370	389,392,393,401,466	11/26/2012	hc

SEARCH NOTES		
Search Notes	Date	Examiner
EAST text search	11/26/2012	hc
updated search	3/12/2013	hc

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
370	393, 401	3/12/2013	hc

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

BIB DATA SHEET

CONFIRMATION NO. 5439

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
13/001,907	12/29/2010	370	2467	P3714US

APPLICANTS

Mohamed Boucadair, Rennes, FRANCE;
Jean-Luc Grimault, Mondeville, FRANCE;

**** CONTINUING DATA ***************************

This application is a 371 of PCT/FR2009/051228 06/26/2009

**** FOREIGN APPLICATIONS ***************************

FRANCE 0854405 06/30/2008

**** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ****

01/31/2011

Foreign Priority claimed	35 USC 119(a-d) conditions met	Verified and Acknowledged	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
☑ Yes ☐ No	☑ Yes ☐ No	/HONG SOL CHO/ Examiner's Signature	FRANCE	9	10	2
	☑ Met after Allowance	HC Initials				

ADDRESS

DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606
UNITED STATES

TITLE

METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

FILING FEE RECEIVED		
980	FEES: Authority has been given in Paper No._____ to charge/credit DEPOSIT ACCOUNT No._____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

BIB (Rev. 05/07).

CI

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13001907	BOUCADAIR ET AL.
	Examiner	**Art Unit**
	HONG CHO	2467

CPC		
Symbol	**Type**	**Version**

CPC Combination Sets				
Symbol	**Type**	**Set**	**Ranking**	**Version**

US ORIGINAL CLASSIFICATION		INTERNATIONAL CLASSIFICATION	
CLASS	**SUBCLASS**	**CLAIMED**	**NON-CLAIMED**
370	393	H 0 4 L 12 / 28 (2006.01.01)	

CROSS REFERENCE(S)						
CLASS	**SUBCLASS (ONE SUBCLASS PER BLOCK)**					
370	401					

NONE		**Total Claims Allowed:**	
(Assistant Examiner)	(Date)	10	
/HONG CHO/ Primary Examiner.Art Unit 2467	03/12/13	O.G. Print Claim(s)	O.G. Print Figure
(Primary Examiner)	(Date)	1	3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13001907	BOUCADAIR ET AL.
	Examiner	**Art Unit**
	HONG CHO	2467

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 10	
/HONG CHO/ Primary Examiner.Art Unit 2467 (Primary Examiner)	03/12/13 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	13001907	BOUCADAIR ET AL.
	Examiner	**Art Unit**
	HONG CHO	2467

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1														
2	2														
3	3														
4	4														
5	5														
6	6														
8	7														
9	8														
10	9														
7	10														

NONE (Assistant Examiner)	(Date)	**Total Claims Allowed:** 10	
/HONG CHO/ Primary Examiner.Art Unit 2467 (Primary Examiner)	03/12/13 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 3

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

8968 7590 03/21/2013
DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/001,907	12/29/2010	INV001Mohamed Boucadair	P3714US	5439

TITLE OF INVENTION: METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	UNDISCOUNTED	$1780	$300	$0	$2080	06/21/2013

EXAMINER	ART UNIT	CLASS-SUBCLASS
CHO, HONG SOL	2467	370-393000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
- ❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- ❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Drinker Biddle & Reath LLP
2
3

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: France Telecom

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Paris, France

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ☒ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:
- ☒ Issue Fee
- ☒ Publication Fee (No small entity discount permitted)
- ❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
- ❑ A check is enclosed.
- ❑ Payment by credit card. Form PTO-2038 is attached.
- ☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 07-0181 (enclose an extra copy of this form).

PTOL-85 (Rev. 02/11)

CI

5. **Change in Entity Status** (from status indicated above)

❑ Applicant certifying micro entity status. See 37 CFR 1.29	NOTE: Absent a valid certification of Micro Entity Status (see form PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.
❑ Applicant asserting small entity status. See 37 CFR 1.27	NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.
❑ Applicant changing to regular undiscounted fee status.	NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature / brian c. rupp / Date 30 April 2013

Typed or printed name Brian C. Rupp Registration No. 35,665

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT
Attorney Docket No. P3714US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	Art Unit: 2467
Boucadair et al.	Examiner: Hong Sol Cho
Application No. 13/001,907	Date of Mailing of "Notice of Allowance and Fee(s) Due": March 21, 2013
Filed: December 29, 2010	

For: METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

TRANSMITTAL OF PAYMENT OF FEE(S) (37 CFR 1.311)

Mail Stop Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Dear Madam:

Applicants hereby pay the issue fee and the publication fee for the above-identified patent application.

Application Status

This application is on behalf of:

☒ other than a small entity or ☐ a small entity.

☐ The verified statement ☐ is attached or ☐ was filed on .

Assignment of Application

☒ This application is assigned to FRANCE TELECOM of Paris, France, and the assignment has been previously submitted to the Patent and Trademark Office.

☐ This application is NOT assigned.

☐ Assignment being submitted under separate cover. Assignment should be directed to Mail Stop ASSIGNMENT.

Fees

☒ Pursuant to 35 CFR 1.18(a), (b) and (c), the issue fee due in this application is $1,780.00.

☒ The publication fee due in this application is $300.00

In re Appln. of Boucadair et al.
Application No. 13/001,907

☐ Advance Order - _____ # of Copies

Payment of Fees

☐ A check in the amount of $

☒ Charge Deposit Account No. 07-0181 for any fee deficiency.

☒ Charge Deposit Account No. 07-0181 in the sum of $2,080.00.

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
One of Attorneys for Applicant(s)
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, IL 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: April 30, 2013

CH01/ 26147754.1

Juniper Exhibit 1002, page 431

Electronic Patent Application Fee Transmittal	
Application Number:	13001907
Filing Date:	29-Dec-2010
Title of Invention:	METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY
First Named Inventor/Applicant Name:	Mohamed Boucadair
Filer:	Brian Charles Rupp/Irina Mikitiouk
Attorney Docket Number:	P3714US
Filed as Large Entity	

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	1501	1	1780	1780
Publ. Fee- Early, Voluntary, or Normal	1504	1	300	300

CI

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
			Total in USD ($)	**2080**

Electronic Acknowledgement Receipt	
EFS ID:	15648765
Application Number:	13001907
International Application Number:	
Confirmation Number:	5439
Title of Invention:	METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY
First Named Inventor/Applicant Name:	Mohamed Boucadair
Customer Number:	8968
Filer:	Brian Charles Rupp/Irina Mikitiouk
Filer Authorized By:	Brian Charles Rupp
Attorney Docket Number:	P3714US
Receipt Date:	30-APR-2013
Filing Date:	29-DEC-2010
Time Stamp:	13:10:16
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$2080
RAM confirmation Number	11879
Deposit Account	070181
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Issue Fee Payment (PTO-85B)	P3714US_Issue_Fee.pdf	1014893 6e50b09e2e08d842e0a0537bcea6f18530a4d32f	no	2
Warnings:					
Information:					
2	Transmittal Letter	P3714US_Issue_Fee_Transmittal.pdf	55806 40fcf2c040f0b7bfc2ca3ca5b87591fc349649ad	no	2
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	32438 c134516736f07ffa6d1c8a3e53c6065ac789330d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	1103137		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
13/001,907	05/28/2013	8451845	P3714US	5439

8968 7590 05/08/2013

DRINKER BIDDLE & REATH LLP
ATTN: PATENT DOCKET DEPT.
191 N. WACKER DRIVE, SUITE 3700
CHICAGO, IL 60606

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 275 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Mohamed Boucadair, Rennes, FRANCE;
Jean-Luc Grimault, Mondeville, FRANCE;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.

PATENT
Attorney Docket No. P3714US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Number: 8,451,845

Issued: May 28, 2013

Name of Patentee: Boucadair et al.

Title of Invention: METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY

REQUEST FOR CERTIFICATE OF CORRECTION OF PATENT FOR APPLICANTS' MISTAKE (37 CFR 1.323)

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Attn: Decision and Certificate of Correction
Branch of the Patent Issue Division

Dear Sir:

It is requested that a Certificate of Correction be issued to correct errors found in the above-identified patent. These errors (1) occurred in good faith, (2) are of a clerical nature, a typographical nature, or a mistake of minor character, and (3) do not materially affect the scope or meaning of the patent, consistent with the provisions of MPEP § 1481.

Correction of the following 3 errors is requested:

(1) The phrase "address match" is to be appended to the sentence ending on column 5, line 38. This correction conforms the sentence to correspondence to claim 6 as filed in the original application and as issued, which ends with the phrase "address match." Without this phrase, the sentence ending on column 5, line 38, is obviously incomplete.

(2) The term "modified" is to be replaced with the term "IPv6" at the end of claim 1 (column 18, line 42). The claim is directed to a method relating to an "IPv6 data packet" and expresses (i) an "identifying" step, (ii) an optional "regularizing" step that modifies the "IPv6 data packet" and which is performed only "if necessary," and (iii) a "routing" step of the data packet to its destination. In those cases where the "regularizing" step is not necessary, then there is no "modified" data packet to be routed. Therefore, the last clause of claim 1 should be expressed as "routing the IPv6 data packet to its destination".

(3) The term "modified" is to be replaced with the term "IP^" at the end of claim 8 (column 20, lines 6-7). This is essentially the same correction as for claim 1, as explained above.

Patent No.: 8,451,845
Issued: May 28, 2013
Patentee: Boucadair et al.

Attached hereto is a Certificate of Correction, which indicates the requested corrections.

The Commissioner is hereby authorized to charge Deposit Account No. 07-0181 in the amount of $100.00 to cover the fee as required by 37 CFR 1.20(a).

Respectfully submitted,

/brian c. rupp/

Brian C. Rupp, Reg. No. 35,665
DRINKER BIDDLE & REATH LLP
191 N. Wacker Drive, Suite 3700
Chicago, Illinois 60606-1698
(312) 569-1000 (telephone)
(312) 569-3000 (facsimile)
Customer No.: 08968

Date: November 4, 2014

ACTIVE/ 76945353.1

CI

Juniper Exhibit 1002, page 438

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 8,451,845

DATED : May 28, 2013

INVENTOR(S) : Mohamed Boucadair; Jean-Luc Grimault

It is certified that errors appear in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

IN THE SPECIFICATION:

Column 5, line 38, replace "contained in the constructed destination." with --contained in the constructed destination address match.--

IN THE CLAIMS:

In Claim 1, Column 18, line 42, replace "routing the modified data packet to its destination" with -- routing the IPv6 data packet to its destination--

In Claim 8, Column 20, lines 6-7, replace " means for routing the modified data packet to its destination" with -- means for routing the IPv6 data packet to its destination--

MAILING ADDRESS OF SENDER:
Brian C. Rupp, Reg. No. 35,665
Drinker Biddle & Reath LLP
191 N. Wacker Drive, Suite 3700
Chicago, IL 60606-1698

ACTIVE/ 76945418.1

PATENT NO. 8,451,845
No. of additional copies
@ $.30 per page
⇨ _____

CI

Electronic Patent Application Fee Transmittal	
Application Number:	13001907
Filing Date:	29-Dec-2010
Title of Invention:	METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY
First Named Inventor/Applicant Name:	Mohamed Boucadair
Filer:	Brian Charles Rupp/Irina Mikitiouk
Attorney Docket Number:	P3714US
Filed as Large Entity	

U.S. National Stage under 35 USC 371 Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Certificate of Correction	1811	1	100	100
Extension-of-Time:				

CI

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
			Total in USD ($)	**100**

Electronic Acknowledgement Receipt	
EFS ID:	20604643
Application Number:	13001907
International Application Number:	
Confirmation Number:	5439
Title of Invention:	METHOD OF RECEIVING A DATA PACKET IN AN IPV6 DOMAIN, AN ASSOCIATED DEVICE AND AN ASSOCIATED HOME GATEWAY
First Named Inventor/Applicant Name:	Mohamed Boucadair
Customer Number:	8968
Filer:	Brian Charles Rupp/Irina Mikitiouk
Filer Authorized By:	Brian Charles Rupp
Attorney Docket Number:	P3714US
Receipt Date:	04-NOV-2014
Filing Date:	29-DEC-2010
Time Stamp:	16:30:03
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	$100
RAM confirmation Number	2879
Deposit Account	070181
Authorized User	
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. 1.492 (National application filing, search, and examination fees) Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)	

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Certificate of Correction	P3714US_Request_for_Certificate_of_Correction.pdf	142506 c4c3b98473f748aef96a2c6f87c8bc6619f387d4	no	3
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	30607 1fb239c9bffc1e617c2105607 95f88d44389647d	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	173113		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

SPE RESPONSE FOR CERTIFICATE OF CORRECTION

DATE : 01-09-15

TO SPE OF : ART UNIT 2467

SUBJECT : Request for Certificate of Correction for Appl. No.: 13/001907 Patent No.: 8451845

CofC mailroom date: 11-04-15

Please respond to this request for a certificate of correction within 7 days.

FOR IFW FILES:

Please review the requested changes/corrections as shown in the **COCIN** document(s) in the IFW application image. No new matter should be introduced, nor should the scope or meaning of the claims be changed.

Please complete the response (see below) and forward the completed response to scanning using document code **COCX**.

FOR PAPER FILES:

Please review the requested changes/corrections as shown in the attached certificate of correction. Please complete this form (see below) and forward it with the file to:

Certificates of Correction Branch (CofC)
Randolph Square – 9D10-A
Palm Location 7580

Note: _____

_____

Angela Green

Angela Green 571.272.9005

CofC Branch 703-756-1814

Thank You For Your Assistance

The request for issuing the above-identified correction(s) is hereby:

Note your decision on the appropriate box.

- ☐ **Approved** — **All** changes apply.
- ☐ **Approved in Part** — Specify below which changes **do not** apply.
- ☐ **Denied** — State the reasons for denial below.

Comments: _____

_____

_____

_____

_____

SPE **Art Unit**

SPE RESPONSE FOR CERTIFICATE OF CORRECTION

DATE : 01-09-15

TO SPE OF : ART UNIT 2467

SUBJECT : Request for Certificate of Correction for Appl. No.: 13/001907 Patent No.: 8451845

CofC mailroom date: 11-04-15

Please respond to this request for a certificate of correction within 7 days.

FOR IFW FILES:

Please review the requested changes/corrections as shown in the **COCIN** document(s) in the IFW application image. No new matter should be introduced, nor should the scope or meaning of the claims be changed.

Please complete the response (see below) and forward the completed response to scanning using document code **COCX**.

FOR PAPER FILES:

Please review the requested changes/corrections as shown in the attached certificate of correction. Please complete this form (see below) and forward it with the file to:

Certificates of Correction Branch (CofC)
Randolph Square – 9D10-A
Palm Location 7580

Angela Green

Note: _____

Angela Green 571.272.9005
CofC Branch 703-756-1814

Thank You For Your Assistance

The request for issuing the above-identified correction(s) is hereby:
Note your decision on the appropriate box.

- [x] **Approved** — **All** changes apply.
- [ ] **Approved in Part** — Specify below which changes **do not** apply.
- [ ] **Denied** — State the reasons for denial below.

Comments: _____

SPE hassan.phillips@uspto.gov Digitally signed by hassan.phillips@uspto.gov DN: cn=hassan.phillips@uspto.gov Date: 2015.01.14 17:00:14 -05'00'

Art Unit 2467

PTOL-306 (REV. 7/03) U.S. DEPARTMENT OF COMMERCE Patent and Trademark Office

CI

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 8,451,845 B2
APPLICATION NO. : 13/001907
DATED : May 28, 2013
INVENTOR(S) : Mohamed Boucadair and Jean-Luc Grimault

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

IN THE SPECIFICATION:

Column 5, line 38, replace "contained in the constructed destination." with --contained in the constructed destination address match.--

IN THE CLAIMS:

In Claim 1, Column 18, line 42, replace "routing the modified data packet to its destination" with --routing the IPv6 data packet to its destination--

In Claim 8, Column 20, lines 6-7, replace "means for routing the modified data packet to its destination" with --means for routing the IPv6 data packet to its destination--

Signed and Sealed this
Tenth Day of February, 2015

Michelle K. Lee

Michelle K. Lee
Deputy Director of the United States Patent and Trademark Office