

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 387 868**

51 Int. Cl.:
H04L 29/12 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 96 Número de solicitud europea: **09794026 .6**
- 96 Fecha de presentación: **26.06.2009**
- 97 Número de publicación de la solicitud: **2297928**
- 97 Fecha de publicación de la solicitud: **23.03.2011**

54 Título: **Procedimiento de recepción de un paquete de datos en un dominio IPv6, dispositivo y pasarela residencial asociados**

30 Prioridad:
30.06.2008 FR 0854405

45 Fecha de publicación de la mención BOPI:
03.10.2012

45 Fecha de la publicación del folleto de la patente:
03.10.2012

73 Titular/es:
**FRANCE TELECOM
6 place d'Alleray
75015 Paris, FR**

72 Inventor/es:
**BOUCADAIR, Mohamed y
GRIMAULT, Jean-Luc**

74 Agente/Representante:
Pérez Barquín, Eliana

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

ES 2 387 868 T3

DESCRIPCIÓN

Procedimiento de recepción de un paquete de datos en un dominio IPv6, dispositivo y pasarela residencial asociados

5 **Campo de la invención**

10 El campo de la invención es el de una red de telecomunicaciones, en particular una red de telecomunicaciones IP en la que son transportados paquetes de datos de un equipo fuente identificado mediante una dirección fuente a un equipo de destino identificado mediante una dirección de destino.

15 Dicha red de telecomunicaciones agrupa una pluralidad de equipos, de conexiones y de funciones dedicadas al transporte de los datos procedentes de equipos terminales conectados a esa red. En particular, las funciones de transporte pueden implementarse gracias a la activación de protocolos de enrutamiento y de transmisión. Una red de telecomunicaciones administrada por un operador también se denomina un dominio.

20 Un proveedor de servicio de conectividad IP despliega una arquitectura dedicada para permitir a los usuarios de equipos terminales que puedan establecer contacto. El acceso al servicio de conectividad IP es gestionado por el proveedor de servicio que se apoya en la red de telecomunicaciones de un operador para enrutar los paquetes de datos emitidos por los equipos terminales hacia sus destinos finales. En algunos casos, dicho proveedor de servicio es también el operador de la red de telecomunicaciones.

25 Dicho proveedor de servicio asigna una dirección IP, generalmente esta dirección es pública, a una pasarela residencial entre una red residencial y la red pública o dominio IP del operador. La pasarela residencial asigna, generalmente, a los terminales de su red residencial direcciones IP privadas.

30 En lo sucesivo, se designará como "pasarela residencial" a cualquier equipo de interconexión entre una red privada y una red operada por un proveedor de servicio, pudiendo ser también la red privada tanto una red residencial como una red de empresa.

En lo sucesivo, la red operada por los proveedores de servicio se designará también mediante la expresión "red pública".

35 Situada en la trayectoria de los paquetes de datos entre un terminal de su red residencial privada y el dominio IP del operador, la pasarela residencial comprende, de forma conocida, una tabla en la que asocia la dirección IP privada y el puerto asociado a ese terminal, con una dirección IP pública de tipo IPv4 y un puerto de esta misma pasarela en la red pública.

40 Esta tabla es conocida por el especialista en la técnica con la denominación "tabla de NAT", procediendo esta expresión del acrónimo NAT (*Network Address Translator* en inglés). Pueden implementarse varios tipos de NAT tales como "Full Cone", "Port Restricted" o también "simétrica".

45 Es admitido comúnmente por la comunidad de los proveedores de servicio IP que el agotamiento de las direcciones IPv4 públicas es una fatalidad. Para evitar este problema, la comunidad se ha movilizado en el pasado, lo que ha conducido a la definición de un nuevo protocolo: IPv6 (*Internet Protocol version 6*). Esta nueva versión del protocolo IP ofrece un gran número de direcciones IP y un mecanismo de enrutamiento jerárquico con rendimiento mejorado. Estos mismos proveedores no son, sin embargo, indiferentes a las alarmas emitidas recientemente por la IETF (*Internet Engineering Task Force*), particularmente en informes presentados en el grupo de trabajo GROW (*Global Routing Operations Working Group*) relativo a un riesgo de agotamiento de las direcciones IPv4 de la IANA (*Internet Assigned Numbers Authority*) a finales de 2010.

50 Sin embargo, esta solución, es decir IPv6, todavía no ha sido muy activada, en la práctica, por los operadores, por razones financieras, estratégicas y técnicas vinculadas a la gestión de la complejidad de las operaciones de transición y de migración.

55 Para limitar el número de direcciones públicas IPv4 necesarias para el suministro de un servicio de conectividad IP a un parque de clientes, una solución de doble NAT, también llamada "NAT de Operador", se ha propuesto e implementado. Ésta consiste en activar una función NAT en la red de telecomunicaciones del operador, de tal manera que las pasarelas residenciales utilicen una dirección privada en sus tablas de NAT hacia el exterior (en lugar de de una dirección pública). De este modo, es la función "NAT de Operador" la que asegura la traducción de las direcciones privadas de las pasarelas residenciales a direcciones públicas, lo que permite a un proveedor de servicio ahorrar un número no despreciable de direcciones públicas IPv4 requeridas para el suministro del servicio de conectividad IP.

Inconvenientes de la técnica anterior

La solución "NAT de Operador" presenta inconvenientes, entre los cuales:

- 5 - Una complejificación del procesamiento de los paquetes de datos IP: debido a la introducción de un segundo nivel de traducción de direcciones, los paquetes de datos deben ser modificados dos veces.
- 10 - La necesidad de adaptar la implementación de los protocolos de señalización aplicativa o ALG (*Application Level Gateway*) convencionales tales como DNS (*Domain Name System*), FTP (*File Transfer Protocol*) o también SIP (*Session Initiation Protocol*). En el caso de SIP, por ejemplo, el establecimiento y el mantenimiento de una sesión de voz en IP necesita que, para mantener actualizada la tabla de NAT de una pasarela residencial, deben implementarse intercambios de señalización frecuentes entre el terminal del abonado y la red pública mediante peticiones de registro de nuevo para mantener las sesiones de NAT activas. En presencia de un doble NAT, dicho mecanismo debe estar previsto también a nivel del equipo que alberga la función "NAT de Operador". La dirección y el puerto públicos que están siendo utilizados efectivamente por el terminal deben estar en comunicación además con la aplicación SIP.
- 15 - Una degradación del servicio de conectividad IP ofrecido por el operador de la red pública de telecomunicaciones debe ser deplorada, particularmente dado que funcionalidades tales como "*port forwarding*" o *DynDNS* no pueden ser soportadas en presencia del "NAT de Operador".
- 20

Por otro lado, dicha solución no podrá impedir, sino solamente retardar, el fenómeno de agotamiento de las direcciones IPv4. Será preciso, por lo tanto, prever a medio plazo un cambio a IPv6. Dicho cambio generará necesariamente un periodo de transición durante el cual los dominios IPv6 deberán interconectarse con dominios IPv4. Ahora bien, no se ha previsto nada en las redes actuales para facilitar dicha interconexión de manera eficaz, óptima y sin instanciación de estados suplementarios en los nodos de red empleados en el suministro del servicio de conectividad IP.

25

Tampoco está prevista la migración progresiva de un direccionamiento IPv4 a un direccionamiento IPv6 a partir de mecanismos de interconexión sencillos entre un dominio IPv6 y un dominio IPv4, particularmente que no necesiten que los terminales cliente implementen a la vez el protocolo IPv4 y el protocolo IPv6. El documento D1 = MYUNG-KI SHIN ET AL: "Ports option support in dual stack transition mechanism (DSTM)", THE 6TH INTERNATIONAL CONFERENCE ON ADVANCED COMMUNICATION TECHNOLOGY, 9-11 FEBRURAY 2004, PHOENIX PARK, COREA, páginas 225-228, describe un procedimiento de recepción de un paquete de datos IPv6 en un dominio IPv6 interconectado con un dominio IPv4.

30

35

Exposición de la invención

La invención mejora la situación con ayuda de un procedimiento de recepción de un paquete de datos IPv6 en un dominio IPv6 interconectado con un dominio IPv4, comprendiendo dicho paquete una dirección IPv6 de destino y una dirección IPv6 fuente.

40

De acuerdo con la invención, dicho procedimiento se ejecuta en una pasarela residencial apta para conectar un terminal del usuario a dicho dominio IPv6 y comprende las siguientes etapas:

45

- identificación de una dirección IPv6 de destino construida mediante concatenación de un prefijo de operador, de una dirección de destino IPv4 y de un número de puerto de destino;
- 50 - si fuera necesario, puesta en conformidad de al menos una dirección del paquete de datos mediante sustitución de dicha dirección, perteneciendo dicha sustitución a un grupo que comprende una sustitución de una dirección construida por una dirección nativa de dicho terminal del usuario y una sustitución de una dirección nativa de dicho terminal del usuario por una dirección construida, y modificación del paquete de datos con ayuda de la dirección puesta en conformidad; y
- 55 - enrutamiento del paquete de datos modificado hacia su destino.

En un contexto de migración del protocolo IPv4 hacia el protocolo IPv6, se considera un primer equipo terminal de un dominio IPv4 que solamente puede emitir y recibir un paquete de datos de acuerdo con el protocolo IPv4. Paralelamente, un segundo equipo terminal del dominio IPv6 solamente puede emitir y recibir un paquete de datos IPv6. De acuerdo con la invención, cuando uno de estos equipos desea enviar un paquete de datos al otro, utiliza su protocolo, pero los datos enrutados en el dominio IPv6 lo son de acuerdo con el protocolo IPv6.

60

El paquete de datos es emitido, por lo tanto, en IPv4 o IPv6, transformado si fuera necesario en un paquete de datos de acuerdo con el protocolo IPv6 para su enrutamiento en el dominio IPv6, y a continuación se transforma de nuevo, si fuera necesario en un paquete de datos IPv4.

65

5 Dicha transformación se apoya en un mecanismo de construcción de dirección de destino IPv6 a partir de una dirección de destino IPv4 del primer terminal mediante concatenación de un prefijo de operador, de esta dirección de destino IPv4 y del número de puerto de destino del paquete. En efecto, se considera el caso en el que un equipo de interconexión del dominio IPv6 con el dominio IPv4 construye una dirección de destino IPv6 a partir de la dirección de destino IPv4 y del puerto de destino. Esta dirección de destino IPv6 construida es enrutable en el dominio IPv6 y comprende las informaciones útiles transportadas por el paquete de datos IPv4.

10 Esta transformación necesita que el segundo terminal del usuario, aunque implemente el protocolo IPv6, disponga de una dirección "ficticia" IPv4, que puede ser la suya o la de una pasarela residencial que administra una red residencial a la que está conectado. Esta dirección, utilizada como dirección de destino de un paquete IPv4 procedente del dominio IPv4, es utilizada por el equipo de interconexión para construir la dirección de destino IPv6 mencionada anteriormente.

15 A la inversa, es posible recuperar la dirección IPv4 y el número de puerto en el origen de una dirección IPv6 construida de acuerdo con dicho mecanismo (es decir respetando el formalismo de construcción de dirección IPv6 que se acaba de mencionar). Por lo tanto, no es necesario almacenar una tabla de traducción de direcciones IPv4 a IPv6 ni mantener estados relativos a sesiones a nivel del nodo de acceso (también llamado nodo de interconexión) de los dos dominios IPv4 e IPv6. La invención permite, por lo tanto, en sentido IPv4 a IPv6 (así como de IPv6 a IPv4), enrutar el paquete de datos IPv4 en forma de un paquete de datos IPv6 hacia su destino y suministrar las informaciones útiles contenidas en el paquete a su destinatario, sin recurrir a tablas de estado pesadas de mantener.

20 De este modo, ni el terminal del usuario IPv6 destinatario o emisor del paquete de datos, ni eventualmente la pasarela residencial que lo gestiona, ni tampoco los enrutadores encargados de enrutar el paquete a su destino necesitan interpretar el protocolo IPv4.

25 Sin embargo, para que el enrutamiento del paquete de datos IPv6 procedente de dicha transformación pueda realizarse como el de un paquete IPv6 nativo, es necesario verificar una conformidad de sus direcciones fuente y destino con respecto al formalismo mencionado anteriormente. El procedimiento de acuerdo con la invención propone, por lo tanto, una solución para identificar que el destino o la procedencia de este paquete pertenecen a un dominio IPv4 y para aplicarle en consecuencia un procesamiento de verificación apropiado.

30 De acuerdo con un aspecto de la invención, cuando el paquete procede de dicho terminal del usuario y su destino es el dominio IPv4, la etapa de puesta en conformidad de la dirección fuente comprende, además, las siguientes etapas:

- 35 - identificación de una dirección IPv6 fuente nativa;
- creación de una entrada en una tabla de traducción de direcciones, asociando dicha entrada dicha dirección fuente nativa a una dirección fuente construida mediante concatenación de un prefijo de operador, de una dirección IPv4 asignada a la pasarela y de un número de puerto fuente que pertenece a un intervalo de números de puerto autorizados por dicha pasarela; y
- 40 - sustitución de la dirección fuente nativa del paquete de datos por la dirección fuente construida.

45 Se trata, en este caso, de una llamada saliente. Cuando se ha podido identificar una dirección de destino construida, puede deducirse de ella que el paquete de datos está destinado a un terminal del usuario del dominio IPv4. En este caso, su dirección fuente debe ser una dirección construida para que un equipo de interconexión del dominio IPv6 con el dominio IPv4 pueda recuperar a continuación la dirección IPv4 fuente y transformar de forma inversa el paquete de datos IPv6 en un paquete de datos IPv4. Si no se ha realizado ningún procesamiento, el paquete no podrá ser transmitido por el nodo de interconexión; ya que la dirección fuente nativa no contiene información relativa a la dirección IPv4 fuente, es decir la dirección IPv4 ficticia del terminal que haya emitido dicho paquete.

50 Si la dirección fuente es nativa, el procedimiento de acuerdo con la invención permite sustituirla por una dirección fuente construida que pertenece a un prefijo o intervalo de direcciones fuente IPv6 autorizadas por la pasarela.

55 En previsión de la recepción de una respuesta a este paquete de datos, una asociación entre la dirección fuente nativa de origen y la dirección fuente construida se añade a una tabla de traducción de direcciones de la pasarela residencial.

60 De este modo, un paquete de datos emitido en respuesta podrá enrutarse hasta el terminal del usuario de la red residencial que había emitido el primer paquete de datos.

65 Una ventaja de la invención es que permite a un terminal del usuario IPv6 utilizar la dirección fuente que desee para emitir paquetes de datos destinados a un dominio IPv4, ya que la pasarela de acuerdo con la invención hace lo necesario para que sean enrutados a su destino.

De acuerdo con un aspecto de la invención, la identificación de la dirección se realiza con ayuda de un identificador comprendido en la dirección de destino.

5 Este identificador puede tener diferentes valores según se trate de una dirección IPv6 nativa o de una dirección IPv6 construida a partir de una dirección IPv4. Una ventaja es permitir una identificación sencilla y rápida de la naturaleza de la dirección del paquete de datos. Dicha solución permite también una mutualización de los equipos de interconexión IPv4-IPv6 entre varios operadores.

10 De acuerdo con otro aspecto de la invención, el procedimiento de recepción comprende, además, una etapa de verificación de una concordancia entre el número de puerto fuente del paquete de datos y el número de puerto fuente de la dirección fuente construida.

15 En efecto, el paquete de datos comprende un número de puerto fuente a nivel de la capa de transporte de acuerdo con el modelo OSI. Para que una respuesta pueda ser enrutada por la red al terminal emisor del primer paquete, es importante que este número de puerto fuente de nivel de transporte concuerde con el número de puerto fuente contenido en la dirección fuente construida del paquete de datos. Si este no es el caso, el procedimiento de acuerdo con la invención permite hacer concordar a los dos números de puerto fuente.

20 Se observará que la etapa de verificación y la etapa de puesta en conformidad de la dirección fuente pueden realizarse simultáneamente. Por ejemplo, la elección de una dirección fuente construida en el prefijo de la pasarela puede integrar la limitación de tener un número de puerto fuente igual al número de puerto fuente del nivel de transporte.

25 De acuerdo con un aspecto de la invención, cuando el paquete de datos procede del dominio IPv4 y tiene como destino el terminal del usuario conectado al dominio IPv6 mediante dicha pasarela residencial, la etapa de puesta en conformidad de la dirección fuente comprende las siguientes etapas:

30 - búsqueda en una tabla de traducción de direcciones de dicha pasarela de una entrada que asocia a dicha dirección de destino una dirección de destino nativa;

- si se ha encontrado una entrada, sustitución de la dirección de destino construida del paquete de datos por la dirección de destino nativa de la entrada.

35 Se observará que el número de puerto de destino se sustituye también por el mostrado en la tabla de traducción de direcciones y de puertos mantenida por la pasarela residencial.

40 En este caso se trata una llamada entrante. El paquete de datos IPv6 se ha construido a partir de un paquete IPv4 por un equipo de interconexión del dominio IPv6 al dominio IPv4. Puede ser que constituya una respuesta a un paquete de datos emitido anteriormente por el terminal del usuario conectado a la pasarela residencial. Ésta consulta, por lo tanto, su tabla de traducción. Si encuentra en ésta una asociación entre la dirección de destino extraída del paquete de datos recibido y una dirección de destino IPv6 nativa, sustituye la dirección de destino y potencialmente el número de puerto de destino construido del paquete de datos por la dirección IPv6 nativa de la entrada y enruta el paquete modificado al terminal destinatario.

45 De acuerdo con otro aspecto de la invención, el procedimiento de recepción comprende, además, una etapa de verificación de una concordancia entre el número de puerto de destino del paquete de datos y el número de puerto de destino contenido en la dirección de destino construida.

50 Dicha verificación permite asegurarse de que el número de puerto de destino del paquete de datos a nivel de transporte coincida correctamente con el número de la dirección de destino construida del paquete. Esta verificación presenta un interés particular si la dirección IPv4 ficticia asignada a la pasarela doméstica es compartida con varias terminales o pasarelas domésticas más. En efecto, en este caso, la discriminación entre estos equipos se realiza en base al intervalo de números de puerto utilizado. Con la invención, el enrutamiento de un paquete emitido por el terminal IPv4 hacia dicha dirección ficticia puede tener lugar hacia la pasarela en cuestión sin encontrar ningún problema de enrutamiento.

60 El procedimiento de recepción puede realizarse en un dispositivo de recepción de un paquete de datos en un dominio IPv6 interconectado a un dominio IPv4, comprendiendo dicho paquete una dirección IPv6 de destino y una dirección IPv6 fuente, caracterizado por que comprende las siguientes etapas:

- identificación de una dirección de destino construida mediante concatenación de un prefijo de operador, de una dirección de destino IPv4 y de un número de puerto de destino;

65 - si fuera necesario, puesta en conformidad de al menos una dirección del paquete de datos; y

- enrutamiento del paquete de datos modificado hacia su destino.

En una realización particular, las diferentes etapas de los procedimientos de recepción de un paquete de datos son determinadas por instrucciones de programas informáticos.

5 En consecuencia, la invención también se refiere a un programa informático en un soporte de información, siendo este programa susceptible de implementarse en un dispositivo de recepción o, de forma más general, en un ordenador, comprendiendo este programa instrucciones adaptadas a la realización de las etapas de un procedimiento de enrutamiento, de recepción o de transmisión, tal como se ha descrito anteriormente.

10 Este programa puede utilizar cualquier lenguaje de programación y estar en forma de código fuente, código objeto o de código intermedio entre código fuente y código objeto, tal como en forma parcialmente compilada, o en cualquier otra forma deseable.

15 La invención también se refiere a un soporte de información legible por un ordenador, y que comprende instrucciones de un programa informático tal como se ha mencionado anteriormente.

20 El soporte de información puede ser cualquier entidad o dispositivo capaz de almacenar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, tal como una ROM, por ejemplo un CD ROM o una ROM de circuito microelectrónico, o también un medio de registro magnético, por ejemplo un disquete (*floppy disc*) o un disco duro.

Por otro lado, el soporte de información puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede ser enrutada mediante un cable eléctrico u óptico, mediante radio o mediante otros medios. El programa de acuerdo con la invención puede descargarse en particular de una red de tipo Internet.

25 Como alternativa, el soporte de información puede ser un circuito integrado en el que está incorporado el programa, estando el circuito adaptado para ejecutar o para ser utilizado en la ejecución del procedimiento en cuestión.

30 La invención también se refiere a una pasarela residencial apta para conectar terminales del usuario a un dominio IPv6 interconectado a un dominio IPv4. De acuerdo con la invención, dicha pasarela comprende:

35 - medios de obtención de una dirección IPv4, de un intervalo de números de puerto autorizados para dicha pasarela y de un intervalo de direcciones IPv6 autorizadas para dicha pasarela, estando dicho intervalo de direcciones IPv6 construido por concatenación de un prefijo de operador, de dicha dirección IPv4 y del intervalo de números de puerto IPv4 autorizados; y

- un dispositivo de recepción de un paquete de datos IPv6 en el dominio IPv6 interconectado al dominio IPv4 de acuerdo con la invención.

40 De acuerdo con la invención, dicha pasarela solamente procesa paquetes de datos IPv6. Sin embargo, se le asigna una dirección IPv4, de modo que pueda ser identificada y contactada por emisores del dominio IPv4. Dicha dirección no es utilizada por la pasarela doméstica para el envío de los paquetes IP.

45 La pasarela residencial puede comprender una tabla de traducción de direcciones, que comprende entradas, que asocian, para una sesión de comunicación que implica el terminal del usuario de su red residencial, al menos una dirección fuente. De acuerdo con la invención, dicha pasarela es apta para registrar en dicha entrada, una dirección fuente IPv6 construida y una dirección fuente IPv6 nativa del terminal del usuario.

Lista de las figuras

50 Otras ventajas y características de la invención serán más claramente evidentes con la lectura de la siguiente descripción de una realización particular de la invención, que se da a modo de simple ejemplo ilustrativo y no limitante, y de los dibujos adjuntos, en los que:

55 - la figura 1 presenta, de forma esquemática, un dominio IPv6 interconectado a un dominio IPv4 de acuerdo con la invención;

- la figura 2 ilustra la estructura de un prefijo de direcciones IPv6 construido de acuerdo con la invención;

60 - la figura 3 presenta, de forma esquemática, las etapas del procedimiento de recepción de un paquete de datos en un dominio IPv6 interconectado con un dominio IPv4 de acuerdo con la invención;

- la figura 4 ilustra la estructura de una dirección IPv6 construida a partir de una dirección de destino IPv4 y de un puerto de destino de acuerdo con una primera realización de la invención;

65 - la figura 5 ilustra la estructura de una dirección de destino IPv6 construida a partir de una dirección IPv4 y de un puerto de destino de acuerdo con la invención, para la realización del procedimiento de recepción de acuerdo con la

primera realización de la invención;

- la figura 6 ilustra la estructura de una dirección fuente IPv6 construida a partir de una dirección fuente IPv4 y de un puerto fuente para la realización del procedimiento de recepción de acuerdo con la primera realización de la invención;

- la figura 7 ilustra la estructura de una dirección IPv6 construida a partir de una dirección IPv4 y de un puerto de destino de acuerdo con una segunda realización de la invención;

- la figura 8 presenta, de forma esquemática, las etapas del procedimiento de recepción de un paquete de datos en un dominio IPv6 interconectado con un dominio IPv4 de acuerdo con la segunda realización de la invención; y

- la figura 9 presenta, de forma esquemática, la estructura de un dispositivo de recepción de un paquete de datos en un dominio IPv6 de acuerdo con la invención;

Descripción de una realización particular de la invención

El principio general de la invención se basa en la construcción de una dirección IPv6 a partir de una dirección IPv4, de un prefijo de operador predeterminado y de un número de puerto. Dicha construcción permite la transformación de un paquete IPv4 que entra en un dominio IPv6 y, a la inversa, de un paquete IPv6 que sale de un dominio IPv6 con destino a un dominio IPv4, sin que sea necesario mantener una tabla de correspondencia entre las direcciones IPv4 e IPv6 en un nodo de acceso al dominio IPv6.

Como recordatorio, las direcciones IPv6 tienen una longitud de 16 octetos, es decir 128 bits, frente a 4 octetos (32 bits) para las direcciones IPv4. Se dispone de este modo de un número potencial de direcciones extremadamente grande con respecto al número de direcciones IPv4. Una dirección IPv6 comprende dos partes:

- la parte de la izquierda (el prefijo) identifica una sub-red del dominio;

- la parte de la derecha identifica una máquina conectada a la sub-red.

Generalmente, los prefijos más largos asignados a una sub-red son prefijos "/64"; es decir que comprenden 64 bits para identificarlos. Los 64 bits de la derecha de la dirección se utilizan entonces para identificar una máquina particular que pertenece a la sub-red. Los prefijos de longitudes más cortas (ejemplo "/56" o incluso "/48") permiten a su vez identificar sub-redes de mayor amplitud, que comprenden a menudo ellas mismas sub-redes "/64". Sin embargo, en el estándar IPv6, nada impide utilizar prefijos más largos que "/64" y, por lo tanto, podemos imaginar, por ejemplo, un prefijo "/116" que identifica una sub-red que puede comprender 4096 máquinas.

Se observará que la única restricción a los prefijos más largos que "/64" consiste simplemente en el hecho de que las máquinas detrás de la sub-red correspondiente no podrán emplear el mecanismo de auto-configuración descrito en el documento RFC2462. Este mecanismo permite a una máquina que conozca su dirección de nivel 2 (por ejemplo su dirección Ethernet MAC) configurar ella misma, en ciertas condiciones, los 64 bits de la derecha de su dirección IPv6, derivando de ella su dirección de nivel 2 siguiendo un algoritmo preciso. Sin embargo, este mecanismo de auto-configuración no es obligatorio y pueden preferirse otros mecanismos como, por ejemplo, el correspondiente al protocolo DHCPv6 [RFC3315] que permite, entre otras cosas, obtener una dirección IPv6 de un servidor DHCPv6.

Si nos interesa ahora, ya no una simple máquina IPv6, sino un enrutador IPv6 (como por ejemplo una pasarela residencial IPv6), se sabe que dicho equipamiento debe disponer de uno (o varios) prefijos IPv6 que representa(n) la(s) sub-red(es) cuyos paquetes enruta. Un enrutador IPv6 debe estar configurado, por lo tanto, con uno (o varios) prefijos.

Una extensión de DHCPv6 permite a un enrutador que requiere uno o varios prefijos IPv6 (como por ejemplo una pasarela residencial) solicitarlos a un equipo que puede delegarlos (típicamente un enrutador aguas arriba). Esta extensión se describe en el RFC 3633 (*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*) y especifica una opción "Identity Association for Prefix Delegation Option" en los mensajes DHCPv6 para pasar el o los prefijos delegados. Una vez que el enrutador que realiza la petición se ha visto delegado uno o más prefijos IPv6, enruta todos los paquetes IPv6 destinados a o procedentes de máquinas cuyas direcciones se inscriben en el(los) prefijo(s) que gestiona.

Se presenta a continuación, en relación con la figura 1, un dominio IPv6 1 que comprende un equipo de interconexión del dominio IPv6 1 con un dominio IPv4 2 o nodo de acceso IPv6/IPv4 40 a un dominio IPv4 2 y un enrutador de acceso 30, apto para enrutar paquetes de datos hacia o procedentes de una pasarela residencial 20 conectada al dominio IPv6 1. Dicha pasarela administra una red residencial 2 a la que están conectados los terminales 21 y 22.

En el contexto de la invención, se considera una pasarela residencial que implementa el protocolo IPv6 en solitario. Debido a esto, dicha pasarela está en condiciones de procesar (en particular, recibir y emitir) solamente paquetes de datos de tipo IPv6.

- 5 Los terminales 21 y 22 son, a su vez, de versión única IPv6 (o puramente IPv6), es decir que solamente implementan el protocolo IPv6. A continuación veremos cómo la invención permite una interconexión de un dominio IPv6 con al menos un dominio IPv4 para terminales IPv6.

Se considera los siguientes casos “híbridos”:

- 10 - enrutamiento de un paquete de datos IPv4 entrante emitido por un terminal del usuario del dominio IPv4 3 con destino a un terminal del usuario 21, 22 de la red residencial de la pasarela 20 conectada al dominio IPv6 1; y
- 15 - enrutamiento de un paquete de datos IPv6 saliente emitido por un terminal del usuario 21, 22 del dominio IPv6 1 hacia un terminal del usuario del dominio IPv4 3.

Dado que los casos de una transmisión de paquetes puramente IPv6 o IPv4 son conocidos por el especialista en la técnica, no se describirán con más detalle.

- 20 Para poder conectarse al dominio o la red IPv6, la pasarela residencial dispone de elementos de conectividad IP suministrados por el proveedor de servicio de conectividad.

Se observará, sin embargo, que la invención no se limita al acceso al servicio de conectividad IP, por ejemplo Internet o Intranet, mediante una pasarela residencial, sino que se aplica también a terminales del usuario en otros contextos de acceso a Internet o de acceso a una red de Intranet. Puede mencionarse, por ejemplo, el acceso a este servicio de conectividad IP desde una red móvil, de acuerdo con la cual un terminal móvil evolucionado podría servir de pasarela, comunicando con otros terminales de su red LAN (mediante Bluetooth por ejemplo) o también el caso de un simple terminal móvil.

- 30 De acuerdo con la invención, la pasarela residencial 20 dispone de los siguientes elementos de conectividad IP:

35 - una dirección IPv4 clásica denominada en lo sucesivo “@IPv4”; en el caso en el que la pasarela aloja en su red residencial terminales cliente puramente IPv6, esta dirección IPv4 se denomina “ficticia” ya que no es utilizada por la pasarela para enviar/recibir tráfico IP; veremos a continuación que es utilizada para construir direcciones IPv6 de acuerdo con la invención;

- un intervalo de números de puerto autorizados denominado ports_pattern/length_of_unvariable;

40 - un prefijo de direcciones IPv6 construidas denominado IPv6_prefix_ports_range; y

- un prefijo de direcciones denominado prefijo IPv6 nativo IPv6_prefix_native; este último prefijo no es, sin embargo, obligatorio; solamente el prefijo IPv6 construido es suficiente.

- 45 Los elementos @IPv4, IPv6_prefix_ports_range e IPv6_prefix_native son elementos de información estándar en el marco habitual de los protocolos IPv4 e IPv6.

De acuerdo con la invención, el elemento de información IPv6 _prefix_ports_range contiene intrínsecamente los elementos @IPv4 y ports_pattern/length_of_unvariable.

- 50 En una realización de la invención, la dirección IPv4 @IPv4 es una dirección shared@IPv4 compartida por varias pasarelas residenciales del dominio IPv6 1 y el intervalo de números de puerto autorizados para la pasarela residencial 20 es un intervalo de números de puerto reservados a esta pasarela.

55 Se entenderá que el hecho de compartir la dirección pública shared@IPv4 entre varias pasarelas residenciales permite ahorrar el número de direcciones IPv4 utilizadas y retardar el fenómeno de agotamiento. Además, su utilización está justificada por la necesidad de interconectar dominios IPv4 con otros IPv6. Esta interconexión se realiza en general mediante direcciones de representación. Si el parque de clientes IPv6 es grande, entonces las direcciones de representación IPv4 requeridas es consecuente.

- 60 Las diferentes pasarelas residenciales que comparten la misma dirección shared@IPv4 son identificadas de forma única por los números de puerto que utilizan, ya que cada una de ellas se beneficia de un intervalo de números de puerto contiguo, ciertamente restringido, pero que le está reservado.

65 La invención propone una interconexión entre dominios IPv6 e IPv4 que necesita la asignación de direcciones IPv4 para funcionar y asegurar, de este modo, una continuidad de conectividad entre terminales heterogéneas (es decir que implementan protocolos de direccionamiento diferentes, tales como IPv4 e IPv6) de manera transparente.

Una ventaja de la realización de la invención, de acuerdo con la cual las direcciones IPv4 son compartidas es, por lo tanto, facilitar la migración hacia el direccionamiento IPv6 mientras se economizan las direcciones IPv4. En un contexto de transición entre los dos modos de direccionamiento IPv4, IPv6, dicho ahorro puede permitir ventajosamente evitar la penuria de direcciones mientras la migración no ha terminado. Otra ventaja es tener una

5 amortización de la inversión inmediata para los equipos IPv6 (ya que la utilización de las capacidades IPv6 no depende del comportamiento de los clientes sino del propio operador).

En lo sucesivo en la descripción, se considera el ejemplo de realización de acuerdo con el cual la dirección IPv4 asignada a la pasarela 20 es una dirección compartida Shared@IPv4.

10 En relación con la figura 1, la pasarela residencial 20 está conectada a la red del operador mediante un enrutador de acceso 30. Se trata del primer enrutador que los paquetes de datos IPv6 e IPv4 encuentran cuando salen de la pasarela residencial.

15 Según la arquitectura de red adoptada a nivel del enrutamiento IPv6, el enrutador de acceso 30 puede anunciar en dirección aguas arriba de la red (es decir hacia la red 1 del proveedor de servicio de conectividad IP) los prefijos IPv6 que enruta, es decir los prefijos IPv6_prefix_ports_range e IPv6_prefix_native de las pasarelas residenciales a las que sirve.

20 El enrutador de acceso 30 obtiene los prefijos IPv6 de las pasarelas residenciales a las que sirve de forma completamente clásica en un entorno de red IPv6. Pueden mencionarse dos métodos que se describen a continuación:

25 1- recibe los anuncios de enrutamiento IPv6 de las pasarelas residenciales a las que sirve (IPv6_prefix_ports_range e IPv6_prefix_native); a tal efecto, cada pasarela residencial anuncia sus prefijos hacia aguas arriba (IPv6_prefix_ports_range e IPv6_prefix_native); o

30 2- obtiene los diferentes IPv6_prefix_ports_range e IPv6_prefix_native mediante delegación de prefijos como se describe en el documento RFC 3633 (*IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*).

En relación con la figura 2, se presenta ahora un ejemplo de constitución de un prefijo de direcciones IPv6 construidas de acuerdo con la invención, tal como el prefijo IPv6_prefix_ports_range asignado a la pasarela residencial 20.

35 Este prefijo IPv6 engloba los bits de la dirección IPv4 pública Shared_@IPv4 y el intervalo de números de puerto autorizados (ports_pattern/length_of_unvariable) para la pasarela 20 y permite, de forma unívoca, enrutar el paquete IPv6 entrante a la pasarela residencial destinataria. Se trata de un prefijo IPv6 que es enrutable en una red IPv6. Podría enrutarse incluso a Internet IPv6, si se seleccionara que fuera un prefijo que se inscribe en el prefijo del operador de red que suministra a la pasarela residencial (particularmente si estaba anunciado en BGP (*Border Gateway Protocol*)). De acuerdo con el ejemplo de la figura 2, este prefijo comprende de izquierda a derecha:

45 - el prefijo IPv6 asignado al nodo de acceso 40: prefijo IPv6/IPv4_Access_Node_prefix; de forma ventajosa, este prefijo se selecciona de tal manera que se inscriba en el prefijo de operador IPv6 IPv6-prov asignado al proveedor de servicio de conectividad IP por su RIR (*Regional Internet Registry*) y, por lo tanto, que comprenda este prefijo de operador en sus primeros bits:

50 - los bits IPv6/IPv4_Access_Node_Service que identifican en el operador el servicio de interconexión IPv6/IPv4_Access_Node de acuerdo con la presente invención; la secuencia compuesta por los bits del prefijo de operador seguidos por los bits IPv6/IPv4_Access_Node_Service compone el prefijo IPv6/IPv4_Access_Node_Service_prefix que identifica al servicio;

55 - bits complementarios que identifican un nodo de acceso particular IPv6/IPv4_Access_Node que sirve a la pasarela residencial; por razones de distribución de la carga (o *Load-balancing*), el prefijo IPv6/IPv4_Access_Node_prefix puede no ser específico para un único nodo de acceso;

- los 32 bits de la dirección Shared_@IPv4 de la pasarela 20;

60 - de forma opcional, 8 bits reservados, ajustados a 0; este octeto puede servir para realizar la distinción entre los diferentes tipos de puertos (UDP, TCP, SCTP, etc.) Tomaría el valor "X" para el procesamiento UDP e "Y" para el procesamiento "TCP", etc.

65 - Los 16 bits que representan el intervalo de números de puerto autorizados para la pasarela o "ports_pattern", con una parte invariable a la izquierda en estos 16 bits (bits de mayor peso), de longitud length_of_unvariable, que es significativa; se observará que, en el caso en el que la dirección IPv4 de la pasarela 20 no es compartida por varias pasarelas residenciales, el intervalo de números de puerto autorizados es de tamaño máximo e idéntico para todas

las pasarelas.

La longitud del prefijo IPv6_prefix_ports_range se establece de la siguiente manera:

- 5 [128 - 16 (longitud de una dirección IPv6 - dirección de codificación de un puerto) = 112 bits Más length_of_unvariable (longitud de los bits invariables que representan el intervalo de puertos fuente autorizados).]

10 Se observará que el prefijo IPv6_prefix_ports_range constituido de acuerdo con la invención es más largo que los prefijos recomendados por el estándar IPv6 para un despliegue IPv6. Sin embargo, esto no impide que sea conforme a los estándares IPv6.

15 El dominio IPv6 1 presentado en relación con la figura 1 comprende al menos un nodo de acceso 40 de acuerdo con la invención. Se observará que éste puede comprender varios nodos más. El nodo de acceso 40 IPv6/IPv4_Access_Node es un enrutador particular *Dual-Stack* (IPv4 e IPv6), es decir que implementa a la vez los protocolos IPv4 e IPv6.

20 En la red 1, el nodo de acceso 40 IPv6/IPv4_Access_Node está típicamente situado aguas arriba del o de los enrutadores de acceso 30 (por lo tanto hacia el núcleo de la red o en un segmento de interconexión con redes adyacentes), como se representa en la figura 1. Dicho nodo de acceso también se denomina nodo de interconexión.

25 El procedimiento de recepción de un paquete de datos IPv6 en el dominio IPv6 se describirá a continuación en relación con la figura 3. De forma ventajosa, es realizado por un dispositivo de recepción comprendido en una pasarela residencial conectada al dominio IPv6, tal como la pasarela 20 y está destinado a tratar tanto paquetes procedentes de la red residencial 2 como paquetes de datos procedentes del dominio IPv4 3. Dicho procedimiento comprende una etapa R1 de identificación de la dirección de destino IPv6 como del tipo dirección de destino IPv6 nativa, o como del tipo de dirección de destino IPv6 construida mediante concatenación de un prefijo de nodo de acceso, de una dirección IPv4 de destino y de un número de puerto IPv4 de destino. Se supone, en este caso, que la pasarela 20 ha obtenido este prefijo previamente, por ejemplo mediante configuración.

30 Éste comprende a continuación una etapa R2 de puesta en conformidad de una dirección del paquete de datos: En el sentido red residencial hacia un dominio IPv6, se trata de la dirección fuente del paquete; en el sentido dominio IPv6 hacia una red residencial, se trata de su dirección de destino. Dicha puesta en conformidad puede conllevar una modificación del paquete de datos. El paquete de datos modificado es enrutado a continuación en R3 a su destino.

35 De acuerdo con una primera realización de la invención, se considera el establecimiento de una llamada saliente hacia un destinatario IPv4 que puede ser, por ejemplo, un servidor Web IPv4 localizado en la red Internet. Un terminal del usuario de la red residencial 2, por ejemplo el PC IPv6. 22 conectado a la pasarela 20, emite un paquete de datos destinado a este interlocutor del dominio IPv4 3. En este caso, la aplicación implementada en el PC es un navegador (*browser*) IPv6. Se recuerda que el terminal del usuario fuente 22 es puramente IPv6.

40 Se distinguen varios casos:

45 - el terminal del usuario 22 emite un paquete de datos IPv6 con ayuda de una dirección fuente igual a una dirección IPv6 construida que le ha sido asignada; o

- el terminal del usuario 22 emite un paquete de datos IPv6 con ayuda de una dirección fuente igual a una dirección IPv6 nativa que le ha sido asignada.

50 Se entiende que el paquete de datos comprende una dirección de destino IPv6 correspondiente al destinatario IPv4 que el terminal debe haber recuperado previamente.

55 El navegador del terminal 22 necesita, por lo tanto, conocer la dirección IPv6 del servidor Web destinatario. Ahora bien, el servidor Web solamente es accesible en IPv4. Es preciso, por lo tanto, que el terminal 22 disponga de una dirección IPv6 que considerará como la dirección del servidor Web (mientras que en realidad el servidor Web solamente dispone de una dirección IPv4).

60 Para ello, una función de traducción de una dirección IPv4 del servidor Web a una dirección IPv6 debe ser implementada por el proveedor de servicio de conectividad IP o por una tercera parte. Esta función de traducción debe respetar un formalismo de construcción de la dirección IPv6 de tal manera que contenga la dirección IPv4 del correspondiente (el servidor Web en nuestro ejemplo). Esta función de traducción se describirá ahora en relación con la figura 4.

65 Dicha función de traducción que llamaremos DNS_IPv4toIPv6 puede ser realizada, por ejemplo, por el nodo de acceso 40 IPv6/IPv4_Access_Node del dominio IPv6 1 pero, de forma más general, se considera que es realizada por un servidor DNS del dominio 1. La función DNS_IPv4toIPv6 es el punto de contacto por defecto para cualquier

petición de resolución DNS emitida por un terminal solicitante. Por defecto, esta función examina en primer lugar los registros IPv6 de tipo "AAAA", dicho de otro modo las direcciones IPv6 nativas. Si un registro ya está presente, una respuesta es entonces emitida hacia el terminal solicitante. Si no está presente ningún registro, una petición de resolución de tipo "A" es realizado entonces por la función de traducción DNS_IPv4toIPv6. En la recepción de la respuesta de un servidor DNS que comprende la dirección IPv4 del interlocutor (el servidor Web en nuestro ejemplo), la función DNS_IPv4toIPv6 transforma la dirección IPv4 recibida en la respuesta en dirección IPv6, según el formalismo presentado en relación con la figura 4 y guarda esta información en su cache.

Se observará que el ejemplo de la figura 4 solamente es una realización, siendo lo esencial que la dirección IPv4 del interlocutor (en este caso el servidor Web) esté inscrita en una dirección IPv6. Si no es recibida ninguna respuesta por parte de un servidor DNS, entonces un mensaje de error es transmitido al terminal solicitante.

Llamaremos IPv6_remoteAddress_out_to_IPv4 a la dirección del destinatario (en el este caso el servidor Web) transformada de este modo en IPv6. Se observará que el terminal solicitante puede recuperar una dirección IPv6 de la máquina distante a contactar mediante otros medios, por ejemplo desde un servidor.

En todos los casos, la dirección IPv6 del interlocutor (en este caso el servidor Web) puede ser una dirección IPv6 nativa o una dirección IPv6 que respecta el formalismo introducido por la presente invención. En el caso de una dirección IPv6_remoteAddress_out_to_IPv4 construida, ésta está incluida en el prefijo IPv6/IPv4_Access_Node_Service_prefix.

En relación con la figura 4, se destaca que la secuencia de 2 octetos más a la derecha está marcada como "reservada" y puesta a 0 por defecto. Este emplazamiento corresponde al de los bits de puertos en una dirección IPv6 IPv4inIPv6_dest_address para los paquetes destinados a un terminal del usuario. Está reservado para poder indicar un puerto en particular en el que el interlocutor (en este caso el servidor Web) desea recibir la llamada. Podría tratarse de un interlocutor IPv4 al que se le asignaría también una dirección IPv4 compartida entre varios interlocutores ya que no dispondría, por lo tanto, de todos los puertos disponibles.

El terminal 22 emite a continuación un paquete de datos IPv6 que comprende la dirección IPv6_remoteAddress_out_to_IPv4 como dirección de destino.

La pasarela residencial 20 de acuerdo con la invención comprende un dispositivo de recepción de un paquete de datos de acuerdo con la invención. En la recepción de este paquete IPv6, dicho dispositivo es apto para realizar el procedimiento de transmisión de un paquete IPv6 con destino en una dirección IPv6 que representa una máquina conectada a un dominio IPv4 de acuerdo con la primera realización de la invención, que se describirá a continuación en referencia a la figura 5.

Dicho procedimiento emplea la etapa R1 de identificación de la dirección de destino IPv6 descrita anteriormente.

De acuerdo con un aspecto de la invención, la pasarela residencial 20 conoce la longitud del prefijo IPv4_Access_Node_Service_prefix, para determinar fácilmente su valor tomando los bits correspondientes en su IPv6_prefix_ports_range. Dicha identificación consiste en clasificar como una dirección construida una dirección IPv6 de destino que se inscribe en el prefijo IPv6/IPv4_Access_Node_Service_prefix y en considerar todas las direcciones fuera de este prefijo como direcciones nativas.

Una ventaja de esta identificación es que es sencilla.

Este método de identificación solamente es válido, sin embargo, en el contexto de un solo operador. Para un despliegue a gran escala con mutualización de nodos de interconexión entre los dominios IPv4 e IPv6, este método ya no es apropiado.

Dicha identificación puede consistir en buscar en la dirección de destino un identificador o "tag", cuyo valor puede ser representativo de una dirección nativa o de una dirección construida. Como ejemplo, como se indica en la figura 4, dicho identificador puede tener una longitud de un solo bit ADDR_TYPE_TAG, con un valor de 0 ó 1 para indicar que se trata de una dirección nativa o construida. El identificador ADDR_TYPE_TAG puede estar situado, por ejemplo, al comienzo de la dirección IPv6 construida para facilitar las operaciones de lectura, o también entre el IPv6/IPv4_Access_Node_Service_prefix y la dirección IPv4.

Una ventaja del identificador ADDR_TYPE_TAG es que permite una mutualización de los equipos de interconexión IPv4-IPv6 entre varios operadores y, por lo tanto, una distribución de los costes. De este modo, un operador Oi puede asegurar la interconexión IPv4-IPv6 para una región Ri (con un conjunto de prefijos IPv4 Pi). Para los otros operadores Oj, solamente las direcciones construidas por un operador Oi (sobre la base de los prefijos IPv4) son visibles, por medio de anuncios BGP.

Se entiende bien que pueden existir otros prefijos diferentes del IPv6/IPv4, pero no se utilizan para proporcionar este servicio de conectividad y el procesamiento que se les aplica es el de un paquete IPv6 nativo, es decir que es

enrutado directamente hacia el enrutador de acceso IPv6 30;

Si la dirección IPv6 de destino se clasifica como construida, el procedimiento de transmisión de acuerdo con la invención realiza una etapa R2 de puesta en conformidad de la dirección fuente del paquete a transmitir.

5 En esta primera realización de la invención, dicha puesta en conformidad consiste en identificar en R₂₁ si la dirección fuente es una dirección construida o nativa. Una dirección se considera como construida si se trata de una dirección IPv6 fuente que se inscribe en el prefijo IPv6/IPv4_Access_Node_Service_prefix, estando todas las direcciones fuera de este prefijo consideradas como direcciones fuente nativas. Si se utiliza el identificador ADDR_TYPE_TAG, entonces una dirección se identifica como construida si el identificador ADDR_TYPE_TAG está situado en "1".

Si la dirección fuente es construida, el paquete de datos es enrutado hacia su destino en R3.

15 Si la dirección IPv6 fuente se clasifica como nativa, el procedimiento de acuerdo con la invención emplea, previamente a esta etapa de enrutamiento, una etapa R₂₂ para seleccionar una dirección IPv6 fuente construida cuyo número de puerto fuente está en el intervalo autorizado ports_pattern/length_of_unvariable asignado a la pasarela 20 y para modificar el paquete de datos sustituyendo la dirección fuente nativa por esta dirección construida. En R₂₄, el procedimiento de acuerdo con la invención crea una entrada en la tabla de traducción de direcciones de la pasarela, comprendiendo dicha entrada una asociación de la dirección fuente nativa y de la dirección fuente construida de este modo.

20 De forma ventajosa, el procedimiento de acuerdo con la invención puede verificar además en R₂₃ una concordancia del número de puerto fuente contenido en la dirección fuente construida con el número de puerto fuente de nivel de transporte del paquete de datos. En relación con la figura 6, se ve que dicha creación consiste en tomar una dirección IPv6 cualquiera de 128 bits comprendida en el IPv6_prefix_ports_range y en volver a copiar, en los 16 bits de la derecha, los bits del puerto fuente utilizado (el puerto TCP o UDP del paquete IPv6 recibido del terminal 22) en el paquete de datos a transmitir.

30 Se entenderá que esta etapa es necesaria para que el nodo de acceso IPv6/IPv4 40 pueda traducir el paquete de datos IPv6 a un paquete de datos IPv4 antes de enrutarlo hacia el dominio IPv4 destinatario. Ésta presenta otra ventaja en el caso en el que la dirección IPv4 asignada a la pasarela residencial 20 es una dirección compartida por varias pasarelas residenciales del dominio IPv6 1. En efecto, como se ha mencionado anteriormente, la pasarela residencial 20 solamente puede utilizar los números de puerto fuente que pertenezcan a un intervalo de números de puerto restringido que le ha sido reservado.

35 Se observará también que, si la pasarela residencial 20 ha restringido correctamente el puerto fuente para que esté en el intervalo de números de puerto autorizados ports_pattern/length_of_unvariable, entonces la dirección fuente construida:

40 - está inscrita en el prefijo IPv6_prefix_ports_range; y

- sus 16 últimos bits son idénticos al número de puerto fuente del paquete IPv6 recibido del terminal por la pasarela;

45 En lo sucesivo, llamaremos IPv6_address_source_ports_range a la dirección fuente IPv6 formada de este modo.

En R3, el paquete IPv6 que comprende la dirección IPv6 fuente restringida IPv6_address_source_ports_range es enrutada a continuación hacia el enrutador de acceso IPv6 30 que sirve a la pasarela.

50 El enrutador de acceso IPv6 30 verifica que la dirección fuente IPv6 IPv6_address_source_ports_range está correctamente autorizada para la pasarela residencial 20. Verifica, en otras palabras, que no haya "spoofing", es decir que la pasarela residencial 20 emita correctamente paquetes IPv6 en su prefijo IPv6_prefix_ports_range autorizado. Para ello, el enrutador de acceso IPv6 30 verifica que la dirección fuente IPv6 IPv6_address_source_ports_range del paquete IPv6 recibido por la pasarela 20 esté correctamente inscrita en el prefijo IPv6_prefix_ports_range asignado a esta pasarela residencial. Esta verificación se realiza de forma clásica de acuerdo con un principio ya utilizado para el tráfico IPv6 nativo.

55 Si esta verificación es positiva, el enrutador de acceso IPv6 30 enruta el paquete IPv6 hacia su destino.

60 Ya que la dirección IPv6 de destino se inscribe en el prefijo IPv6/IPv4_Access_Node_prefix que caracteriza el nodo de acceso IPv6/IPv4_Access_Node 40 al dominio IPv6, el paquete de datos es enrutado hacia este nodo de acceso. Se supone, por ejemplo, que dicho nodo está situado en el dominio IPv6 1 más cercano del o de los dominios IPv4 al que sirve, para optimizar el enrutamiento de los paquetes de datos hacia estos dominios, pero la invención no se limita a dicha situación del nodo de acceso 40, pudiendo estar situado dicho nodo de acceso en cualquier lugar en el dominio 1.

65 En la recepción del paquete IPv6, el nodo de acceso IPv6/IPv4_Access_Node 40 enruta el paquete de datos saliente

a su destino en un dominio IPv4 de la siguiente manera:

- extrae una dirección de destino IPv4 y de un puerto de destino de la dirección de destino IPv6 y una dirección fuente IPv4 y de un puerto fuente de la dirección fuente IPv6;

5 - traduce a continuación el paquete IPv6 en un paquete IPv4 que tiene las siguientes características:

- su dirección fuente IPv4 es la dirección IPv4 Shared_@IPv4 de la pasarela residencial 20. Es esta dirección Shared_@IPv4 la que verá el destinatario del paquete de datos IPv4 transmitido (el servidor Web). Como recordatorio, esta dirección IPv4 Shared_@IPv4 está incluida en el prefijo IPv6_prefix_ports_range y, por lo tanto, en la dirección IPv6 fuente IPv6_address_source_ports_range. En relación con la figura 8, la dirección IPv4 Shared_@IPv4 puede extraerse de los bits 24 a 55;

10

- su dirección de destino IPv4 es la dirección IPv4 del interlocutor. En relación con la figura 4, la dirección IPv4 del destinatario puede extraerse de los bits 24 a 55 de la dirección IPv6_remoteAddress_out_to_IPv4 del paquete de datos IPv6 recibido por el nodo de acceso 40;

15

- el valor del número de puerto fuente del paquete de datos IPv4 traducido es el número del puerto fuente del paquete IPv6 recibido;

20

- el número de puerto de destino del paquete de datos IPv4 traducido es el mismo que el del paquete IPv6;

- la parte útil del paquete IPv6 es la parte útil del paquete IPv4 traducido;

25 se observará que los campos de la cabecera del paquete IPv6 se traducen a campos IPv4 correspondientes de forma clásica, por ejemplo de acuerdo con los principios del estándar NAT-PT (*Network Address Translation-Protocol Translation*)

- enruta finalmente el paquete IPv4 traducido hacia su destinatario (el servidor Web IPv4 en nuestro ejemplo).

30 Se entiende que, cuando la dirección IPv4 asignada a la pasarela residencial 20 es una dirección pública compartida entre varias pasarelas, es necesario que el número de puerto fuente contenido en la dirección IPv6 fuente construida del paquete de datos recibido pertenezca correctamente al intervalo de números de puerto reservados a esta pasarela. En efecto, si este no fuera el caso, el nodo de acceso podría traducir el paquete IPv6 a transmitir en un paquete de datos IPv4, pero los eventuales paquetes de respuesta emitidos por el destinatario no llegarían a la pasarela residencial.

35 De forma ventajosa, el nodo de acceso 40 controla la pertenencia del puerto fuente al intervalo de números de puerto fuente asignado a la pasarela 20. Dicha etapa consiste en controlar que los últimos 16 bits de la dirección fuente IPv6 del paquete sean idénticos a los 16 bits del puerto fuente en el campo correspondiente TCP o UDP del paquete IPv6. Se trata de un control indirecto, que puede realizarse después de la verificación por el enrutador de acceso de que la pasarela residencial ha enviado correctamente un paquete cuya dirección fuente está en su prefijo. Al finalizar estas dos etapas, puede ser cierto que la pasarela residencial 20 ha emitido correctamente un paquete de datos que comprende un puerto fuente incluido en su intervalo de puertos autorizados y no ha utilizado el de otra pasarela residencial.

40 De acuerdo con una segunda realización de la invención, se considera el caso de un paquete de datos IPv4-in-pt que entra en un dominio IPv6 procedente de un dominio IPv4 y destinado a un terminal del usuario del dominio IPv6 1, por ejemplo el terminal 21. El terminal se sitúa detrás de la pasarela residencial 20 que dispone de una dirección IPv4 @IPv4 o Shared_@IPv4 y de un intervalo de puertos autorizados ports_pattern/length_of_unvariable.

45 El paquete IPv4-in-pt entrante, si está destinado al terminal del usuario 21 de la red residencial de la pasarela residencial 20, comprende una dirección de destino IPv4 igual a Shared_@IPv4 y un puerto de destino que se inscribe en el intervalo de números de puerto autorizados ports_pattern/length_of_unvariable de la pasarela residencial 20.

50 Como se ha mencionado anteriormente en relación con la figura 2, la dirección Shared_@IPv4 y el intervalo de números de puerto ports_pattern/length_of_unvariable se encuentran en el prefijo IPv6_prefix_ports_range de la pasarela residencial 20.

60 El paquete IPv4-in-pt es recibido por el nodo de acceso 40. En efecto, en una etapa previa, el proveedor de conectividad IP ha anunciado a los dominios IPv4 con los que tiene una interfaz, las direcciones IPv4 asignadas a pasarelas residenciales del dominio 1 a cuyo destino tenía el encargo de enrutar los paquetes IPv4. Ha realizado este anuncio, por medio del propio nodo de acceso 40 o de un ASBR (*Autonomous System Border Router*) de acuerdo con una técnica conocida por el especialista en la técnica.

65

El paquete IPv4-in-pt comprende una dirección de destino @IPv4 o shared@IPv4 gestionada por el nodo de acceso 40 y un puerto de destino dest-port. El nodo de acceso 40 es apto para construir una dirección de destino IPv6 IPv4inIPv6_dest_address mediante concatenación de un prefijo IPv6/IPv4_Access_Node_prefix del nodo de acceso 40, de dicha dirección de destino IPv4 shared-@IPv4 y del número de puerto de destino dest-port, como se describe en relación con la figura 7.

El número de puerto de destino dest-port es insertado en la parte derecha de la dirección de destino IPv6 construida. Éste inserta, por lo tanto, a la vez los 32 bits de la dirección IPv4 de destino del paquete IPv4 recibido y los 16 bits del puerto de destino dest-port para construir una dirección IPv6 de destino construida que llamaremos IPv4inIPv6_dest_address.

El nodo de acceso 40 genera a continuación un paquete de datos IPv6 IPv4inIPv6-pt a partir de la dirección de destino IPv6 IPv4inIPv6_dest_address construida y del paquete de datos IPv4 recibido. Una realización consiste en traducir el paquete IPv4 recibido a un paquete IPv6:

- cuya dirección fuente IPv6 es una de las direcciones IPv6 de las que dispone el propio IPv6/IPv4_Access_Node 40 (para una de sus interfaces); y

- cuya dirección de destino IPv6 es la dirección IPv4inIPv6_dest_address.

Otra realización consiste en traducir el paquete IPv4 IPv4-in-pt recibido en un paquete IPv6 al que se le asocia la dirección IPv6 construida después de haber extraído previamente del paquete IPv4 recibido su dirección IPv4 de destino, su puerto de destino, su dirección IPv4 fuente y su puerto fuente.

El paquete de datos IPv6 IPv4inIPv6-pt generado con ayuda de la dirección de destino IPv6 construida es enrutado al dominio IPv6 1. El paquete IPv4inIPv6-pt pasa, por lo tanto, por el núcleo de enrutamiento IPv6 del nodo de acceso 40 IPv6/IPv4_Access_Node.

Mediante construcción, su dirección de destino IPv4inIPv6_dest_address se inscribe en el prefijo IPv6_prefix_ports_range de la pasarela residencial 20. El paquete IPv4inIPv6-pt es enrutado hacia la interfaz del nodo de acceso IPv6/IPv4_Access_Node 40 que sirve a la ruta IPv6 correspondiente hacia la pasarela residencial 20.

Se observará que si la dirección de destino IPv4inIPv6_dest_address no se inscribiera en ningún prefijo IPv6_prefix_ports_range (o ningún prefijo que lo englobe), el paquete sería destruido de un momento a otro en la ruta, ya que no podría ser enrutado hacia ningún prefijo IPv6_prefix_ports_range y, por lo tanto, hacia ninguna pasarela residencial.

Si la dirección de destino IPv4inIPv6_dest_address se inscribe correctamente en el prefijo IPv6_prefix_ports_range, el paquete IPv4inIPv6-pt llega al enrutador_de acceso_dual_stack 30 que sirve a la pasarela residencial 20 que alberga al terminal del usuario 21 en su red residencial 2. Es enrutado por el enrutador_de acceso_dual_stack 30 hacia la pasarela residencial, que conoce la ruta hacia el prefijo IPv6_prefix_ports_range.

De acuerdo con esta segunda realización de la invención, la pasarela residencial 20 comprende un dispositivo que emplea el procedimiento de recepción del paquete de datos IPv4inIPv6-pt de acuerdo con la invención. Dicho procedimiento se describirá a continuación en relación con la figura 8.

Cuando el paquete IPv4inIPv6-pt llega a la pasarela residencial 20, ésta realiza la etapa R'1 de identificación de la dirección de destino descrita anteriormente.

Si una dirección de destino nativa es identificada, el paquete de datos es enrutado directamente hacia el terminal del usuario destinatario, en una etapa R'3.

Si una dirección de destino construida es identificada, por ejemplo con ayuda de un identificador comprendido en la dirección de destino, la etapa de puesta en conformidad del procedimiento de recepción de un paquete de datos de acuerdo con la invención comprende una etapa R'21 de búsqueda en la tabla de traducción de la pasarela residencial de una entrada que comprende la dirección de destino construida. Si esta búsqueda es positiva, dicha entrada asocia a la dirección de destino construida una dirección de destino nativa IPv6_address_native-UE del terminal destinatario. En R'23, el procedimiento de acuerdo con la invención sustituye la dirección de destino construida por esta dirección nativa en el paquete de datos IPv6. Esta sustitución es particularmente ventajosa en el caso en el que el paquete de datos IPv4-in-pt forma parte de una respuesta a un paquete de datos emitido previamente por el terminal destinatario 21 con su dirección fuente IPv6 nativa, y para el que la pasarela había almacenado, en efecto, previamente esta dirección nativa en su tabla de NAT antes de su transmisión, como se describe en la realización anterior de la invención. En ese momento, había creado la entrada en su tabla de traducción y sustituido esta dirección nativa por la dirección construida del terminal 21, para permitir al nodo de acceso 40 extraer de ella una dirección fuente IPv4 durante la transformación del paquete IPv6 saliente en un paquete IPv4.

De forma ventajosa, la etapa de puesta en conformidad comprende además una etapa R'22 de verificación de una concordancia del puerto de destino de nivel de transporte del paquete de datos con el número de puerto de destino contenido en la dirección de destino del paquete. Si los dos números de puerto no concuerdan, el paquete es rechazado. Esto no debe tener lugar si la traducción ha sido realizada por el nodo de acceso, pero esta etapa puede utilizarse para realizar un control del flujo procedente del nodo de acceso.

En R'3, el paquete de datos es enrutado por la pasarela hacia el terminal destinatario de su red residencial.

En el ejemplo descrito en relación con la figura 1, la pasarela residencial 20 de acuerdo con la invención comprende un dispositivo 25 de recepción de un paquete de datos en un dominio IPv6, que se describirá ahora en relación con la figura 10. Éste comprende los elementos materiales que se encuentran de forma clásica en un ordenador convencional o un enrutador especializado, a saber un procesador 25₁, una memoria viva de tipo RAM 25₂. Una memoria muerta de tipo ROM 25₃ y medios 25₄ de telecomunicaciones con la red 1.

De acuerdo con la invención, el dispositivo 25 comprende una memoria 25₅ que comprende una base de datos en la que se almacena una tabla de traducción de direcciones o NAT entre el dominio 1 y su red residencial 3.

Se observará que esta memoria también puede ser externa al dispositivo 25 siempre que éste pueda acceder a ella.

La memoria muerta 25₅ constituye un soporte de registro de acuerdo con la invención. Este soporte memoriza el programa informático de acuerdo con la invención. Este programa comprende instrucciones para la ejecución de las etapas del procedimiento de recepción de un paquete entrante de acuerdo con la invención que acaba de describirse en referencia a las figuras 3, 5 y 8.

Se observará también que el dispositivo de recepción también puede estar incluido en un terminal del usuario conectado directamente a la red 1 del proveedor de servicio de conectividad.

En resumen, la invención permite una segunda fase de migración de los servicios de conectividad IP a IPv6 con ayuda de mecanismos de enrutamiento de los paquetes que tienen en cuenta los siguientes hechos:

- La migración final a IPv6 requeriría varios años (una escala de 10 años mínimo). Esto se debe principalmente al gran número de actores a "convencer" para un pase a IPv6, el gran número de AS (*Autonomous System*) (más de 17000); de la diversidad de los mecanismos de interconexión. Además, debe precisarse que el problema de las direcciones solamente concierne a priori a los operadores. Los clientes no tienen ninguna razón para modificar la arquitectura de sus redes locales. Una empresa "sin identificar" no tiene motivaciones para migrar sus servidores FTP, HTTP, etc., a IPv6. Los operadores deben esperar un largo trabajo de acompañamiento para el pase a IPv6.

- Los operadores de servicios sufren un problema de agotamiento de direcciones IPv4 tal como se ha descrito en la sección más arriba.

- La simple migración a IPv6 de un dominio dado no resuelve el problema de la conectividad global (ponerse en contacto con cualquier máquina distante presente en Internet). En efecto, debe implementarse una interconexión con el mundo IPv4.

- Una solución a base de NAT-PT con estado no es recomendada. El servicio suministrado se degradaría, visto que los servicios con valor añadido vinculados al "port forwarding" configurado por los clientes no funcionarán y dependerán del comportamiento de la "caja" de interconexión entre una nube IPv4 y otra IPv6.

Los mecanismos de enrutamiento de los paquetes IP de acuerdo con la invención permiten promover la utilización del protocolo IPv6 de la siguiente manera:

- Activación de IPv6 e implementación de una solución que permite promover el tráfico IPv6 basada en una función de interconexión situada en la red, que es sin estado. La solución de la invención solamente utiliza la conectividad IPv6 de las pasarelas residenciales e implica la utilización de terminales del usuario y pasarelas residenciales IPv6. Debido a esto, estos equipos solamente están en condiciones de procesar (recibir y emitir) paquetes de datos de tipo IPv6.

La solución de la invención permite:

- que la red de acceso sea solamente IPv6 y, de este modo, que el operador de acceso no tenga que gestionar el enrutamiento IPv4 en el acceso;

- que las pasarelas residenciales no tengan ninguna noción de IPv4 y solamente gestionen IPv6;

- que los terminales de la red residencial de la pasarela residencial puedan utilizar solamente IPv6.

Una misma dirección IPv4 puede asignarse a varias pasarelas residenciales (u otros equipos en contextos diferentes del acceso a Internet residencial). Se trata de una asignación ficticia a nivel de la pasarela residencial, ya que las pasarelas residenciales no gestionan el enrutamiento IPv4. Los principios básicos son los siguientes:

- 5 - intervalo de puertos fuente autorizados a nivel de cada pasarela para las comunicaciones salientes;
- prefijo IPv6 particular IPv6_prefix_ports_range.

10 Los paquetes IPv4 entrantes en el dominio IPv6 no son encapsulados por el IPv6/IPv4_Access_Node para ser enrutados hacia la pasarela residencial, sino que son traducidos a paquetes IPv6.

15 - Para las comunicaciones salientes, su resolución DNS de un interlocutor IPv4, devolvemos al terminal del usuario iniciador una dirección IPv6 construida sobre la base de la dirección IPv4 del interlocutor. El terminal del usuario utiliza entonces esta dirección de destino IPv6 para emitir los paquetes de datos. Para emitir este paquete, puede utilizar su dirección fuente IPv6 nativa o construida.

20 - Si ha utilizado su dirección fuente nativa, la pasarela residencial transforma la dirección IPv6 nativa fuente en una dirección fuente construida IPv6 que comprende su propia dirección IPv4 compartida entre las pasarelas (Shared_@IPv4) y el puerto fuente (inscrito en el intervalo fuente autorizado).

25 - Un equipo de interconexión del dominio IPv6 con el dominio IPv4 verifica que la pasarela residencial ha utilizado correctamente su intervalo de puertos autorizados, comparando la parte de la dirección fuente que contiene los bits de puerto fuente y el puerto fuente en el campo de puerto del paquete IPv6. Traduce el paquete IPv6 a un paquete IPv4 para transmitirlo al interlocutor utilizando:

- para la dirección fuente IPv4: los bits en la dirección IPv6 fuente que contienen Shared_@IPv4;
- para la dirección de destino IPv4: los bits en la dirección IPv6 que contiene la dirección IPv4 del interlocutor.

REIVINDICACIONES

1. Procedimiento de recepción de un paquete de datos IPv6 en un dominio IPv6 interconectado con un dominio IPv4, comprendiendo dicho paquete una dirección IPv6 de destino y una dirección IPv6 fuente, implementándose dicho procedimiento en una pasarela residencial apta para conectar un terminal del usuario (21, 22) a dicho dominio IPv6, que comprende las siguientes etapas:
- identificación de una dirección IPv6 de destino construida mediante concatenación de un prefijo de operador, de una dirección de destino IPv4 y de un número de puerto de destino;
 - si fuera necesario, puesta en conformidad de al menos una dirección del paquete de datos mediante sustitución de dicha dirección, perteneciendo dicha sustitución a un grupo que comprende una sustitución de una dirección construida por una dirección nativa de dicho terminal del usuario (21, 22) y una sustitución de una dirección nativa de dicho terminal del usuario (21, 22) por una dirección construida, y modificación del paquete de datos con ayuda de la dirección puesta en conformidad; y
 - enrutamiento del paquete de datos modificado hacia su destino.
2. Procedimiento de recepción de acuerdo con la reivindicación 1, caracterizado por que, cuando el paquete de datos procede de dicho terminal del usuario y está destinado al dominio IPv4, la etapa de puesta en conformidad de la dirección fuente comprende además las siguientes etapas:
- identificación de una dirección IPv6 fuente nativa;
 - creación de una entrada en una tabla de traducción de direcciones, asociando dicha entrada, dicha dirección fuente nativa a una dirección fuente construida mediante concatenación de un prefijo de operador, de una dirección IPv4 asignada a la pasarela y de un número de puerto fuente que pertenece a un intervalo de números de puerto autorizados para dicha pasarela; y
 - sustitución de la dirección fuente nativa del paquete de datos por la dirección fuente construida.
3. Procedimiento de recepción de acuerdo con la reivindicación 2, caracterizado por que la identificación de la dirección se realiza con ayuda de un identificador comprendido en la dirección de destino.
4. Procedimiento de recepción de acuerdo con la reivindicación 2, caracterizado por que comprende además una etapa de verificación de una correspondencia entre el número de puerto fuente del paquete de datos y el número de puerto fuente de la dirección fuente construida.
5. Procedimiento de recepción de acuerdo con la reivindicación 1, caracterizado por que, cuando el paquete de datos procede del dominio IPv4 y está destinado a dicho terminal del usuario, la etapa de puesta en conformidad de la dirección de destino comprende las siguientes etapas:
- búsqueda, en una tabla de traducción de direcciones de la pasarela, de una entrada que asocia a dicha dirección de destino construida una dirección de destino nativa;
 - si se ha encontrado una entrada, sustitución de la dirección de destino construida del paquete de datos por la dirección de destino nativa de la entrada.
6. Procedimiento de recepción de acuerdo con la reivindicación 5, caracterizado por que comprende además una etapa de verificación de una correspondencia entre el número de puerto de destino del paquete de datos y el número de puerto de destino contenido en la dirección de destino construida.
7. Dispositivo de recepción de un paquete de datos en un dominio IPv6 interconectado a un dominio IPv4, comprendiendo dicho paquete una dirección IPv6 de destino y una dirección IPv6 fuente, estando dicho dispositivo destinado a ser empleado en una pasarela residencial apta para conectar un terminal del usuario (21, 22) a dicho dominio IPv6, que comprende los siguientes medios
- medio de identificación de una dirección IPv6 de destino construida mediante concatenación de un prefijo de operador, de una dirección de destino IPv4 y de un número de puerto de destino;
 - medio de, si fuera necesario, puesta en conformidad de al menos una dirección del paquete de datos mediante sustitución de dicha dirección, perteneciendo dicha sustitución a un grupo que comprende una sustitución de una dirección construida en una dirección nativa de dicho terminal del usuario (21, 22) y una sustitución de una dirección nativa de dicho terminal del usuario (21, 22) en una dirección construida, y modificación del paquete de datos con ayuda de la dirección puesta en conformidad; y

- medio de enrutamiento del paquete de datos modificado hacia su destino.

8. Pasarela residencial apta para conectar terminales del usuario de una red residencial a un dominio IPv6 interconectado a un dominio IPv4, que comprende:

5 - medios de obtención de una dirección IPv4, de un intervalo de números de puerto autorizados para dicha pasarela y de un intervalo de direcciones IPv6 autorizadas para dicha pasarela, estando dicho intervalo de direcciones IPv6 construido mediante concatenación de un prefijo de operador, de dicha dirección IPv4 y del intervalo de números de puerto IPv4 autorizados; y

10 - un dispositivo de recepción de un paquete de datos IPv6 en el dominio IPv6 interconectado al dominio IPv4 de acuerdo con la reivindicación 7.

15 9. Pasarela residencial de acuerdo con la reivindicación 8, que comprende una tabla de traducción de direcciones, que comprende entradas, que asocian, para una sesión de comunicación que implica el terminal del usuario de su red residencial, al menos una dirección fuente, caracterizada por que dicha pasarela es apta para registrar en dicha entrada, una dirección IPv6 fuente construida y una dirección IPv6 fuente nativa.

20 10. Producto programa informático descargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, caracterizado por que comprende instrucciones de código de programa que, cuando son ejecutadas por un procesador, hacen que este procesador ejecute el procedimiento de recepción de un paquete de datos en un dominio IPv6 de acuerdo con la reivindicación 1.

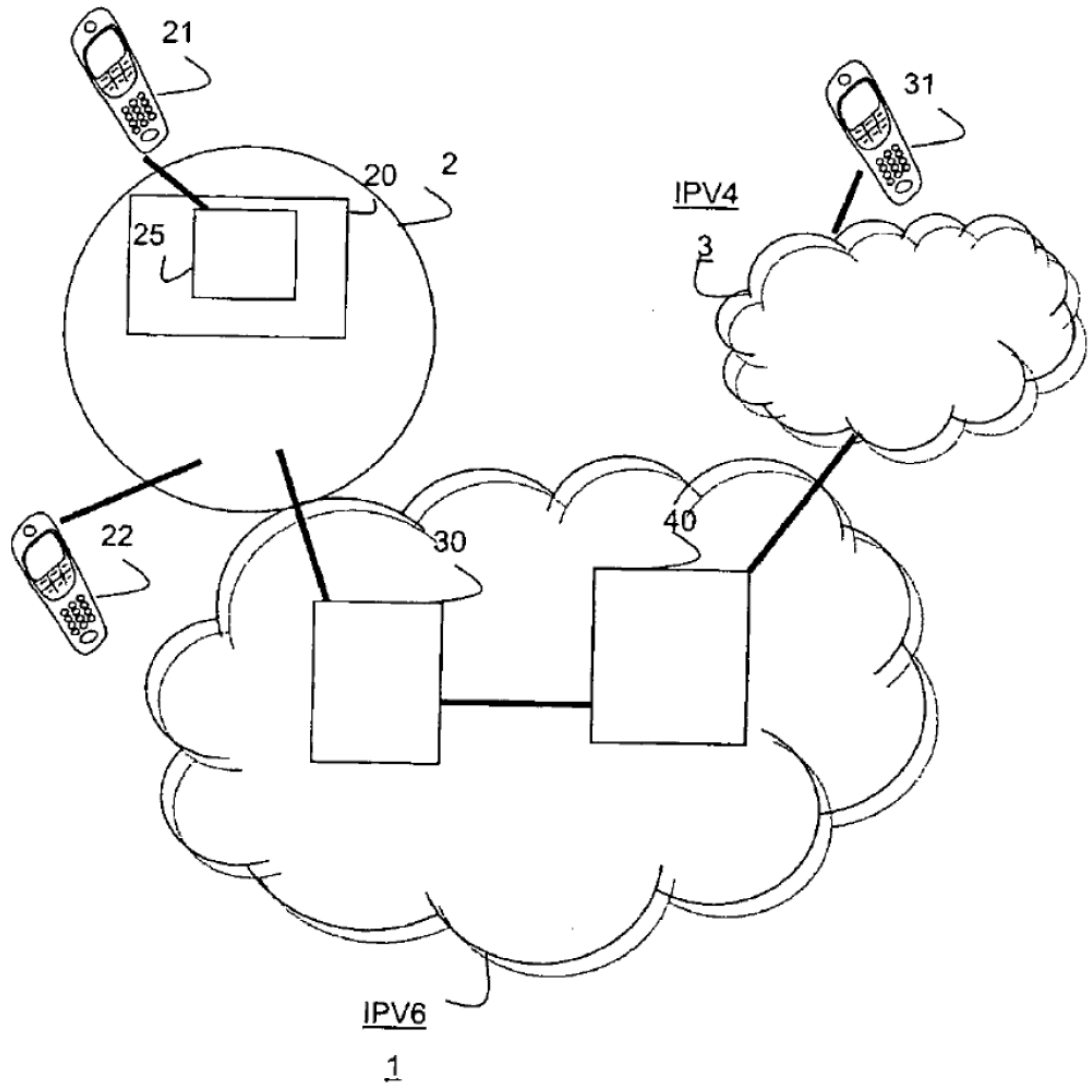


FIG. 1

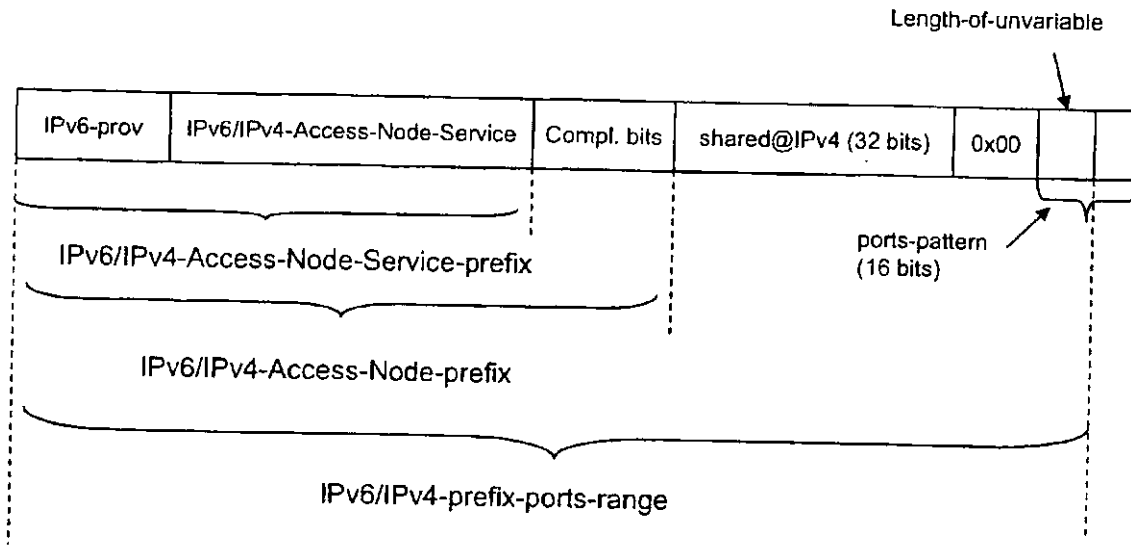


FIG. 2

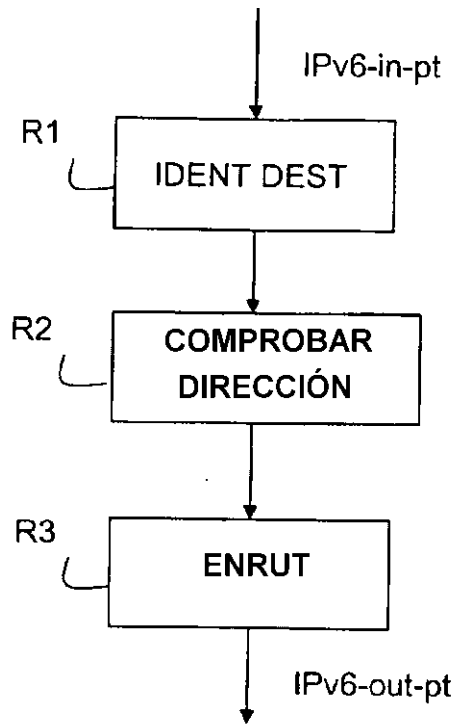


FIG. 3

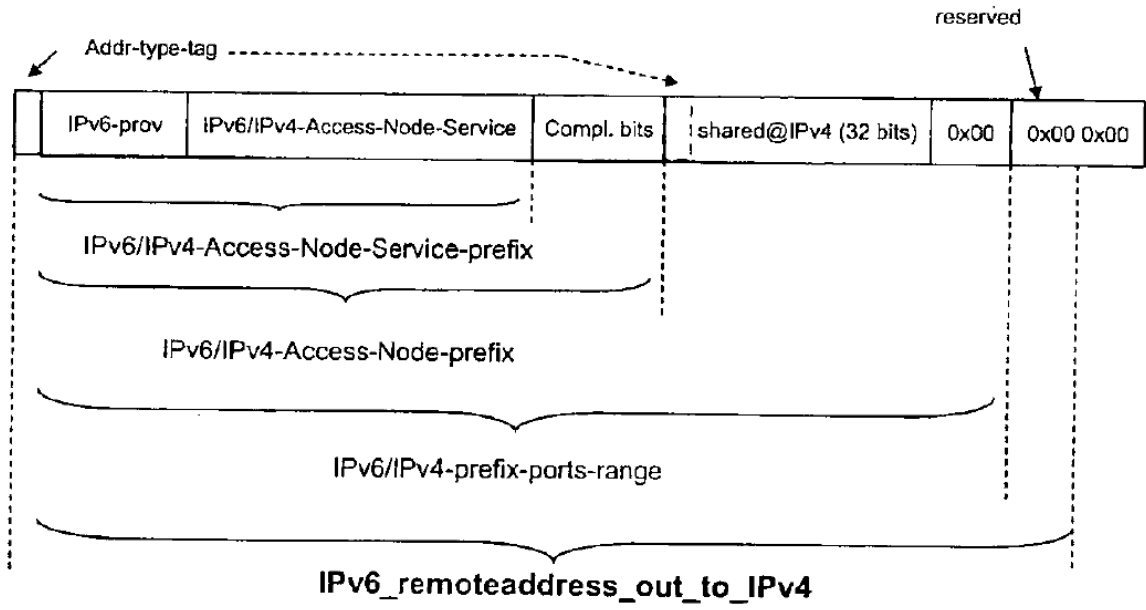


FIG. 4

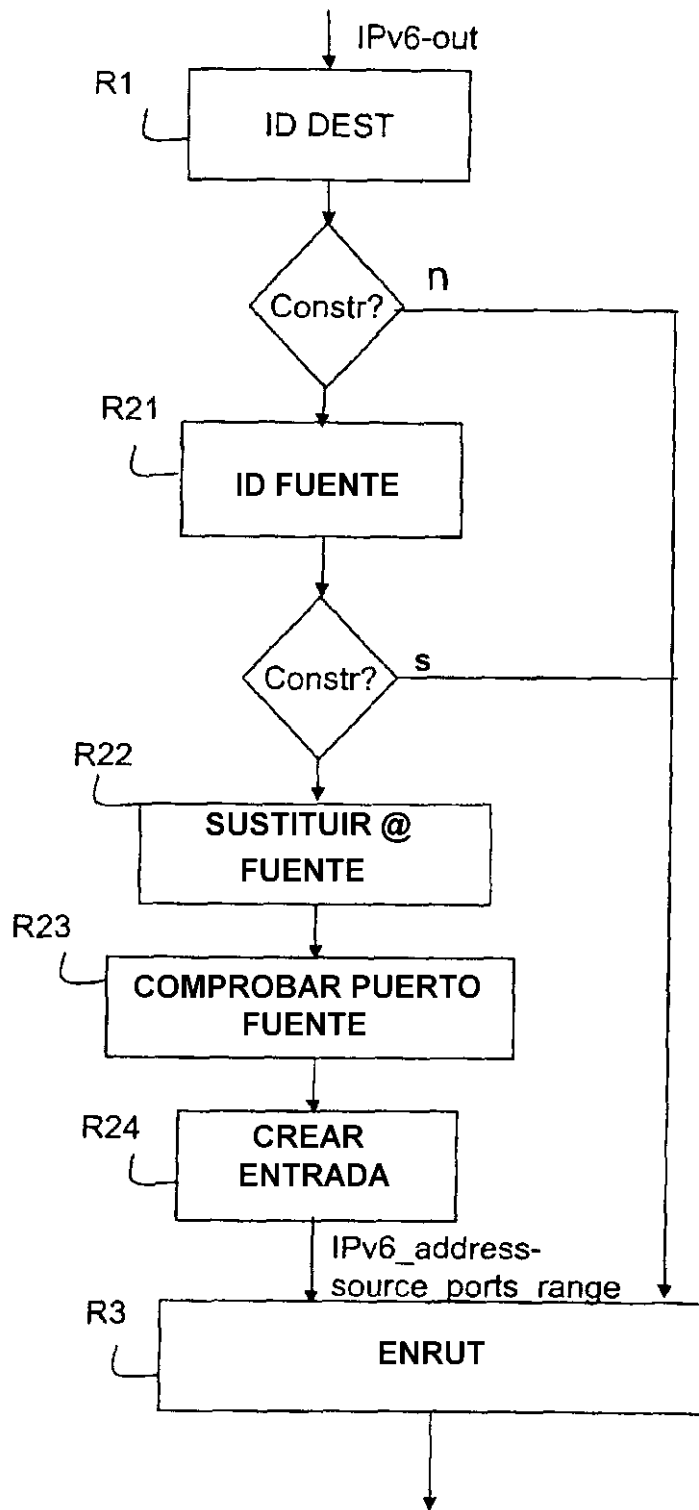


FIG. 5

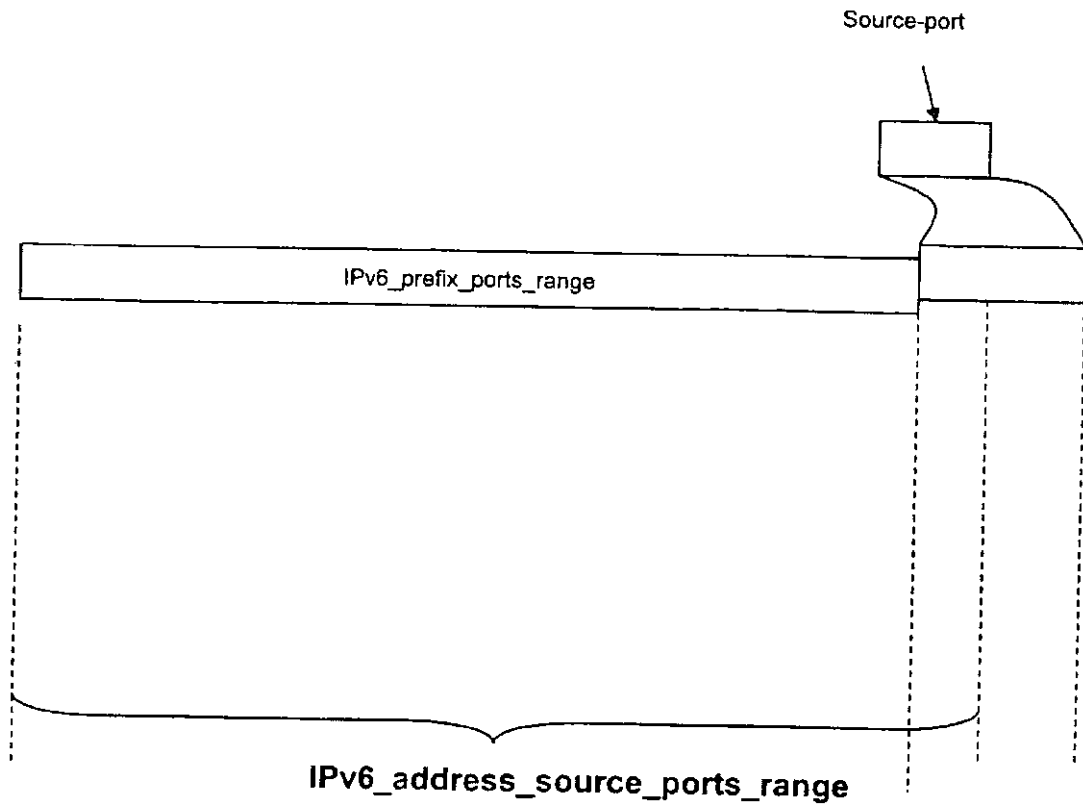


FIG. 6

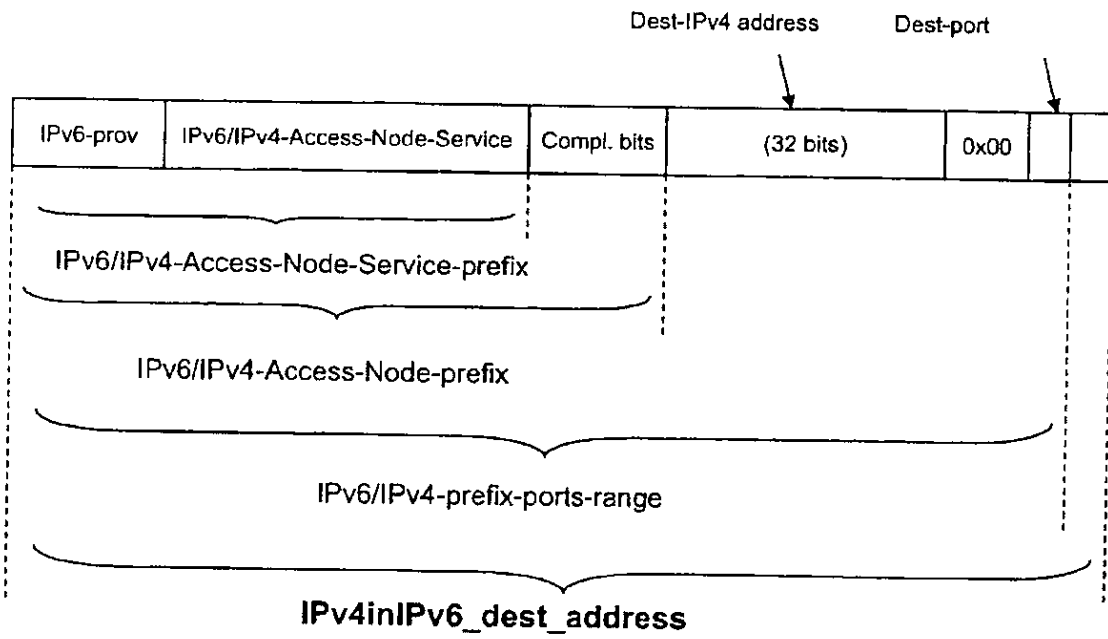


FIG. 7

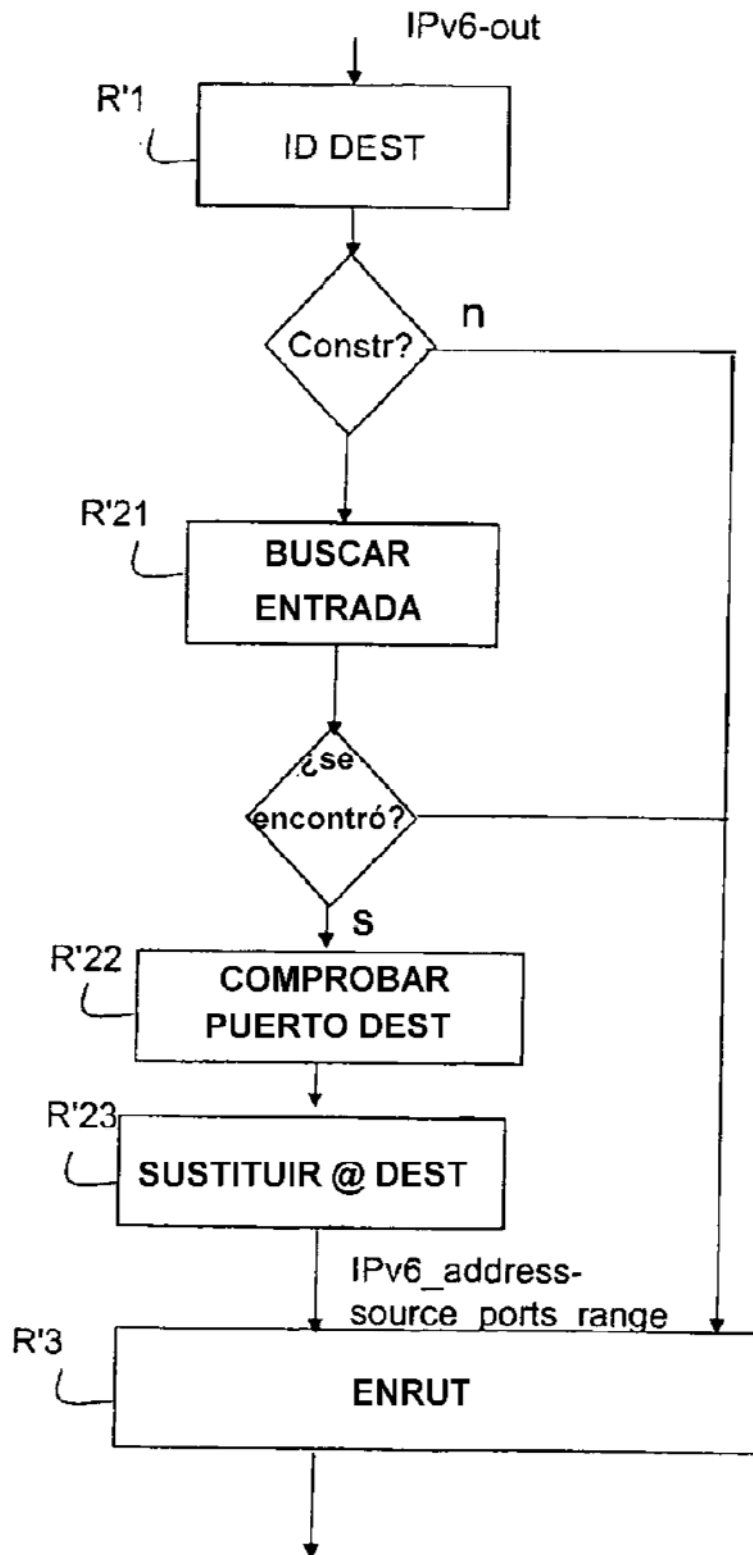


FIG. 8

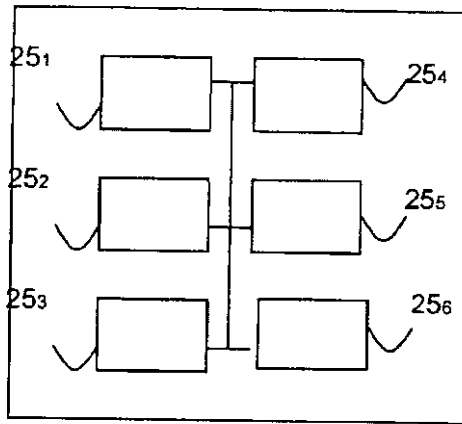


FIG. 9