(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 608 865**

(51) Int. CI.:

H04L 12/28 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.08.2008 PCT/CN2008/001529**

(87) Fecha y número de publicación internacional: **04.03.2010 WO10022535**

(96) Fecha de presentación y número de la solicitud europea: **26.08.2008 E 08783677 (1)**

(97) Fecha y número de publicación de la concesión europea: **28.09.2016 EP 2320604**

(54) Título: **Procedimiento y dispositivo para transferir un paquete en un nodo de acceso IPV6**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.04.2017

(73) Titular/es:

ALCATEL LUCENT (100.0%)
148/152 route de la Reine
92100 Boulogne-Billancourt, FR

(72) Inventor/es:

WEN, HAIBO y
LIU,GANG

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Procedimiento y dispositivo para transferir un paquete en un nodo de acceso IPV6

Campo técnico

La presente invención se refiere a un dispositivo de nodo de acceso en una red de acceso en un entorno IPv6 y, más específicamente, a un procedimiento y un aparato para reenviar paquetes en un dispositivo de nodo de acceso en una red de acceso IPv6.

Descripción de la técnica relacionada

Con la evolución de la red, el agotamiento de las direcciones IPv4, y también los más y más dispositivos en la red en locales de clientes (CPN), como la red de usuario doméstico y la red empresarial, que requieren estar habilitados para Internet, una red de acceso está comenzando su transición para soportar IPv6. Broadband Forum ha estado trabajando en la normalización para desarrollar una red de acceso de línea de abonado digital (DSL) que esté habilitada para IPv6.

Un nodo de acceso (AN) es el primer dispositivo absolutamente controlado de un operador en la red de acceso. Por lo tanto, comprobar la validez de los paquetes y eliminar los paquetes no válidos en el nodo de acceso es de vital importancia para la seguridad de la red del operador. En una red de acceso IPv4, se implementan medidas de seguridad de red tales como la anti-suplantación de direcciones IP en el AN para asegurar la red y también evitar el robo de servicio. Sin embargo, es bastante difícil implementar la anti-suplantación de direcciones IP en un entorno IPv6 de la misma manera que en el IPv4. Las razones se presentan a continuación.

1) A medida que se conectan más y más dispositivos a través de la CPN al AN del operador, deben añadirse muchos más registros para la anti-suplantación de direcciones IP al AN, lo que requerirá que el AN tenga una alta capacidad de almacenamiento y un gran rendimiento operativo y aumentar aún más el coste de construcción de los dispositivos de nodo de acceso en la red de acceso IPv6.

2) Muchos terminales de usuario en la CPN IPv6 no obtienen direcciones IPv6 desde un dispositivo de red tal como un servidor DHCPv6 del operador sino que forman una lista de direcciones IPv6 basada en un mecanismo de autoconfiguración de direcciones sin estado o mediante la interacción con un dispositivo, tal como una pasarela residencial, usando el servidor DHCPv6 local. Por lo tanto, el AN no puede obtener la lista de direcciones IPv6 usada actualmente por los terminales de usuario en la CPN actual, y mucho menos comprobar la validez de los paquetes comprobando si la dirección IPv6 de origen en cada paquete es una dirección IPv6 actualmente usada, tal como se hace en la red IPv4.

Los documentos US 7 360 245 B1 y US 2004/078485 A1 describen mecanismos de filtrado para identificar la suplantación de direcciones IP de origen en redes privadas.

Sumario de la invención

Por lo tanto, la presente invención se propone para resolver los problemas técnicos anteriores que existen durante la implementación de un control de seguridad de red, tal como la anti-suplantación de direcciones IP, en la red de acceso IPv6, como se define en las reivindicaciones adjuntas. Basándose en la presente invención, se guardan prefijos de red válidos en el dispositivo de nodo de acceso en la red de acceso IPv6, se comprueba un prefijo de red en una dirección IPv6 de origen de un paquete de la CPN y si se descubre que el prefijo de red en la dirección IPv6 de origen del paquete pertenece a los prefijos de red válidos guardados, entonces el dispositivo de nodo de acceso reenvía el paquete. Puesto que solo la parte de prefijo de red en las direcciones IPv6 se somete a una comprobación, se guarda una pequeña cantidad de información de prefijos de red válidos en el dispositivo de nodo de acceso, lo que evita que se requiera un gran espacio de almacenamiento para guardar directamente una gran cantidad de direcciones IPv6 válidas. Preferentemente, el dispositivo de nodo de acceso puede obtener automáticamente los prefijos de red válidos correspondientes a la CPN rastreando los mensajes de asignación de prefijos de red enviados a la pasarela residencial.

Breve descripción de los dibujos

Otros objetos, características y ventajas de la presente invención serán más evidentes a partir de la descripción de las realizaciones no limitantes, cuando se consideran junto con las figuras, en las que

la figura 1 ilustra una vista estructural topológica esquemática de una red de acceso IPv6 de acuerdo con una realización específica de la presente invención;

la figura 2 ilustra una vista de flujo de mensajes de un procedimiento para reenviar un paquete en un dispositivo de nodo de acceso en una red de acceso IPv6 de acuerdo con una realización específica de la presente invención;

la figura 3 ilustra un diagrama de bloques de un aparato para reenviar un paquete en un dispositivo de nodo de

acceso en una red de acceso IPv6 de acuerdo con otra realización específica de la presente invención;

la figura 4 ilustra una vista de flujo de mensajes de un procedimiento para reenviar un paquete en un dispositivo de nodo de acceso en una red de acceso IPv6 de acuerdo con otra realización específica de la presente invención;

la figura 5a ilustra una vista estructural esquemática de las opciones IA_PD en el protocolo DHCPv6; y

la figura 5b ilustra una vista estructural esquemática de las opciones IAprefix en el protocolo DHCPv6.

Los mismos o similares números de referencia indican las mismas o similares características o dispositivos de etapa (módulos) en todas las figuras.

Descripción detallada de la realización preferida

En una vista esquemática de diseño topológico de una red de acceso IPv6 de acuerdo con una realización específica de la presente invención, como se ilustra en la figura 1, un proveedor de acceso a la red (NAP) se conecta a través de un dispositivo de nodo de acceso con una o más pasarelas 31 residenciales (RGW). Cada RGW 31 se conecta con una red en locales de clientes (CPN). Los n terminales de usuario (n es un número natural que equivale a 1, 2,...) se conectan con la RGW 31 para obtener un prefijo de red o una dirección IPv6 de la RGW 31 y enviar un paquete que contiene la dirección IPv6 del terminal de usuario, como una dirección IP de origen, al NAP a través de la RGW 31. El NAP se conecta con una red de uno o más proveedores de servicios de red (NSP) a través de un dispositivo de red tal como un encaminador de borde, en el que el dispositivo de red incluye un servidor de protocolo dinámico de configuración de ordenador principal (DHCPv6), un servidor de autenticación, autorización y contabilidad (AAA), etc.

La figura 2 ilustra una vista de flujo de mensajes de un procedimiento para reenviar un paquete en un dispositivo de nodo de acceso en una red de acceso IPv6 de acuerdo con una realización específica de la presente invención. En lo sucesivo en el presente documento, la realización específica de la presente invención, como se ilustra en la figura 2, se explicará en detalle junto con la figura 1.

En primer lugar, un dispositivo 41 de nodo de acceso recibe un paquete de la RGW 31 en la etapa S21. El paquete contiene una dirección IPv6 de origen.

Opcionalmente, pueden usarse variantes de las técnicas de comunicación para la transmisión de paquetes entre el dispositivo 41 de nodo de acceso y la pasarela 31 residencial, tal como la técnica de línea de abonado digital (DSL), una conexión de fibra óptica, una conexión por cable, o técnicas de transmisión inalámbrica que se incluyen en la norma IEEE 802.16.

A continuación, el dispositivo 41 de nodo de acceso obtiene un prefijo de red en la dirección IPv6 de origen correspondiente del paquete recibido en la etapa S22.

A continuación, en la etapa S23, el dispositivo 41 de nodo de acceso evalúa si el prefijo de red en la dirección IPv6 de origen del paquete es un prefijo de red válido de la CPN correspondiente a la RGW 31. En la red IPv6, las direcciones IPv6 usadas por todos los terminales de usuario dentro de una CPN pertenecen habitualmente a uno o más espacios de direcciones. Es decir, la misma CPN se asigna normalmente a uno o más espacios de direcciones IPv6, es decir, corresponde a uno o más prefijos de red.

Opcionalmente, estos prefijos de red pueden asignarse a la CPN por un servidor de asignación de prefijos de red (por ejemplo, un servidor DHCPv6), o pueden configurarse o especificarse de antemano por otros servidores de configuración durante el despliegue de la red. Durante la implementación real de la presente invención, después de que la CPN obtenga los prefijos de red válidos anteriores, estos prefijos de red válidos pueden notificarse por la RGW 31 al dispositivo 41 de nodo de acceso conectado con la RGW 31, o el dispositivo 41 de nodo de acceso puede obtener estos prefijos de red válidos rastreando un mensaje relevante enviado por el servidor de asignación de prefijos de red o el servidor de configuración a la RGW.

Por lo tanto, cuando el dispositivo 41 de nodo de acceso obtiene los prefijos de red válidos de la CPN correspondientes a la RGW 31, es posible comprobar si el prefijo de red en la dirección IPv6 de origen del paquete enviado a través de la pasarela 31 residencial desde el terminal de usuario dentro de la CPN es uno de estos prefijos de red válidos.

Preferentemente, la red 41 de nodo de acceso prealmacena los prefijos de red válidos correspondientes a la CPN en la forma de un conjunto, es decir, la red 41 de nodo de acceso prealmacena un conjunto de prefijos de red válidos para la CPN. De esta manera, en la etapa S23 simplemente se evalúa si el prefijo de red en la dirección IPv6 de origen obtenido a partir del paquete pertenece al conjunto de prefijos de red válidos prealmacenados para la CPN por el dispositivo 41 de nodo de acceso.

Más preferentemente, para cada elemento de conjunto o parte de los elementos de conjunto del conjunto de prefijos de red válidos guardados para la CPN por el dispositivo 41 de nodo de acceso, es decir, para cada prefijo de red

válido o parte de los prefijos de red válidos, se guarda la información de duración válida para indicar durante qué período de tiempo el espacio de direcciones IPv6 representado por el prefijo de red válido se usa por la CPN correspondiente. En general, la información de duración válida de un prefijo de red válido puede expresarse de las siguientes formas:

1) especificando una hora de inicio y un periodo de tiempo

Por ejemplo, si la hora de inicio de la información de duración válida del prefijo de red válido 3FFE:FFFF:0:C000::/54 son las 20:00 del 8 de agosto de 2008 y el período de tiempo es de 2000 segundos, indica que el prefijo de red válido es válido dentro de los 2000 segundos a partir de las 20:00 del 8 de agosto de 2008, es decir, el terminal de usuario dentro de la CPN puede usar la dirección IPv6 en el espacio de direcciones representado por el prefijo de red válido para enviar paquetes. En este punto, el prefijo de red válido en el conjunto de prefijos de red válidos puede expresarse como (3FFE:FFFF:0:C000::/54, 20:00 del 8 de agosto de 2008, 2000 segundos). La tabla 1 muestra un conjunto de prefijos de red válidos que tienen una información de duración válida expresada en la forma anterior, comprendiendo el conjunto tres prefijos de red válidos y la información de duración válida respectiva.

Tabla 1

Número de serie	Prefijo de red	Hora de inicio	Periodo de tiempo
prefijo de red válido 1	3FFE:FFFF:0:C000::/54	20:00 del 8 de agosto de 2008	2000 segundos
prefijo de red válido 2	3FFE:EEEE:0:C000::/54	20:00 del 8 de julio de 2008	200000 segundos
prefijo de red válido 3	3FFE:DDDD:0:C000::/54	20:00 del 8 de junio de 2008	300000 segundos

2) especificando un plazo

Por ejemplo, si el plazo de la información de duración válida del prefijo de red válido 3FFE:FFFF:0:C000::/54 son las 20:00 del 24 de agosto de 2008, indica que este prefijo de red válido es válido para las 20:00 del 24 de agosto de 2008, es decir, el terminal de usuario dentro de la CPN puede usar la dirección IPv6 en el espacio de direcciones representado por el prefijo de red válido para enviar paquetes. En este punto, el prefijo de red válido en el conjunto de prefijos de red válidos puede expresarse como (3FFE:FFFF:0:C000::/54, 20:00 del 24 de agosto de 2008). La tabla 2 muestra un conjunto de prefijos de red válidos que tienen información de duración válida expresada en la forma anterior, comprendiendo el conjunto dos prefijos de red válidos y la información de duración válida respectiva.

Tabla 2

Número de serie	Prefijo de red	Plazo
prefijo de red válido 1	3FFE:FFFF:0:C000::/54	20:00 del 8 de agosto de 2008
prefijo de red válido 2	3FFE:EEEE:0:C000::/54	20:00 del 8 de agosto de 2008

Como una realización preferida de la presente invención, en el caso de que el conjunto de prefijos de red válidos guardados para la CPN por el dispositivo 41 de nodo de acceso guarde información de duración válida adicional de cada prefijo de red válido, el dispositivo 41 de nodo de acceso evalúa adicionalmente si cada prefijo de red válido en el conjunto de prefijos de red válidos ha expirado, de acuerdo con la información de duración válida correspondiente a cada prefijo de red válido; si un determinado prefijo de red válido ha expirado, el dispositivo 41 de nodo de acceso lo borra del conjunto de prefijos de red válidos. Por ejemplo, un prefijo de red válido en el conjunto de prefijos de red válidos, como se muestra en la tabla 2, es (3FFE:EEEE:0:C000::/54, 20:00 del 24 de agosto de 2008). Si la hora actual del sistema son las 20:05 del 24 de agosto de 2008, significa que este prefijo de red válido ha expirado, es decir, el terminal de usuario dentro de la CPN no debe usar la dirección IPv6 en el espacio de direcciones representado por este prefijo de red válido para enviar paquetes nunca más. En este punto, el dispositivo 41 de nodo de acceso borra, a continuación, el prefijo de red válido (3FFE:EEEE:0:C000::/54, 20:00 del 24 de agosto de 2008) del conjunto de prefijos de red válidos. En consecuencia, después de que se borre este prefijo de red válido, el conjunto de prefijos de red válidos en la tabla 2 puede ser como se muestra en la tabla 3.

Tabla 3

Número de serie	Prefijo de red	Plazo
prefijo de red válido 1	3FFE:EEEE:0:C000::/54	20:00 del 8 de septiembre de 2008

Opcionalmente, durante la implementación real de la presente invención, si un prefijo de red válido ha expirado

puede evaluarse mediante el escaneo periódico de cada prefijo de red válido en el conjunto de prefijos de red válidos y basándose en la información de duración válida correspondiente y la hora actual del sistema; si un determinado prefijo de red válido ha expirado, se borra del conjunto de prefijos de red válidos. Preferentemente, puede iniciarse un temporizador correspondiente de acuerdo con la información de duración válida correspondiente a un prefijo de red válido; en el caso de un suceso de tiempo de espera del temporizador, el prefijo de red válido correspondiente se borra del conjunto de prefijos de red válidos.

Si un determinado prefijo de red válido en el conjunto de prefijos de red válidos no tiene una información de duración válida correspondiente a guardar, entonces se cree que este prefijo de red válido se asigna a la CPN correspondiente a la pasarela 31 residencial para su uso todo el tiempo, es decir, este prefijo de red válido no expirará a medida que transcurra el tiempo.

Preferentemente, la RGW 31 correspondiente a la CPN pide un prefijo de red válido de la CPN desde el servidor de asignación de prefijos de red (por ejemplo, el servidor DHCPv6 u otro servidor AAA). Por lo tanto, el servidor de asignación de prefijos de red normalmente envía un mensaje de respuesta de asignación de prefijos de red a la RGW 31. De acuerdo con la estructura topológica de una red de acceso IPv6, como se ilustra en la figura 1, estos mensajes de respuesta de asignación de prefijos de red deben pasar a través del dispositivo 41 de nodo de acceso antes de llegar a la RGW 31, de manera que el dispositivo 41 de nodo de acceso pueda rastrear de manera conveniente, adecuada y eficiente estos mensajes de respuesta de asignación de prefijos de red, obtener los prefijos de red válidos asignados a la CPN y añadirlos a un conjunto de prefijos de red válidos guardados para esta CPN (en este punto, si el dispositivo 41 de nodo de acceso no contiene un conjunto de prefijos de red válidos correspondiente, en primer lugar se crea un conjunto de prefijos de red válidos vacío antes de realizar la operación de adición). Cuando el dispositivo 41 de nodo de acceso obtiene, a partir del mensaje de respuesta de asignación de prefijos de red rastreado, un prefijo de red válido asignado a la CPN junto con la información de duración válida correspondiente al prefijo de red válido, entonces el dispositivo 41 de nodo de acceso añade el prefijo de red válido y su información de duración correspondiente al conjunto de prefijos de red válidos. Por ejemplo, si el prefijo de red válido asignado es 3FFE:FFFF:0:C000::/54 y la información de duración válida representada por un plazo son las 20:00 del 24 de agosto de 2008, entonces (3FFE:FFFF:0:C000::/54, 20:00 del 24 de agosto de 2008) pueden añadirse conjuntamente al conjunto de prefijos de red válidos de la CPN correspondiente a la RGW 31. Específicamente,

1) si el conjunto de prefijos de red válidos ya contiene un prefijo de red válido (3FFE:FFFF:0:C000::/54, 20:00 del 21 de agosto de 2008), entonces la información de duración válida 20:00 del 21 de agosto de 2008, correspondiente al prefijo de red válido, se actualiza como 20:00 del 24 de agosto de 2008, o (3FFE:FFFF:0:C000::/54, 20:00 del 21 de agosto de 2008) se borran del conjunto de prefijos de red válidos y a continuación (3FFE:FFFF:0:C000::/54, 20:00 del 24 de agosto de 2008) se añaden al conjunto.

2) si el conjunto de prefijos de red válidos ya contiene un prefijo de red válido 3FFE:FFFF:0:C000::/54 sin una información de duración válida correspondiente, entonces, las 20:00 del 24 de agosto de 2008 se usa como información de duración válida del prefijo de red válido, es decir, el conjunto de prefijos de red válidos actualizado incluye el elemento (3FFE:FFFF:0:C000::/54, 20:00 del 24 de agosto de 2008);

3) en otros casos, es decir, si el conjunto de prefijos de red válidos no contiene el prefijo de red 3FFE:FFFF:0:C000::/54, (3FFE:FFFF:0:C000::/54, 20:00 del agosto 24 de 2008) se añaden al conjunto de prefijos de red válidos como un nuevo elemento.

Preferentemente, el servidor de asignación de prefijos de red mencionado anteriormente comprende un servidor DHCPv6 o un encaminador de delegación, y el mensaje de respuesta de prefijo de red enviado a la RGW 31 comprende un mensaje de respuesta DHCP para una delegación de prefijo o un mensaje de reconfiguración DHCP para una delegación de prefijo .

Preferentemente, durante la implementación real de la presente invención, el dispositivo 41 de nodo de acceso se conecta normalmente con una pluralidad de diferentes pasarelas residenciales. En este punto, con el fin de diferenciar fácilmente una pasarela residencial a la que se enviará el mensaje de respuesta DHCP rastreado o el mensaje de reconfiguración DHCP, el dispositivo 41 de nodo de acceso comprende además las siguientes etapas:

en primer lugar, el dispositivo 41 de nodo de acceso inserta un identificador lógico, que se usa por un dispositivo de acceso local para identificar una pasarela residencial, en un mensaje DHCP ascendente (en el presente documento de solicitud, un mensaje DHCP que se envía por la RGW 31 a través del dispositivo 41 de nodo de acceso al servidor DHCPV6 se denomina “mensaje DHCP ascendente” y un mensaje DHCP que se envía por el servidor DHCPv6 a través del dispositivo 41 de nodo de acceso a la RGW 31 se denomina “mensaje DHCP descendente”) recibido desde la pasarela residencial y, a continuación, reenvía el mensaje DHCP ascendente;

en segundo lugar, tras recibir un mensaje DHCP descendente desde el servidor DHCPv6 o el encaminador de delegación, el dispositivo 41 de nodo de acceso evalúa, de acuerdo con el identificador lógico usado por el dispositivo de nodo de acceso local para identificar la pasarela residencial como contenida en el mismo, si el mensaje DHCP descendente se envía a la pasarela residencial correspondiente al identificador lógico contenido

y reenvía el mensaje DHCP descendente a la pasarela residencial. Diferentes identificadores lógicos corresponden a diferentes pasarelas residenciales con las que está conectado el dispositivo 41 de nodo de acceso.

Específicamente, el mensaje DHCP ascendente comprende un mensaje de solicitud DHCP, un mensaje de petición DHCP, un mensaje de renovación DHCP, un mensaje de reconstrucción DHCP y similares en el protocolo DHCPv6; el mensaje descendente comprende un mensaje de anuncio DHCP para una delegación de prefijo, un mensaje de respuesta DHCP para una delegación de prefijo, y un mensaje de reconfiguración DHCP para una delegación de prefijo.

Preferentemente, si el dispositivo 41 de nodo de acceso y la RGW 31 se conectan a través de una línea de abonado digital, el dispositivo 41 de nodo de acceso usa habitualmente un número de línea DSL único para representar esta línea de abonado digital. En este punto, el número de línea DSL puede seleccionarse como un identificador lógico usado para identificar la pasarela residencial por el dispositivo de nodo de acceso local durante la implementación real de la presente invención.

Por último, si el dispositivo 41 de nodo de acceso determina en la etapa S23 que el prefijo de red de la dirección IP de origen del paquete es uno de los prefijos de red válidos de la CPN o pertenece al conjunto de prefijos de red válidos de la CPN, a continuación, el dispositivo 41 de nodo de acceso reenvía el paquete en la etapa S24.

Cabe señalar que las actualizaciones descritas anteriormente en el conjunto de prefijos de red válidos, tales como el borrado y la adición, pueden implementarse mientras que el dispositivo de nodo de acceso comprueba y reenvía el prefijo de red de la dirección IPv6 de origen del paquete. Es decir, no existe un requisito estricto sobre la secuencia de tiempo entre las actualizaciones en el conjunto de prefijos de red válidos, tales como el borrado y la adición, y las etapas S21-S23.

La figura 3 ilustra un diagrama de bloques de un aparato para reenviar un paquete en un dispositivo de nodo de acceso en una red IPv6 de acuerdo con otra realización específica de la presente invención. En lo sucesivo en el presente documento, la realización específica de la presente invención, como se ilustra en la figura 3, se explicará en detalle junto con la figura 1.

En el dispositivo 41 de nodo de acceso, el aparato para reenviar un paquete comprende una unidad 410 de recepción, una unidad 411 de obtención, una unidad 412 de evaluación, una unidad 413 de reenvío, una unidad 414 de borrado, y una unidad 415 de rastreo. Con fines de concisión, el aparato para reenviar un paquete comprende muchos submedios contenidos en las realizaciones preferidas. En virtud de las enseñanzas de la presente solicitud, los expertos en la materia apreciarán que solo la unidad 410 de recepción, la unidad 411 de obtención, la unidad 412 de evaluación y la unidad 413 de reenvío son esenciales para la implementación de la presente invención y que otros medios pueden ser medios ópticos.

En primer lugar, el dispositivo 41 de nodo de acceso recibe un paquete de la RGW 31 por medio de la unidad 410 de recepción, comprendiendo el paquete una dirección IPv6 de origen.

A continuación, el dispositivo 41 de nodo de acceso obtiene un prefijo de red en la dirección IPv6 de origen correspondiente a partir del paquete recibido por medio de la unidad 411 de obtención.

A continuación, el dispositivo 41 de nodo de acceso evalúa, por medio de la unidad 412 de evaluación, si el prefijo de red en la dirección IPv6 de origen del paquete es uno de los prefijos de red válidos de la CPN correspondientes a la RGW 31. La unidad 412 de evaluación guarda todos los prefijos de red válidos de la CPN correspondientes a la RGW 31, es decir, los prefijos de red asignados a la CPN. En otras palabras, los terminales de usuario dentro de la CPN pueden usar direcciones IPv6 de espacios IPv6 representados por estos prefijos de red para enviar paquetes.

Preferentemente, la unidad 412 de evaluación prealmacena los prefijos de red válidos correspondientes a la CPN en la forma de un conjunto, es decir, prealmacena un conjunto de prefijos de red válidos de la CPN. De esta manera, es posible que la unidad 412 de evaluación simplemente evalúe si el prefijo de red en la dirección IPv6 de origen obtenido a partir del paquete pertenece al conjunto de prefijos de red válidos prealmacenados de la CPN.

Más preferentemente, para cada elemento de conjunto o parte de los elementos de conjunto del conjunto de prefijos de red válidos de la CPN guardados por la unidad 412 de evaluación, es decir, para cada prefijo de red válido o parte de los prefijos de red válidos, la información de duración válida se guarda para indicar durante qué período de tiempo el espacio de direcciones IPv6 representado por el prefijo de red válido se usa por la CPN correspondiente. En este punto, la unidad 414 de borrado evalúa si cada prefijo de red válido en el conjunto de prefijos de red válidos ha expirado, de acuerdo con la información de duración válida correspondiente a cada prefijo de red válido; si un determinado prefijo de red válido ha expirado, entonces la unidad 414 de borrado lo borra del conjunto de prefijos de red válidos.

Opcionalmente, durante la implementación real de la unidad 414 de borrado, si un prefijo de red válido ha expirado, puede evaluarse escaneando periódicamente cada prefijo de red válido en el conjunto de prefijos de red válidos y basándose en la información de duración válida correspondiente y la hora actual del sistema; si un determinado

prefijo de red válido ha expirado, se borra del conjunto de prefijos de red válidos. Preferentemente, puede iniciarse un temporizador correspondiente de acuerdo con la información de duración válida correspondiente a un prefijo de red válido; en el caso de un suceso de tiempo de espera del temporizador, la unidad 414 de borrado borra el prefijo de red válido correspondiente del conjunto de prefijos de red válidos.

Preferentemente, la RGW 31 correspondiente a la CPN pide un prefijo de red válido de la CPN desde el servidor de asignación de prefijos de red (por ejemplo, el servidor DHCPv6 u otro servidor AAA). Por lo tanto, el servidor de asignación de prefijos de red envía normalmente un mensaje de respuesta de asignación de prefijos de red a la RGW 31. En este punto, la unidad 415 de rastreo puede rastrear de manera conveniente, adecuada y eficiente estos mensajes de respuesta de asignación de prefijos de red, obtener los prefijos de red válidos asignados a la CPN y añadirlos a un conjunto de prefijos de red válidos correspondientes a la CPN guardados por la unidad 413 de evaluación (en este punto, si la unidad 413 de evaluación no contiene un conjunto de prefijos de red válidos correspondiente, en primer lugar se crea un conjunto de prefijos de red válidos vacio antes de realizar la operación de adición).

Cuando un mensaje de respuesta de asignación de prefijos de red contiene tanto un prefijo de red válido asignado a la CPN como la información de duración válida correspondiente, la unidad 415 de rastreo obtiene, a continuación, el prefijo de red válido asignado a la CPN junto con la información de duración válida correspondiente rastreando el mensaje de respuesta de asignación de prefijos de red y añade el prefijo de red válido y su información de duración válida correspondiente al conjunto de prefijos de red válidos guardados por la unidad 413 de evaluación.

De manera similar, la unidad 415 de rastreo puede realizar una operación de adición al conjunto de prefijos de red de válidos correspondientes a la CPN guardados por la unidad 413 de evaluación usando el procedimiento descrito anteriormente.

Preferentemente, la unidad 415 de rastreo obtiene el prefijo de red válido asignado a la CPN y la información de duración válida correspondiente rastreando un mensaje de respuesta DHCP para una delegación de prefijo o un mensaje de reconfiguración DHCP para una delegación de prefijo, que se envía por el servidor DHCPv6 o el encaminador de delegación a la RGW 31.

Preferentemente, durante la implementación real de la presente invención, el dispositivo 41 de nodo de acceso se conecta normalmente con una pluralidad de diferentes pasarelas residenciales. En este punto, con el fin de diferenciar fácilmente una pasarela residencial a la que se enviará el mensaje de respuesta DHCP rastreado o el mensaje de reconfiguración DHCP, la unidad 415 de rastreo se usa además de la siguiente manera:

en primer lugar, la unidad 415 de rastreo inserta un identificador lógico, que se usa por un dispositivo de acceso local para identificar una pasarela residencial, en un mensaje DHCP ascendente recibido desde la pasarela residencial y, a continuación, reenvía el mensaje DHCP ascendente;

en segundo lugar, tras recibir un mensaje DHCP descendente desde el servidor DHCPv6 o el encaminador de delegación, la unidad 415 de rastreo evalúa, de acuerdo con el identificador lógico usado por el dispositivo de nodo de acceso local para identificar la pasarela residencial contenida en el mismo, si el mensaje DHCP descendente se envía a la pasarela residencial correspondiente al identificador lógico contenido, y reenvía el mensaje DHCP descendente a la pasarela residencial.

Específicamente, el mensaje DHCP ascendente comprende un mensaje de solicitud DHCP, un mensaje de petición DHCP, un mensaje de renovación DHCP, un mensaje de reconstrucción DHCP y similares en el protocolo DHCPv6; el mensaje descendente comprende un mensaje de anuncio DHCP para una delegación de prefijo, un mensaje de respuesta DHCP para una delegación de prefijo, y un mensaje de reconfiguración DHCP para una delegación de prefijo.

Preferentemente, si el dispositivo 41 de nodo de acceso y la RGW 31 se conectan a través de una línea de abonado digital, el dispositivo 41 de nodo de acceso usa habitualmente un número de línea DSL único para representar esta línea de abonado digital. En este punto, el número de línea DSL puede seleccionarse como un identificador lógico usado para identificar la pasarela residencial por el dispositivo de nodo de acceso local durante la implementación real de la presente invención.

Por último, si la unidad 413 de evaluación determina que el prefijo de red de la dirección IP de origen del paquete es uno de los prefijos de red válidos de la CPN o pertenece al conjunto de prefijos de red válidos de la CPN prealmacenados por el dispositivo 41 de nodo de acceso, entonces el paquete se reenvía por medio de la unidad 414 de reenvío.

La figura 4 ilustra una vista de flujo de mensajes de un procedimiento para reenviar un paquete en un dispositivo de nodo de acceso en una red IPv6 de acuerdo con otra realización específica de la presente invención. En lo sucesivo en el presente documento, la realización específica de la presente invención, como se ilustra en la figura 4, se explicará en detalle junto con las figuras 1, 5a y 5b.

En la red de acceso IPv6 de acuerdo con esta realización, el dispositivo 41 de nodo de acceso se conecta con

diferentes pasarelas residenciales a través de diferentes líneas de abonado digital; en el dispositivo 41 de nodo de acceso, diferentes líneas de abonado digital se representan únicamente por diferentes números de línea DSL (n.º de línea DSL) y se conectan con diferentes pasarelas residenciales. Mientras tanto, la RGW 31 corresponde a una CPN donde los terminales de usuario envían paquetes al dispositivo 41 de nodo de acceso a través de la pasarela residencial.

Después de conectarse con el dispositivo 41 de nodo de acceso, la RGW 31 envía en primer lugar un mensaje de solicitud DHCP al servidor DHCPv6 en la etapa S31, pidiendo al servidor DHCPv6 la asignación a un prefijo de red correspondiente. El mensaje de solicitud DHCP contiene la información opción-IA_PD, como se ilustra en la figura 5a.

Tras recibir el mensaje de solicitud DHCP enviado por la RGW 31, el dispositivo 41 de nodo de acceso añade el número de línea DSL de la línea de abonado digital, que conecta el dispositivo 41 de nodo de acceso con la RGW 31, al mensaje de solicitud DHCP por medio de la opción ID de abonado de agente de retransmisión definida en el protocolo DHCPv6 y, posteriormente, reenvía el mensaje de solicitud DHCP al servidor DHCPv6, en la etapa S32. Cabe señalar que este número de línea DSL puede reemplazarse por un identificador lógico usado para diferenciar una pasarela residencial por el dispositivo 41 de nodo de acceso, diferenciando el dispositivo 41 de nodo de acceso diferentes pasarelas residenciales que están conectadas con el mismo de acuerdo con diferentes identificadores lógicos. Por ejemplo, opcionalmente, cuando el dispositivo 41 de nodo de acceso usa diferentes números de serie para indicar únicamente diferentes pasarelas residenciales conectadas con el mismo, el número de línea DSL anterior puede reemplazarse por un número de serie que indica la RGW 31.

Tras recibir un mensaje de anuncio DHCP enviado por el servidor DHCPv6, el dispositivo 41 de nodo de acceso elimina el número de línea DSL contenido del mensaje en la etapa S33 y reenvía el mensaje de anuncio DHCP, que ya no contiene el número de línea DSL, a la pasarela residencial correspondiente al número de línea DSL en la etapa S34.

De manera similar, el dispositivo 41 de nodo de acceso recibe un mensaje de petición DHCP enviado por la RGW 31 en la etapa S35, en el que el mensaje de petición DHCP contiene la opción-IA_PD, como se ilustra en la figura 5a, y la opción IA_PD contiene la información de opción-IAprefijo, como se ilustra en la figura 5b. Posteriormente, el dispositivo 41 de nodo de acceso añade el número de línea DSL de la línea de abonado digital, que conecta el dispositivo 41 de nodo de acceso con la RGW 31, al mensaje de petición DHCP por medio de la opción ID de abonado de agente de retransmisión definida en el protocolo DHCPv6 y reenvía el mensaje de petición DHCP al servidor DHCPv6, en la etapa S36.

Tras recibir un mensaje de respuesta DHCP para la delegación enviado por el servidor DHCPv6, el dispositivo 41 de nodo de acceso elimina el número de línea DSL contenido del mensaje en la etapa S37 y reenvía el mensaje de respuesta DHCP para la delegación, que ya no contiene el número de línea DSL, a la pasarela residencial 31 correspondiente al número de línea DSL en la etapa S38. El mensaje de respuesta de DHCP para la delegación contiene la información de opción-IAprefijo, como se ilustra en la figura 5b, un prefijo IPv6 contenido en la opción-IAprefijo es un prefijo de red asignado a la RGW 31 por el servidor DHCPv6 y la información de duración válida correspondiente representada por el prefijo de red, que es la del momento en el que la RGW 31 recibe el mensaje de respuesta DHCP para la delegación, es una hora de inicio y la duración válida contenida en la opción-IAprefijo es un periodo de tiempo.

Con las etapas S31 a S38, el dispositivo 41 de nodo de acceso puede obtener el prefijo de red válido asignado a la RGW 31 por el servidor DHCPv6 y la información de duración válida correspondiente del mensaje de respuesta DHCP rastreado para la delegación. Por ejemplo, si el dispositivo 41 de nodo de acceso recibe un mensaje de respuesta DHCP para la delegación enviado por el servidor DHCPv6 a la RGW 31, a las 20:00 del 9 de septiembre de 2008, en el que el prefijo IPv6 contenido es 3FFE:FFFF:0:C000::/54, la duración válida contenida es de 2000 segundos, y el dispositivo 41 de nodo de acceso no guarda ningún conjunto de prefijos de red válidos para una CPN correspondiente a la RGW 31, entonces el dispositivo 41 de nodo de acceso creará una lista, como se muestra en la tabla 4, para guardar el prefijo de red válido 3FFE:FFFF:0:C000::/54 asignado a la CPN y la información de duración válida correspondiente.

Tabla 4

Número de serie	Prefijo de red	Hora de inicio	Periodo de tiempo
prefijo de red válido 1	3FFE:FFFF:0:C000::/54	20:00 del 9 de septiembre de 2008	2000 segundos

Posteriormente, en la etapa S39, un terminal de usuario dentro de la CPN obtiene la información de prefijo de red válido de la RGW 31 por medio del mecanismo de autoconfiguración sin estado de dirección IPv6 y forma una dirección IPv6 disponible usando la información de prefijo de red válido junto con su propia información del dispositivo. En la etapa S40, el terminal de usuario envía un paquete a la RGW 31 usando la dirección IPv6 recién formada como una dirección IP de origen del paquete. A continuación, la RGW 31 reenvía el paquete al dispositivo

41 de nodo de acceso en la etapa S41. Por ejemplo, si un prefijo de red asignado a la RGW 31 es 3FFE:FFFF:0:C000::/54, una posible dirección IPv6 formada por el terminal de usuario es 3FFE:FFFF:0:C000:1111:2222:AAAA:BBBB. A continuación, el dispositivo 41 de nodo de acceso obtiene en la etapa S42 el prefijo de red 3FFE:FFFF:0:C000::/54 a partir de la dirección IPv6 de origen del paquete del terminal de usuario reenviado por la RGW 31, compara en la etapa S43 este prefijo de red con el conjunto de prefijos de red válidos de la CPN correspondiente a la RGW 31, como se muestra en la tabla 4, para determinar si el prefijo de red pertenece al conjunto de prefijos de red válidos, como se muestra en la tabla 4 y, finalmente, reenvía el paquete a la red NSP u otro dispositivo dentro de la red de acceso en la etapa S44.

Las realizaciones específicas de la presente invención se han descrito anteriormente. Debe entenderse que la presente invención no se limita a la realización específica anterior, y que los expertos en la materia pueden hacer diversas variaciones o modificaciones dentro del alcance de las reivindicaciones adjuntas. La solución técnica de la presente invención puede implementarse en software o en hardware.

REIVINDICACIONES

1. Un procedimiento para reenviar un paquete desde una pasarela (31) residencial en un dispositivo (41) de nodo de acceso en una red de acceso IPv46, estando el procedimiento **caracterizado por** comprender las etapas de:

obtener un primer prefijo de red asignado a dicha pasarela (31) residencial por un servidor de asignación de prefijos de red;
añadir el primer prefijo de red a un conjunto de prefijos de red válidos prealmacenados para una red en locales de clientes correspondiente a dicha pasarela (31) residencial;
recibir un paquete de dicha pasarela (31) residencial;
obtener un segundo prefijo de red en una dirección IPv6 de origen de dicho paquete;
evaluar si el segundo prefijo de red en la dirección IPv6 de origen de dicho paquete pertenece al conjunto de prefijos de red; y
reenviar dicho paquete en el segundo prefijo de red perteneciente al conjunto de prefijos de red válidos.

2. El procedimiento de acuerdo con la reivindicación 1, **caracterizado porque**
el conjunto de prefijos de red válidos prealmacenados para dicha red en locales de clientes por el dispositivo (41) de nodo de acceso comprende uno o más prefijos de red válidos y la información de duración válida correspondiente, y **porque** el procedimiento comprende además las etapas de:

evaluar si el uno o más prefijos de red válidos han expirado de acuerdo con la información de duración válida correspondiente a cada prefijo de red válido en dicho conjunto de prefijos de red válidos, y
borrar el uno o más prefijos de red válidos y la información de duración válida correspondiente de dicho conjunto de prefijos de red válidos tras la expiración del uno o más prefijos de red válidos.

3. El procedimiento de acuerdo con la reivindicación 1 o 2, **caracterizado porque** la obtención del primer prefijo de red asignado a dicha pasarela (31) residencial incluye rastrear un mensaje de respuesta de asignación de prefijo de red enviado a dicha pasarela (31) residencial por el servidor de asignación de prefijos de red.

4. El procedimiento de acuerdo con la reivindicación 3, **caracterizado porque** la obtención incluye además:

rastrear el mensaje de respuesta de asignación de prefijo de red enviado a dicha pasarela (31) residencial por el servidor de asignación de prefijos de red para una información de duración válida correspondiente al primer prefijo de red,
añadir la información de duración válida correspondiente al conjunto de prefijos de red válidos prealmacenados para dicha red en locales de clientes por el dispositivo (41) de nodo de acceso; y
reemplazar la información de duración válida correspondiente al primer prefijo de red con la información de duración válida obtenida si el primer prefijo de red asignado a dicha red en locales de clientes ya está contenido en dicho conjunto de prefijos de red válidos.

5. El procedimiento de acuerdo con la reivindicación 3 o 4, **caracterizado porque** el servidor de asignación de prefijos de red comprende un servidor DHCPv6 o un encaminador de delegación, y dicho mensaje de respuesta de asignación de prefijo de red comprende un mensaje de respuesta DHCP para una delegación de prefijo o un mensaje de reconfiguración DHCP para una delegación de prefijo.

6. El procedimiento de acuerdo con la reivindicación 5, **caracterizado por** comprender además las etapas de:

recibir un mensaje DHCP ascendente de dicha pasarela (31) residencial, insertar en el mensaje DHCP ascendente un identificador lógico usado para identificar dicha pasarela (31) residencial por el dispositivo (41) de nodo de acceso, y reenviar dicho mensaje DHCP ascendente;
recibir un mensaje DHCP descendente del servidor DHCPv6 o el encaminador de delegación mencionados, y reenviar el mensaje DHCP descendente a la pasarela (31) residencial correspondiente de acuerdo con el identificador lógico contenido usado para identificar dicha pasarela (31) residencial por el dispositivo (41) de nodo de acceso.

7. El procedimiento de acuerdo con la reivindicación 6, **caracterizado porque** dicho mensaje DHCP ascendente comprende un mensaje de solicitud DHCP, un mensaje de petición DHCP, un mensaje de renovación DHCP, y un mensaje de reconstrucción DHCP, y dicho mensaje DHCP descendente comprende un mensaje de anuncio DHCP para una delegación de prefijo, un mensaje de respuesta DHCP para una delegación de prefijo, y un mensaje de reconfiguración DHCP para una delegación de prefijo.

8. El procedimiento de acuerdo con la reivindicación 6, **caracterizado porque** dicho dispositivo (41) de nodo de acceso y dicha pasarela (31) residencial se conectan a través de una línea de abonado digital, y el identificador lógico usado para identificar dicha pasarela (31) residencial por el dispositivo (41) de nodo de acceso comprende un número de línea de dicha línea de abonado digital.

9. Un aparato para reenviar un paquete desde una pasarela (31) residencial en un dispositivo (41) de nodo de acceso en una red de acceso IPv6, estando el aparato **caracterizado por** comprender:

una unidad (411) de obtención configurada para obtener un primer prefijo de red asignado a dicha pasarela (31) residencial por un servidor de asignación de prefijos de red, estando el aparato configurado para añadir el primer prefijo de red a un conjunto de prefijos de red válidos prealmacenados para una red en locales de clientes correspondiente a dicha pasarela (31) residencial;
una unidad (410) de recepción configurada para recibir un paquete desde dicha pasarela (31) residencial;
la unidad (411) de obtención configurada, además, para obtener un segundo prefijo de red en una dirección IPv6 de origen de dicho paquete;
una unidad (412) de evaluación configurada para evaluar si el segundo prefijo de red en la dirección IPv6 de origen de dicho paquete pertenece al prefijo de red válido de una red en locales de clientes correspondiente a dicha pasarela (31) residencial; y
una unidad (413) de reenvío configurada para reenviar dicho paquete en el segundo prefijo de red perteneciente al conjunto de prefijos de red válidos.

10. El aparato de acuerdo con la reivindicación 9, **caracterizado porque** el conjunto de prefijos de red válidos prealmacenados para dicha red en locales de clientes por el dispositivo (41) de nodo de acceso comprende uno o más prefijos de red válidos y la información de duración válida correspondiente, y **porque** el aparato comprende además:

una unidad (414) de borrado configurada para
evaluar si el uno o más prefijos de red válidos han expirado de acuerdo con la información de duración válida correspondiente a cada prefijo de red válido en dicho conjunto de prefijos de red válidos, y
borrar el uno o más prefijos de red válidos y la información de duración válida correspondiente de dicho conjunto de prefijos de red válidos tras la expiración del uno o más prefijos de red válidos.

11. El aparato de acuerdo con la reivindicación 9 o 10, **caracterizado por** comprender además:

una unidad (415) de rastreo configurada para rastrear un mensaje de respuesta de asignación de prefijo de red enviado a dicha pasarela (31) residencial por el servidor de asignación de prefijos de red, para obtener el primer prefijo de red.

12. El aparato de acuerdo con la reivindicación 11, **caracterizado porque** dicha unidad (415) de rastreo está configurada además para:

rastrear el mensaje de respuesta de asignación de prefijo de red enviado a dicha pasarela (31) residencial por el servidor de asignación de prefijos de red, para obtener una información de duración válida correspondiente al primer prefijo de red,
añadir la información de duración válida correspondiente al conjunto de prefijos de red válidos prealmacenados para dicha red en locales de clientes por el dispositivo (41) de nodo de acceso; y
reemplazar la información de duración válida correspondiente al primer prefijo de red con la información de duración válida obtenida si el primer prefijo de red asignado a dicha red en locales de clientes ya está contenido en dicho conjunto de prefijos de red válidos.

13. El aparato de acuerdo con la reivindicación 11 o 12, **caracterizado porque** el servidor de asignación de prefijos de red comprende un servidor DHCPv6 o un encaminador de delegación, y dicho mensaje de respuesta de asignación de prefijo de red comprende un mensaje de respuesta DHCP para una delegación de prefijo o un mensaje de reconfiguración DHCP para una delegación de prefijo.

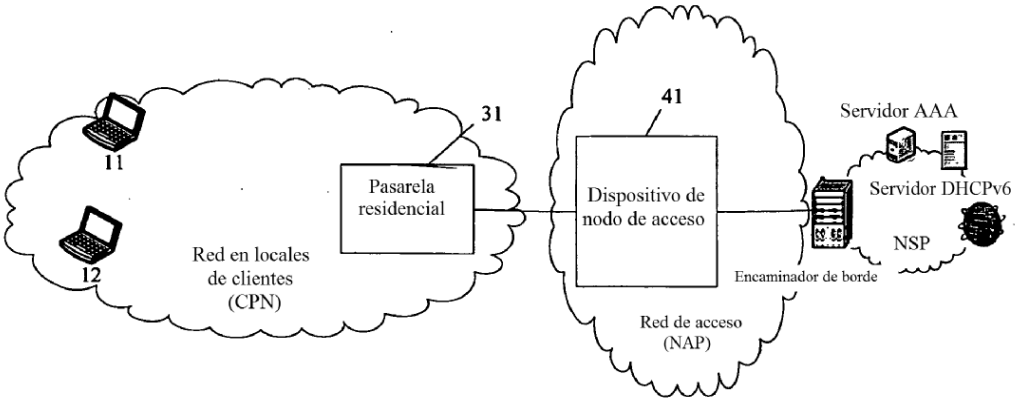
11
12
31
Pasarela residencial
Red en locales de clientes (CPN)
41
Dispositivo de nodo de acceso
Red de acceso (NAP)
Servidor AAA
Servidor DHCPv6
NSP
Encaminador de borde

Fig. 1

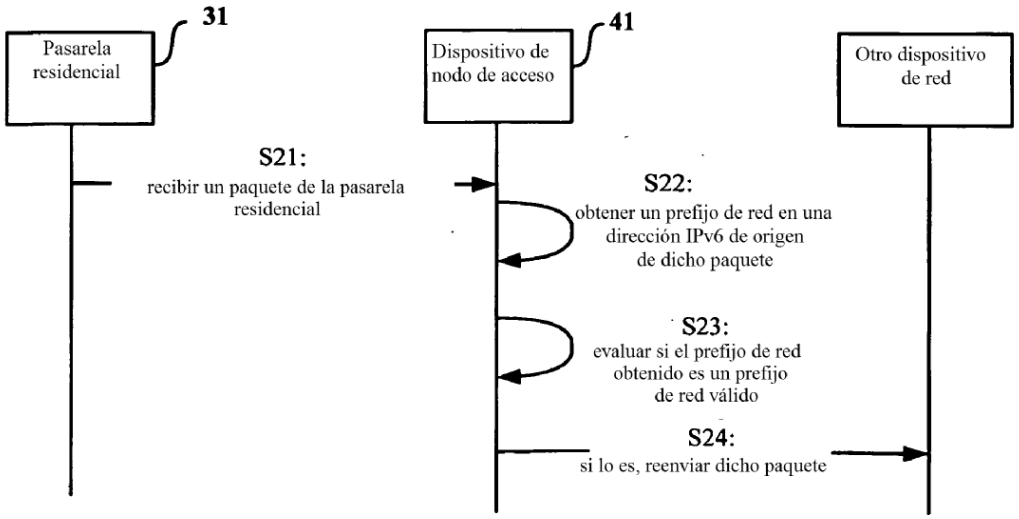
Pasarela residencial
31
Dispositivo de nodo de acceso
41
Otro dispositivo de red
S21:
recibir un paquete de la pasarela residencial
S22:
obtener un prefijo de red en una dirección IPv6 de origen de dicho paquete
S23:
evaluar si el prefijo de red obtenido es un prefijo de red válido
S24:
si lo es, reenviar dicho paquete

Fig. 2

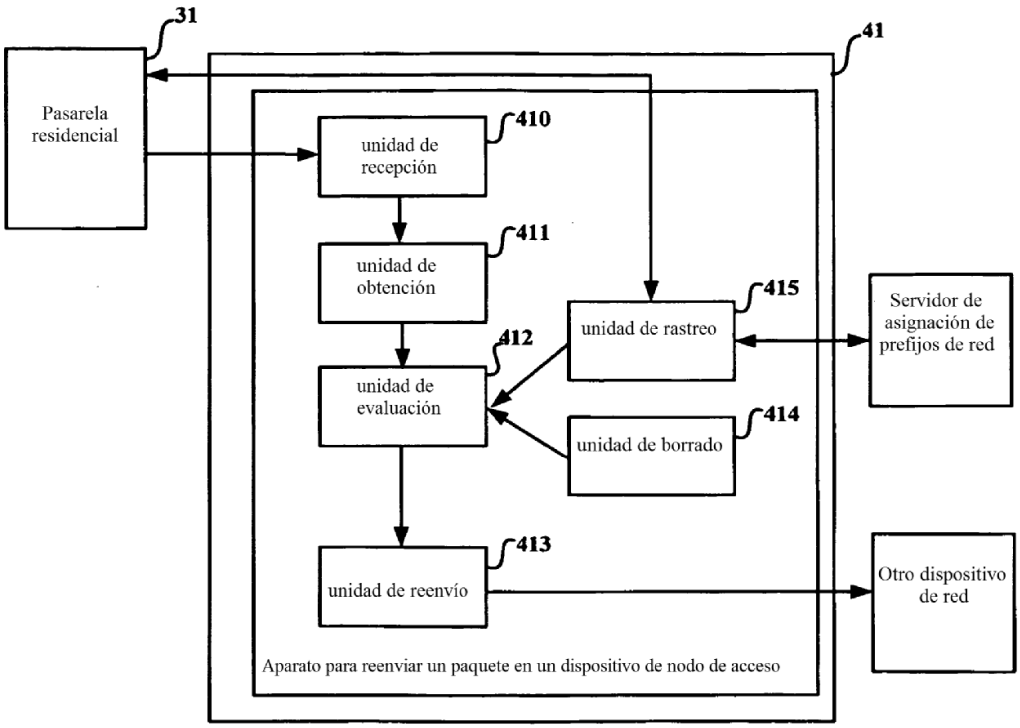
31
41
Pasarela residencial
410
unidad de recepción
411
unidad de obtención
412
unidad de evaluación
413
unidad de reenvío
415
unidad de rastreo
414
unidad de borrado
Servidor de asignación de prefijos de red
Otro dispositivo de red
Aparato para reenviar un paquete en un dispositivo de nodo de acceso

Fig. 3

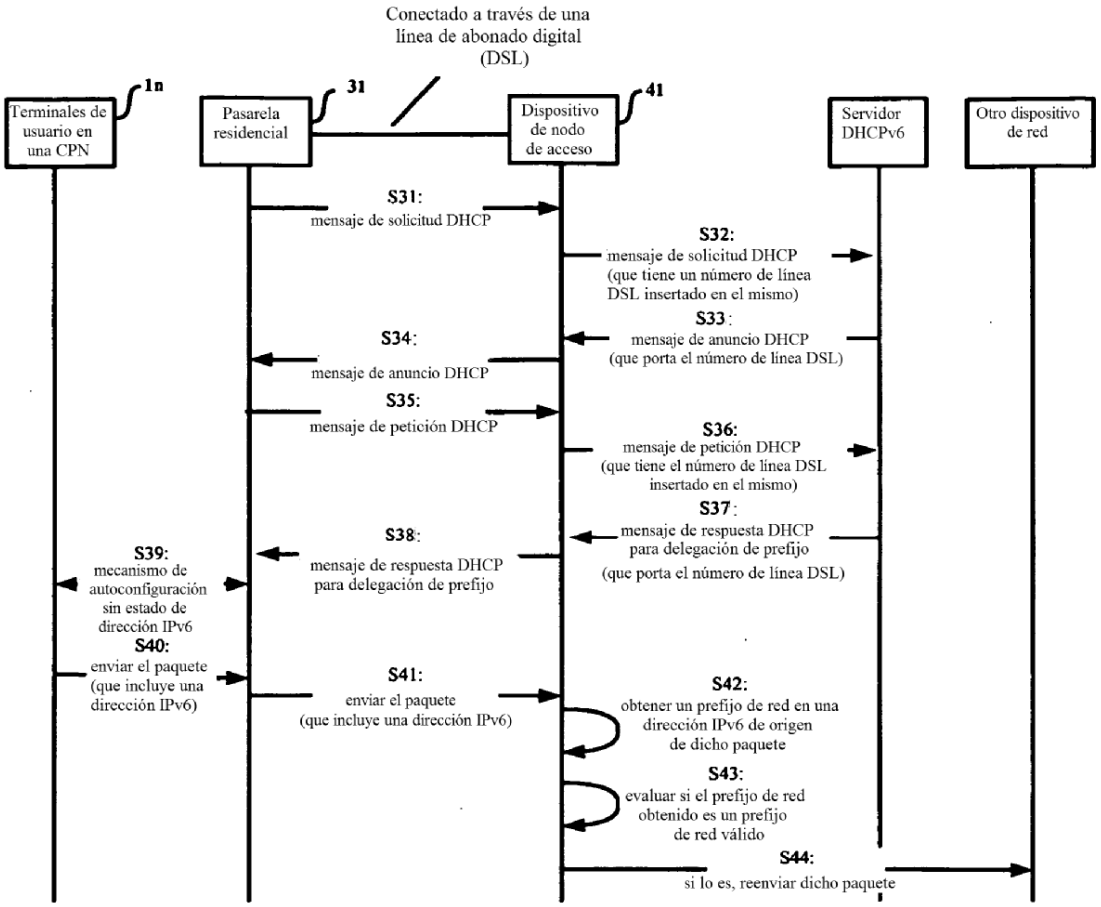
Conectado a través de una línea de abonado digital (DSL)
Terminales de usuario en una CPN
1n
Pasarela residencial
31
Dispositivo de nodo de acceso
41
Servidor DHCPv6
Otro dispositivo de red
S31: mensaje de solicitud DHCP
S32: mensaje de solicitud DHCP (que tiene un número de línea DSL insertado en el mismo)
S33: mensaje de anuncio DHCP (que porta el número de línea DSL)
S34: mensaje de anuncio DHCP
S35: mensaje de petición DHCP
S36: mensaje de petición DHCP (que tiene el número de línea DSL insertado en el mismo)
S37: mensaje de respuesta DHCP para delegación de prefijo (que porta el número de línea DSL)
S38: mensaje de respuesta DHCP para delegación de prefijo
S39: mecanismo de autoconfiguración sin estado de dirección IPv6
S40: enviar el paquete (que incluye una dirección IPv6)
S41: enviar el paquete (que incluye una dirección IPv6)
S42: obtener un prefijo de red en una dirección IPv6 de origen de dicho paquete
S43: evaluar si el prefijo de red obtenido es un prefijo de red válido
S44: si lo es, reenviar dicho paquete

Fig. 4

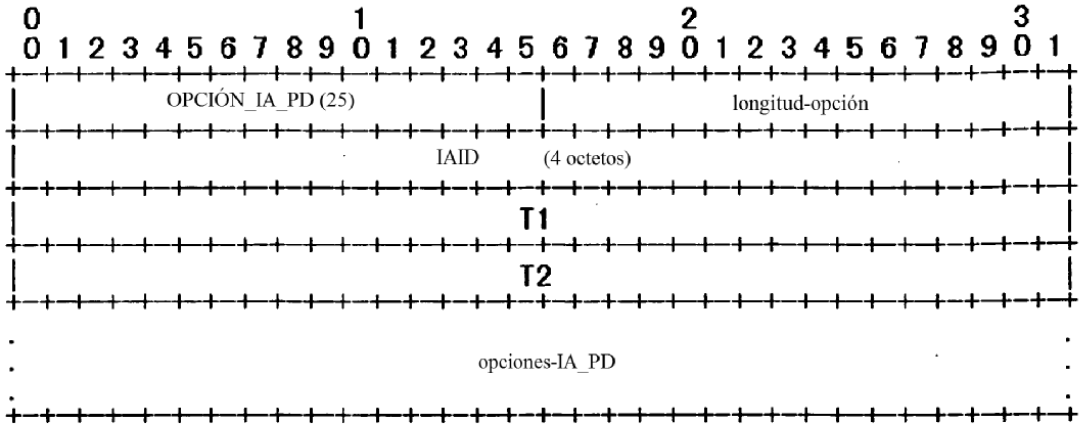
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
OPCIÓN_IA_PD (25)
longitud-opción
IAID
(4 octetos)
T1
T2
opciones-IA_PD

Fig. 5a

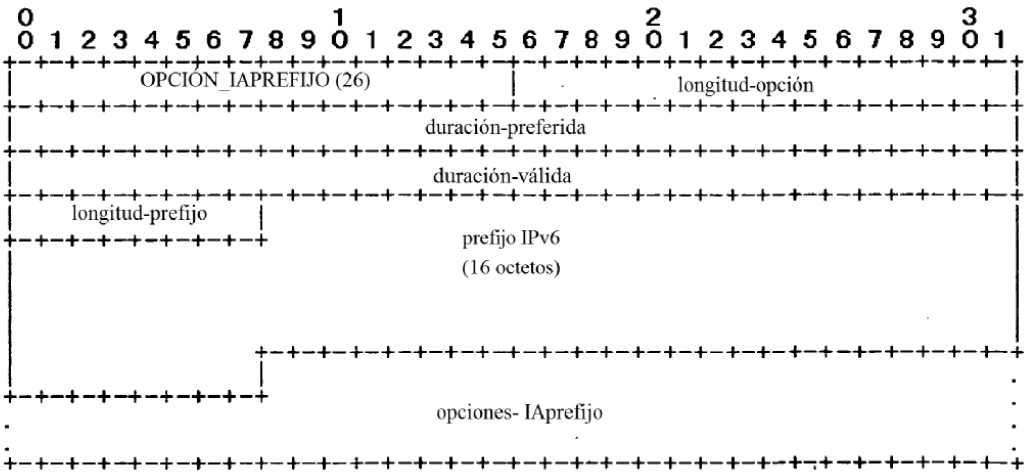
0 1 2 3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
OPCIÓN_IAPREFIJO (26)
longitud-opción
duración-preferida
duración-válida
longitud-prefijo
prefijo IPv6
(16 octetos)
opciones- IAprefijo

Fig. 5b