(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 384 162**

(51) Int. CI.:
H04L 12/24 (2006.01)
H04L 12/26 (2006.01)
H04L 29/12 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **10733212 .4**
(96) Fecha de presentación: **13.01.2010**
(97) Número de publicación de la solicitud: **2383934**
(97) Fecha de publicación de la solicitud: **02.11.2011**

(54) Título: **Método y sistema de vigilancia de la vivacidad de sesiones IP, pasarela doméstica y equipo de red**

(30) Prioridad:
21.01.2009 CN 200910001997

(45) Fecha de publicación de la mención BOPI:
02.07.2012

(45) Fecha de la publicación del folleto de la patente:
02.07.2012

(73) Titular/es:
Huawei Technologies Co., Ltd.
Huawei Administration Building Bantian
Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:
ZHENG, Ruobin

(74) Agente/Representante:
Lehmann Novo, Isabel

DESCRIPCIÓN

Método y sistema de vigilancia de la vivacidad de sesiones IP, pasarela doméstica y equipo de red.

CAMPO DE LA INVENCIÓN

La presente invención se refiere al campo de las tecnologías de comunicaciones y, en particular, a un método y un sistema para la vigilancia del estado activo de sesiones de protocolo de Internet (IP), a una pasarela doméstica (HGW) y a un dispositivo de red.

ANTECEDENTES DE LA INVENCIÓN

En una red de acceso una sesión IP representa una sesión de conexión de acceso a la red asociada con una dirección IP de un usuario, la "sesión IP" y una sesión de protocolo de punto a punto (PPP) son de homólogo a homólogo y la "sesión IP" y la "sesión "PPP" se denominan colectivamente sesión de abonado. La sesión PPP adopta un mecanismo particular de detección de PPP activo, y una sesión IPv4 adopta un mecanismo particular de detección de reenvío bidireccional (BFD) activa o de detección de protocolo de resolución de dirección (ARP) activo.

La "sesión IP" se termina generalmente en un nodo de borde IP, tal como una pasarela de red de banda ancha (BNG) o un servidor de acceso remoto de banda ancha (BRAS), y el otro lado de la "sesión IP" se termina generalmente en un dispositivo de usuario, tal como una HGW, es decir que la "sesión IP" es una conexión de sesión establecida entre el dispositivo de usuario y el nodo de borde IP y constituye una sesión de un solo salto. La "sesión IP" se utiliza para que una red gestione el acceso de usuarios a la red, tal como la carga y el estado. La "sesión IP" utiliza una dirección IP o un prefijo de dirección IP como identificador de la "sesión IP".

La técnica anterior tiene las desventajas siguientes: En la técnica anterior una HGW bajo la IPv4 soporta una traducción de dirección de red (NAT) y una "sesión IPv4" es un "solo salto IPv4", mientras que una HGW bajo la IPv6 es un enrutador y generalmente no soporta la NAT, y en este caso un dispositivo de usuario en el que se termine la "sesión IP" no es necesariamente una HGW, y puede ser un equipo de usuario (UE) siguiente a la HGW, y en ese momento la "sesión IPv6" necesita ser extendida hasta un "múltiple salto IPv6", pero ninguna solución de la técnica anterior resuelve el modo en que el UE siguiente a la HGW recorre la HGW para materializar una vigilancia del estado activo (actividad) de una "sesión IPv6 de múltiples saltos".

Los documentos WO 2008/141572 A1 y EP 2 139 189 A1 proporcionan un método y un sistema para realizar una vigilancia del estado activo en sesiones de abonado, así como un dispositivo de borde. En el método se realiza una vigilancia del estado activo en un grupo de sesiones de abonado y un resultado de la vigilancia del estado activo del grupo de sesiones de abonado sirve como resultado de vigilancia del estado activo de una pluralidad de sesiones de abonados en el grupo de sesiones de abonado. No se cita ningún discriminador.

El documento WO 2008/067760 A1 proporciona un sistema para vigilar la vivacidad de sesiones IP. El método incluye uno o más dispositivos de vigilancia de sesión y un dispositivo de control de sesión, y cada uno de los uno o más dispositivos de vigilancia de sesión está adaptado para adquirir el estado de una sesión IP en uno o más dispositivos vigilados y reportar el estado de la sesión IP al dispositivo de control de sesión. No se cita ningún discriminador.

SUMARIO DE LA INVENCIÓN

Las realizaciones de la presente invención proporcionan un método y un sistema para vigilar el estado activo de sesiones IP, una HGW y un dispositivo de red, que materializan una vigilancia del estado activo de una sesión "IPv6 de múltiples saltos".

Según un aspecto de la invención, la presente invención proporciona un método de vigilancia del estado activo de sesiones IP correspondiente a la reivindicación 1 independiente, el cual incluye:

recibir, por un UE o un nodo de borde IP, un mensaje BFD enviado por una HGW, en donde un primer valor de campo discriminador incluido en el mensaje BFD es una diferencia entre un prefijo de dirección IP del UE y un prefijo de dirección IP de la HGW; y

vigilar, por el UE o el nodo de borde IP, si una sesión IP entre el nodo de borde IP y el UE está activa según el primer valor del campo discriminador en el mensaje BFD;

en donde el UE está conectado al nodo de borde IP a través de la HGW.

Según otro aspecto de la invención, la presente invención proporciona una HGW correspondiente a la reivindicación 12 independiente, la cual incluye:

un módulo de recepción configurado para recibir un mensaje BFD enviado por un UE o un nodo de borde IP, en

donde el UE está conectado al nodo de borde IP a través de la HGW; y

un módulo de reenvío configurado para enviar el mensaje BFD, incluyendo el primer valor de campo discriminador, al nodo de borde IP o al UE de acuerdo con el mensaje BFD recibido por el módulo de recepción, en donde el primer valor del campo discriminador es una diferencia entre un prefijo de dirección IP del UE y un prefijo de dirección IP de la HGW.

Según un tercer aspecto de la invención, la presente invención proporciona un dispositivo de red correspondiente a la reivindicación 17 independiente, el cual incluye:

un módulo de recepción configurado para recibir un mensaje BFD enviado por una HGW, en donde un primer valor de campo discriminador incluido en el mensaje BFD es una diferencia entre un prefijo de dirección IP de un UE y un prefijo de dirección IP de la HGW; y

un módulo de procesamiento configurado para vigilar si una sesión IP entre un nodo de borde IP y el UE está activa de acuerdo con el primer valor del campo discriminador en el mensaje BFD;

en donde el dispositivo de red es el nodo de borde IP y el UE está conectado al nodo de borde IP a través de la HGW.

En el método y el sistema para la vigilancia del estado activo de sesiones IP, en la HGW y en el dispositivo de red según las realizaciones de la presente invención, se utiliza una “BFD multisalto” como mecanismo de vigilancia del estado activo de una “sesión IPv6 multisalto”, de modo que se puede establecer una “sesión IPv6” entre el UE siguiente al HGW y el nodo de borde IP, y se puede extender una “sesión IP de un solo salto” a una “sesión IP multisalto”, realizando así una vigilancia del estado activo de la “sesión IPv6 de múltiples saltos”.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es una diagrama estructural esquemático de un sistema de “sesión IPv6” según la presente invención;

La figura 2 es un diagrama esquemático de un plano de datos de una “sesión IPv6 multisaltos” según la presente invención;

La figura 3 es un diagrama de principio esquemático de un mandatario de vigilancia del estado activo de una “sesión IPv6” según la presente invención;

La figura 4 es un diagrama esquemático de un método de vigilancia del estado activo de una sesión IP según una primera realización de la presente invención;

La figura 5 es un diagrama esquemático de un método de vigilancia del estado activo de una sesión IP conforme a una segunda realización de la presente invención;

La figura 6 es un diagrama esquemático de un método de vigilancia del estado activo de una sesión IP según una tercera realización de la presente invención;

La figura 7 es un diagrama estructural esquemático de una HGW según una realización de la presente invención;

La figura 8 es un diagrama estructural esquemático de un dispositivo de red según una realización de la presente invención; y

La figura 9 es un diagrama estructural esquemático de un sistema de vigilancia del estado activo de una sesión IP según una realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS REALIZACIONES

Las soluciones técnicas según las realizaciones de la presente invención se ilustran adicionalmente en lo que sigue con referencia a los dibujos adjuntos y a realizaciones específicas.

La figura 1 es un diagrama estructural esquemático de un sistema de “sesión IPv6” según la presente invención. Como se muestra en la figura 1, una HGW es un enrutador de tres capas y realiza una función de “mandatario” de “sesión IPv6 activa” (vigilancia del estado activo). Se pueden combinar una pluralidad de UEs o una pluralidad de “sesiones IPv6” para formar un grupo de UEs o un grupo de “sesiones IPv6” según una clasificación de dominios de gestión, regiones geográficas o servicios. Una “sesión IP 0” es una “sesión IPv6” de un solo salto establecida entre la HGW y una BNG, con la HGW como abonado; una “sesión IP n” es una “sesión IPv6” establecida entre un UE (particularmente un usuario nómada) y una BNG, con el UE como abonado, la “sesión IP n” es una “sesión” multisalto, un salto del UE a la HGW es un primer salto y un salto de la HGW a un “nodo de borde IP” es un segundo salto; y la HGW solicita un prefijo de dirección a través de una delegación de prefijo (PD) del protocolo de configuración dinámica del anfitrión (DHCP), por ejemplo un prefijo de dirección “prefijo Z” de 56 bits. La HGW

extiende diferentes subprefijos para el UE siguiente a través del “prefijo Z”; por ejemplo, usuarios diferentes tienen subprefijos diferentes de 64 bits, o un usuario fijo y un usuario nómada tienen subprefijos diferentes de 64 bits. La “sesión IP” utiliza una dirección/prefijo IP como identificador de la “sesión IP”; por ejemplo, la “sesión IP 0” utiliza el “prefijo Z” de 56 bits como identificador y la “sesión IP n” utiliza un “prefijo Yn” de 64 bits como identificador, en donde n = 1, 2, 3…

La figura 2 es un diagrama esquemático de un plano de datos de una “sesión IPv6 multisalto” según la presente invención. Como se muestra en la figura 2, en el plano de datos una “sesión IP multisalto” entre una BNG y un UE es transportada sobre una “sesión IP” de un solo salto entre la BNG y una HGW. La figura 3 es un diagrama de principio esquemático de un mandatario de vigilancia del estado activo de una “sesión IPv6” según la presente invención. Como se muestra en la figura 4, la figura 5 y la figura 6, un bloque “P” representa un homólogo de sesión y la presente invención proporciona principalmente dos soluciones.

En la solución 1 se utiliza una “BFD multisalto” como mecanismo de vigilancia del estado activo de una “sesión IPv6 multisalto”, un mandatario de vigilancia del estado activo (un mandatario de sesión IPv6 activa) está dispuesto en la HGW y se transmite transparentemente un mensaje de protocolo “BFD multisalto” o se modifica un campo discriminador del mensaje de protocolo BFD.

En la solución 2 se dispone un “mandatario de sesión IPv6 activa” en la HGW, un “UE heredado” ejecuta una “sesión activa” de un primer salto adoptando una “detección de vecino inalcanzable de un solo salto (NUD)”/”BFD”, la BNG ejecuta una “sesión activa” de un segundo salto adoptando una “BFD de un solo salto”, y el “mandatario de sesión IPv6 activa” realiza una retransmisión del estado activo de la NUD/BFD del primer salto a la BFD del segundo salto. Se puede combinar una pluralidad de UEs o una pluralidad de “sesiones IPv6” para formar un grupo de UEs o un grupo de sesiones IPv6 según una clasificación de dominios de gestión, regiones geográficas o servicios, y un mandatario puede utilizar diferentes puertos de red de área amplia (WAN) para que se correspondan con diferentes grupos de UEs o grupos de “sesiones IPv6”. Especialmente, cuando un grupo de UEs o un grupo de “sesiones IPv6” contiene solamente un UE o una “sesión IPv6”, el mandatario puede utilizar puertos WAN diferentes para que se correspondan con diferentes UEs o “sesiones IPv6”.

La figura 4 es un diagrama esquemático de un método de vigilancia del estado activo de una sesión IP según una primera realización de la presente invención. En esta realización un “mandatario de sesión IPv6 activa” dispuesto en una HGW realiza una vigilancia del estado activo de una “sesión IPv6 de múltiples saltos” en un modo de transmisión transparente. Un nodo de borde IP puede incluir una BNG o un BRAS, y en cada realización de la presente invención el nodo de borde IP se ilustra tomando la BNG como ejemplo. Como se muestra en la figura 4, la vigilancia del estado activo de la “sesión IP” entre un UE y una BNG incluye: La HGW reenvía un mensaje BFD enviado al UE y a la BNG, en donde un primer valor de campo discriminador en el mensaje BFD es una diferencia entre un prefijo de dirección IP del UE y un prefijo de dirección IP de la HGW; el UE recibe el mensaje BFD y vigila si una sesión IP entre el UE y la BNG está activa de acuerdo con el primer valor del campo discriminador. Para una dirección de enlace descendente, la BNG envía el mensaje BFD al UE, y después de recibir el mensaje el UE puede determinar que una “sesión BFD” correspondiente está activa de acuerdo con un valor de un campo “discriminador” en el mensaje en combinación con un identificador de “sesión BFD” predefinido, y dado que la “sesión BFD” está asociada con la “sesión IP”, el UE puede determinar si la “sesión IP” está activa. La BNG recibe un mensaje BFD y vigila si la sesión IP entre la BNG y el UE está activa de acuerdo con el primer valor del campo discriminador en el mensaje BFD. Para una dirección de enlace ascendente, el UE envía el mensaje BFD a la BNG, y después de recibir el mensaje la BNG puede determinar si una “sesión IPv6” correspondiente está activa de acuerdo con un valor de un campo “discriminador” en el mensaje en combinación con un identificador de “sesión BFD” predefinido.

La vigilancia del estado activo de la “sesión IPv6” entre la HGW y la BNG incluye: La HGW recibe el mensaje BFD enviado por la BNG y vigila si una sesión IP entre la HGW y la BNG está activa de acuerdo con un segundo valor del campo discriminador en el mensaje BFD, en donde el segundo valor del campo discriminador se ajusta a un valor especial, por ejemplo “0” o “0xFFFF”. En la dirección de enlace descendente la BNG envía el mensaje BFD a la HGW, y la HGW puede determinar la “sesión BFD” correspondiente de acuerdo con el valor del campo “discriminador” en el mensaje BFD y, por consiguiente, puede vigilar un estado activo de la “sesión IP” asociada. La BNG recibe un mensaje BFD enviado por la HGW y vigila si la sesión IP entre la BNG y la HGW está activa de acuerdo con una información relacionada con la dirección IP de origen y/o el segundo valor del campo discriminador en el mensaje BFD, en donde la información relacionada con la dirección IP de origen incluye una dirección IP de origen o un prefijo de dirección IP de origen. En la dirección de enlace ascendente, después de recibir el mensaje BFD enviado por la BNG, la HGW puede determinar la “sesión BFD” correspondiente de acuerdo con una dirección IP de origen del mensaje, es decir, una dirección/prefijo IP de origen de la BNG, y/o el valor del campo “discriminador” en el mensaje BFD, y, por consiguiente, puede vigilar un estado activo de la “sesión IP” asociada.

Específicamente, en el modo de transmisión transparente de la HGW:

La “sesión BFD” adoptada por “estado activo” de la “sesión IPv6” de un solo salto ejecuta una interacción “activa” con una dirección de la HGW o una dirección de la BNG, y el campo “discriminador” del mensaje BFD se ajusta a “0”

o “0xFFFF”.

La “sesión BFD” adoptada para “sesión IPv6 activa” de la “sesión IPv6” multisalto ejecuta una interacción “activa” con una dirección del UE o una dirección de la BNG, y el valor del campo “discriminador” en el mensaje BFD se ajusta a (Yn-Z), en donde n = 1, 2, 3…, es decir, una diferencia entre un “prefijo Yn” y un “prefijo Z”. Por ejemplo, si el “prefijo Yn = 2002:db8:200:122::/64” y el “prefijo Z = 2002:db8:200:100::/56”, entonces Yn-Z = 0x22, como se muestra en la tabla 1

TABLA 1

	0 a 15 bits	15 a 31 bits	32 a 47 bits	48 a 55 bits	56 a 63 bits
Prefijo Yn	0x2002	0x0db8	0x0200	0x01	0x22
Prefijo Z	0x2002	0x0db8	0x0200	0x01	0x00
Yn-Z	0	0	0	0	0x22

El BNG/UE asocia la “sesión BFD” con una “sesión IPv6”/grupo de “sesiones IPv6” correspondientes de acuerdo con el valor del campo “discriminador” en el mensaje BFD. El campo “discriminador” puede incluir un campo “mi discriminador” o un campo “su discriminador”. Además, bajo el mismo “prefijo Yn” un usuario puede tener una pluralidad de direcciones IP y una pluralidad de “sesiones IP”; la pluralidad de “sesiones IP” puede utilizarse como un grupo de “sesiones IP” a asociar con el valor del campo “discriminador” en el mensaje BFD, es decir que el campo “discriminador” del mensaje BFD puede representar un grupo de “sesiones IP” bajo el mismo “prefijo Yn”, y así el primer valor del campo discriminador está configurado para identificar una sesión IP o múltiples sesiones IP bajo el mismo prefijo de dirección IP del UE.

Opcionalmente, un prefijo de dirección IP de origen está configurado para identificar una sesión IP y la “sesión BFD” de un solo salto utiliza el “prefijo Z” como identificador de la “sesión”, y la “sesión BFD” multisalto utiliza el “prefijo Z” o el “prefijo Yn” como identificador de la “sesión”.

Tomando la figura 4 como ejemplo, se puede identificar una “sesión IP 0” con un “prefijo Z” y se puede adoptar una “sesión BFD 0” para soportar el estado “activo”, y el campo “discriminador” del mensaje BFD se ajusta a “0” o “0xFFFF”, y el BNG/UE asocia la “sesión BFD 0” con una “sesión IPv6 0” de acuerdo con el prefijo de dirección IP de origen, el “prefijo Z” y el valor del campo “discriminador” (0 o 0xFFFF) del mensaje BFD.

Una “sesión IP 1” puede identificarse con un “prefijo Y1” y adoptar una “sesión BFD 1” para soportar el estado “activo”, y el campo “discriminador” del mensaje BFD se ajusta a (Y1-Z); y el BNG/UE asocia la “sesión BFD 1” con una “sesión IPv6 1” correspondiente de acuerdo con el valor del campo “discriminador” (Y1-Z) del mensaje BFD.

Una “sesión IP n” puede identificarse con un “prefijo Yn” y adoptar una “sesión BFD n” para soportar el estado “activo”, y el campo “discriminador” del mensaje BFD se ajusta a (Yn-Z); y el BNG/UE asocia la “sesión “BFD n” con una “sesión IPv6 n” correspondiente de acuerdo con el valor del campo “discriminador” (Yn-Z) del mensaje BFD.

En otra realización más de la presente invención un “mandatario de sesión IPv6 activa” dispuesto en una HGW realiza una vigilancia del estado activo de una “sesión IPv6 de múltiples saltos” en un modo de mandatario. El modo de mandatario es: La HGW recibe un mensaje de detección enviado entre un UE o una BNG, modifica un primer valor del campo discriminador en el mensaje de detección y reenvía luego el mensaje de detección modificado a la BNG o al UE; y se vigila, por el UE o por la BNG, si una sesión IP entre la BNG y el UE está activa de acuerdo con el primer valor del campo discriminador en el mensaje de detección. Para el modo de mandatario se introducen respectivamente diferentes ajustes de puerto de la HGW.

Un caso del modo de mandatario es como se muestra en la figura 4. Para la vigilancia del estado activo de la “sesión IP” entre el UE y la BNG, la modificación del primer valor del campo discriminador en el mensaje de detección y el reenvío subsiguiente del mensaje de detección modificado a la BNG o al UE incluyen específicamente: recibir, por la HGW, el mensaje BFD enviado por el UE, modificar el primer valor del campo discriminador en el mensaje BFD convirtiéndolo en la diferencia entre el prefijo de dirección IP del UE y el prefijo de dirección IP de la HGW y enviar seguidamente el mensaje BFD modificado a la BNG. La HGW recibe el mensaje BFD enviado por la BNG, en donde el primer valor del campo discriminador en el mensaje BFD es la diferencia entre el prefijo de dirección IP del UE y el prefijo de dirección IP de la HGW, modifica el primer valor del campo discriminador convirtiéndolo en un valor reconocible por el UE y envía el mensaje BFD modificado al UE. La “sesión BFD” adaptada para “sesión IPv6 activa” de la “sesión IPv6” multisalto ejecuta una interacción “activa” con una dirección del usuario o una dirección de la BNG, y el “mandatario de sesión IPv6 activa” modifica un valor de un campo “discriminador” de un mensaje BFD de primer salto convirtiéndolo en (Yn-Z), es decir, una diferencia entre el “prefijo Yn” y el “prefijo Z”, y reenvía luego el mensaje en un segundo salto; o bien el “mandatario de sesión IPv6 activa” modifica el valor del campo

"discriminador" (Yn-Z) de un mensaje BFD de segundo salto convirtiéndolo en un valor reconocible por el UE/BNG, y reenvía luego el mensaje en el primer salto. Asimismo, el BNG/UE asocia la "sesión BFD" con una "sesión IPv6" de acuerdo con el valor del campo "discriminador" del mensaje BFD. El campo "discriminador" puede incluir un campo "mí discriminador" o un campo "su discriminador". Además, bajo el mismo "prefijo Yn" un usuario puede tener una pluralidad de direcciones IP y una pluralidad de "sesiones IP"; la pluralidad de "sesiones IP" puede utilizarse como un grupo de "sesiones IP" a asociar con el valor del campo "discriminador en el mensaje BFD, es decir, el campo "discriminador" del mensaje BFD puede representar un grupo de "sesiones IP" bajo el mismo "prefijo Yn". Opcionalmente, la "sesión BFD" de un solo salto utiliza el "prefijo Z" como identificador de la "sesión"; y la "sesión BFD" multisalto utiliza el "prefijo Z" o el "prefijo Yn" como identificador de la "sesión".

La vigilancia del estado activo de la "sesión IPv6" entre la HGW y la BNG se realiza por el mismo método que el método en el que el "mandatario de sesión "IPv6 activa" dispuesto en la HGW realiza la "sesión IPv6 de múltiples saltos" en el modo de transmisión transparente, y los detalles no se describen aquí nuevamente.

Otro caso del modo de mandatario es como se muestra en la figura 5. La figura 5 es un diagrama esquemático de un método de vigilancia del estado activo de una sesión IP de acuerdo con una segunda realización de la presente invención. En esta realización un "mandatario de sesión IPv6 activa" dispuesto en una HGW realiza una vigilancia del estado activo de una "sesión IPv6 de múltiples saltos" en un modo de mandatario, y un "mandatario" utiliza diferentes puertos WAN para que se correspondan con diferentes grupos de UEs o grupos de sesiones IPv6. Por ejemplo, en la figura 5 un puerto WAN 0 corresponde al usuario 1 hasta el usuario n.

Para la vigilancia del estado activo de la "sesión IPv6" entre el UE y la BNG, la HGW recibe un mensaje BFD o NUD enviado por el UE a través de un puerto de red de área local (LAN) correspondiente. Para el mensaje BFD se reconstruye un mensaje de vigilancia del estado activo de un salto siguiente, es decir que se cambian tanto una dirección de origen como una dirección de destino del mensaje de vigilancia del salto siguiente; por ejemplo, en la dirección de enlace ascendente se modifica la dirección de destino convirtiéndola en la dirección de la BNG y se modifica la dirección de origen convirtiéndola en la dirección de la HGW. El procesamiento incluye específicamente: Se modifica el primer valor del campo discriminador en el mensaje BFD convirtiéndolo en la diferencia entre el prefijo de dirección IP del UE y el prefijo de dirección IP de la HGW, y luego el mensaje BFD reconstruido, incluyendo el primer valor modificado del campo discriminador, es enviado a la BNG a través de un puerto WAN correspondiente a los diferentes puertos LAN. Para el mensaje NUD, la HGW recibe el mensaje NUD enviado por el UE, reconstruye un mensaje BFD de un salto siguiente y envía el mensaje BFD reconstruido a la BNG. En la dirección de enlace descendente la HGW recibe el mensaje BFD enviado por la BNG a través de un puerto WAN, en donde el primer valor del campo discriminador en el mensaje BFD es la diferencia entre el prefijo de dirección IP del UE y el prefijo de dirección IP de la HGW, modifica el primer valor del campo discriminador convirtiéndolo en un valor correspondiente al prefijo de dirección IP del UE, reconstruye el mensaje BFD y envía el mensaje BFD, incluyendo el primer valor modificado del campo discriminador, al UE a través de los puertos LAN correspondientes.

La vigilancia de "sesión IPv6" activa entre la HGW y la BNG incluye: La HGW recibe el mensaje BFD enviado por la BNG y vigila si una sesión IP entre la HGW y la BNG está activa de acuerdo con un segundo valor del campo discriminador en el mensaje BFD, en donde el segundo valor del campo discriminador se ajusta a un valor especial, por ejemplo "0" o "0xFFFF". En la dirección de enlace descendente la BNG envía el mensaje BFD a la HGW, y la HGW puede determinar la "sesión BFD" correspondiente de acuerdo con el valor del campo "discriminador" en el mensaje BFD y, por consiguiente, puede vigilar un estado activo de la "sesión IP" asociada. La BNG recibe el mensaje BFD enviado por la HGW y vigila si la sesión IP entre la BNG y la HGW está activa de acuerdo con el segundo valor del campo discriminador en el mensaje BFD. En la dirección de enlace ascendente, después de recibir el mensaje BFD enviado por la BNG, la HGW puede determinar la "sesión BFD" correspondiente de acuerdo con el valor del campo "discriminador" en el mensaje BFD y, por consiguiente, puede vigilar un estado activo de la "sesión IP" asociada.

Específicamente, la "sesión BFD" adoptada para el estado "activo" de la "sesión IPv6" de un solo salto ejecuta una interacción "activa" con una dirección de la HGW o una dirección de la BNG, y el campo "discriminador" del mensaje BFD se ajusta a un valor especial, por ejemplo "0" o "0xFFFF".

La "sesión IPv6 activa" de la "sesión IPv6" multisalto se completa adoptando dos saltos únicos. A través de un procedimiento "activo" en el que el "mandatario" retransmite el primer salto y el segundo salto, se mantiene la sincronización de estado "activo" entre el primer salto y el segundo salto, y el campo "discriminador" de la "sesión BFD" puede ajustarse o modificarse a través del "mandatario".

El primer salto ejecuta la función "activa" adoptando la "sesión NUD/BFD" de un solo salto y el segundo salto ejecuta la función "activa" adoptando la "sesión BFD" de un solo salto.

La "sesión NUD/BFD" de un solo salto adoptada por el primer salto ejecuta la interacción "activa" con la dirección del usuario o la dirección del "mandatario", en donde la dirección del "mandatario" puede ser una dirección de un puerto LAN de la HGW, y el campo "discriminador" del mensaje BFD se ajusta a un valor correspondiente a "prefijo Yn" (n = 1, 2, 3,…). Por ejemplo, se recomienda utilizar los últimos 32 bits del "prefijo Yn" como valor del campo

"discriminador", o bien el valor es (Yn-Z), en donde n = 1, 2, 3, …

En el primer salto el UE/HGW asocia la "sesión BFD" con una "sesión IPv6" correspondiente de acuerdo con el valor del campo "discriminador" del mensaje BFD.

La "sesión BFD" de un solo salto adoptada por el segundo salto ejecuta la interacción "activa" con la dirección de la BNG o la dirección del mandatario, en donde la dirección del mandatario puede ser una dirección de un puerto WAN de la HGW, y el campo "discriminador" del mensaje BFD se ajusta a (Yn-Z), en donde n = 1, 2, 3, …, es decir, la diferencia entre el "prefijo Yn" y el "prefijo Z".

El "mandatario de sesión IPv6 activa" modifica un valor de un campo "discriminador" de un mensaje BFD de primer salto convirtiéndolo en (Yn-Z) y luego reenvía el mensaje en el segundo salto; o bien el "mandatario de sesión IPv6 activa" modifica el valor del campo "discriminador" (Yn-Z) de un mensaje BFD de segundo salto convirtiéndolo en un valor correspondiente al "prefijo Yn" y luego reenvía el mensaje en el primer salto.

En el segundo salto la BNG/HGW asocia la "sesión BFD" con una "sesión IPv6" correspondiente de acuerdo con la dirección/prefijo IP de origen y/o el valor del campo "discriminador" en el mensaje BFD. El "mandatario" utiliza diferentes puertos WAN para que se correspondan con diferentes grupos de UEs o grupos de sesiones IPv6, y bajo el mismo puerto WAN la BNG/HGW distingue "sesiones IPv6" o grupos de "sesiones IPv6" de usuarios diferentes de acuerdo con el valor del campo "discriminador" en el mensaje BFD.

Opcionalmente, la "sesión BFD" de un solo salto utiliza el "prefijo Z" como identificador de la "sesión"; y la "sesión BFD" multisalto utiliza el "prefijo Z" o el "prefijo Yn" como identificador de la "sesión".

Tomando la figura 5 como ejemplo, una "sesión IP 0" puede identificarse con un "prefijo Z" y adoptar una "sesión BFD 0" para soportar el estado "activo", y el campo "discriminador" del mensaje BFD se ajusta a "0" o "0xFFFF"; y el BNG/UE asocia la "sesión BFD 0" con una "sesión IPv6 0" correspondiente de acuerdo con el prefijo de dirección IP de origen "prefijo Z" y el valor del campo "discriminador" (0 o 0xFFFF) del mensaje BFD.

Una "sesión IP 1" puede identificarse con un "prefijo Y1" y adoptar una "sesión BFD 11" y la "sesión BFD 0" para soportar el estado "activo", y el campo "discriminador" del mensaje de la "sesión BFD 0" se ajusta a (Y1-Z); la BNG/HGW asocia la "sesión BFD 0" con una "sesión IPv6 1" correspondiente de acuerdo con el prefijo de dirección IP de origen "prefijo Z" y el valor del campo "discriminador" (Y1-Z) del mensaje BFD; y el HGW/UE asocia la "sesión BFD 11" con una "sesión IPv6 1" correspondiente de acuerdo con el prefijo de dirección IP de origen "prefijo Y1" del mensaje BFD.

Una sesión IP n puede identificarse con un "prefijo Yn" y adoptar una "sesión BFD 1n" y la "sesión BFD 0" para soportar el estado "activo", y el campo "discriminador" del mensaje de la "sesión BFD 0" se ajusta a (Yn-Z); y el campo "discriminador" de la "sesión BFD 1n" se ajusta a los últimos 32 bits del "prefijo Yn". La BNG/HGW asocia la "sesión BFD 0" con una "sesión IPv6 n" correspondiente de acuerdo con el prefijo de dirección IP de origen "prefijo Z" y el valor del campo "discriminador" (Yn-Z) del mensaje BFD; y el HGW/UE asocia la "sesión BFD 1n" con una "sesión IPv6 n" correspondiente de acuerdo con el prefijo de dirección IP de origen "prefijo Yn" del mensaje "BFD".

En el procedimiento de reenvío del mensaje de detección y de vigilancia del estado activo de la "sesión IPv6" la HGW ejecuta, además, una operación de sincronización de estado de homólogos de sesión. La operación incluye: El "mandatario" recoge un código de diagnóstico (código de diagnóstico BFD) o un estado NUD de un salto en la "sesión IP" y ejecuta una expresión en el otro salto a través del código de diagnóstico (código de diagnóstico BFD) o el estado NUD.

Tomando la figura 5 como ejemplo, cuando tanto el primer salto como el segundo salto son la "sesión BFD", en la dirección de enlace ascendente el "mandatario" se encarga de replicar un valor de "código de diagnóstico" del mensaje BFD del primer salto convirtiéndolo en un campo de "código de diagnóstico" del mensaje BFD del segundo salto, o bien el "mandatario" se encarga de diagnosticar un estado activo de un homólogo de sesión 1 (homólogo1) del primer salto, generar luego un código de diagnóstico correspondiente (código de diagnóstico BFD) para el estado activo del homólogo de sesión 1 (homólogo1) y notificarlo a un homólogo de sesión 2 (homólogo2) a través de un mensaje BFD. La BNG distingue el estado activo de "sesiones IPv6" de usuarios diferentes de acuerdo con el valor del campo "discriminador" del mensaje BFD; y en la dirección de enlace descendente el "mandatario" se encarga de replicar un valor "de código de diagnóstico" del mensaje BFD del segundo salto convirtiéndolo en un campo de "código de diagnóstico" de los mensajes BFD de primer salto de todas las "sesiones IP", o bien el "mandatario" se encarga de diagnosticar el estado activo del homólogo de sesión 2 (homólogo2) del segundo salto, generar luego un código de diagnóstico correspondiente (código de diagnóstico BFD) para el estado activo del homólogo de sesión 2 (homólogo2) y notificarlo al homólogo de sesión 1 (homólogo1) de todas las "sesiones IP" del código de diagnóstico a través de un mensaje BFD del primer salto.

Cuando un salto es la NUD, mientras que el otro salto es una "sesión BFD", en la dirección de enlace ascendente el "mandatario" se encarga de diagnosticar el estado activo del homólogo de sesión 1 (homólogo1) del primer salto a

través de un mecanismo NUD, generar luego un código de diagnóstico correspondiente (código de diagnóstico BFD) para el estado activo del primer salto y notificarlo al homólogo de sesión 2 (homólogo2) a través de un mensaje BFD. La BNG distingue el estado activo de "sesión IPv6" de usuarios diferentes de acuerdo con el valor del campo "discriminador" del mensaje BFD; por ejemplo, después de enviar un mensaje de solicitación de vecino (NS) al homólogo 1, si el "mandatario" no recibe un mensaje de aviso de vecino (NA) respondido por el homólogo 1 en un tiempo dado, el "mandatario" genera un código de diagnóstico correspondiente (código de diagnóstico BFD), tal como un "código de diagnóstico = 1" indicando tiempo de detección de control expirado, un "código de diagnóstico = 2" indicando función de eco fallida o un "código de diagnóstico = 3" indicando sesión señalada de vecino caída del homólogo 1, y luego lo notifica al homólogo2 a través de un mensaje BFD.

Como alternativa, cuando un salto es la NUD, mientras que el otro salto es la "sesión BFD", en la dirección de enlace descendente el "mandatario" se encarga de generar una acción NUD correspondiente en los primeros saltos de todas las "sesiones IP" de acuerdo con el valor de "código de diagnóstico" del mensaje BFD del segundo salto. Por ejemplo, cuando el "código de diagnóstico" del mensaje BFD del segundo salto indica sesión señalada de vecino caída, ruta caída, tiempo de detección de control expirado, función de eco fallida, plano de reenvío repuesto o administrativamente caído del homólogo 2, el "mandatario" indica vecino inalcanzable a los homólogos de todas las "sesiones IP" a través de la NUD; por ejemplo, después de recibir el mensaje NS del homólogo 1, el "mandatario" puede no retornar el mensaje NA al homólogo 1, o bien el "mandatario" deja activamente de iniciar el mensaje NS para el homólogo 1.

En la figura 6 se muestra otro caso más del modo de mandatario. La figura 6 es un diagrama esquemático de un método de vigilancia del estado activo de una sesión IP de acuerdo con una tercera realización de la presente invención. En esta realización un "mandatario de sesión IPv6 activa" dispuesto en una HGW realiza una vigilancia del estado activo de una "sesión IPv6 de múltiples saltos" en un modo de mandatario, y un mandatario utiliza diferentes puertos WAN para que se correspondan con diferentes UEs o sesiones IPv6. Por ejemplo, en la figura 6 un puerto WAN 1 corresponde a un usuario 1 y un puerto WAN n corresponde a un usuario n.

Para la vigilancia del estado activo de la "sesión IPv6" entre el UE y la BNG, la HGW recibe un mensaje BFD o NUD enviado por el UE a través de un puerto LAN. Para el mensaje BFD se reconstruye un mensaje de vigilancia del estado activo de un salto siguiente, es decir que se cambian tanto una dirección de origen como una dirección de destino del mensaje de vigilancia del salto siguiente. Por ejemplo, en la dirección de enlace ascendente se modifica la dirección de destino convirtiéndola en la dirección de la BNG y se modifica la dirección de origen convirtiéndola en la dirección de la HGW, lo que incluye específicamente: Se modifica el primer valor del campo discriminador en el mensaje BFD convirtiéndolo en un valor correspondiente al prefijo de dirección IP del UE, y el mensaje BFD reconstruido, incluyendo el primer valor modificado del campo discriminador, es enviado luego a la BNG a través de un puerto WAN correspondiente al puerto LAN. Para el mensaje NUD, la HGW recibe el mensaje NUD enviado por el UE, reconstruye un mensaje BFD de un salto siguiente y envía el mensaje BFD reconstruido a la BNG. En la dirección de enlace descendente la HGW recibe el mensaje BFD enviado por la BNG a través de un puerto WAN, en donde el primer valor del campo discriminador en el mensaje BFD es un valor correspondiente al prefijo de dirección IP del UE, reconstruye un mensaje BFD o NUD y envía el mensaje NUD o el mensaje BFD, incluyendo el primer valor del campo discriminador, al UE a través de un puerto LAN correspondiente al puerto WAN.

La vigilancia de "sesión IPv6" activa entre la HGW y la BNG incluye: La HGW recibe el mensaje BFD enviado por la BNG y vigila si una sesión IP entre la HGW y la BNG está activa de acuerdo con un segundo valor del campo discriminador en el mensaje BFD, en donde el segundo valor del campo discriminador se ajusta a un valor especial, por ejemplo "0" o "0xFFFF". En la dirección de enlace descendente la BNG envía el mensaje BFD a la HGW, y la HGW puede determinar la "sesión BFD" correspondiente de acuerdo con el valor del campo "discriminador" en el mensaje BFD y, por consiguiente, puede vigilar un estado activo de la "sesión IP" asociada. La BNG recibe el mensaje BFD enviado por la HGW y vigila si la sesión IP entre la BNG y la HGW está activa de acuerdo con el segundo valor del campo discriminador en el mensaje BFD. En la dirección de enlace ascendente, después de recibir el mensaje BFD enviado por la BNG, la HGW puede determinar la "sesión BFD" correspondiente de acuerdo con el valor del campo "discriminador" en el mensaje BFD y, por consiguiente, puede vigilar un estado activo de la "sesión IP" asociada.

Específicamente, la "sesión BFD" adoptada por el estado "activo" de la "sesión IPv6" de un solo salto ejecuta una interacción "activa" con una dirección de la HGW o una dirección de la BNG, y el campo "discriminador" del mensaje BFD se ajusta a "0" o "0xFFFF".

La "sesión IPv6 activa" de la "sesión IPv6" multisalto se completa adoptando dos saltos únicos. A través de un procedimiento "activo" en el que "el mandatario" retransmite el primer salto y el segundo salto, se mantiene la sincronización de estado "activo" entre el primer salto y el segundo salto.

El primer salto ejecuta la función "activa" adoptando la "sesión NUD/BFD" de un solo salto y el segundo salto ejecuta la función "activa" adoptando la "sesión BFD" de un solo salto.

La "sesión NUD/BFD" de un solo salto adoptada por el primer salto ejecuta la interacción "activa" con la dirección del

usuario o la dirección del “mandatario”, en donde la dirección del “mandatario” puede ser un dirección de un puerto LAN de la HGW, y se ajusta el campo “discriminador” del mensaje BFD a un valor correspondiente al “prefijo Yn” (n = 1, 2, 3, …). Por ejemplo, se utilizan los últimos 32 bits del “prefijo Yn” como valor del campo “discriminador”, o bien el valor es (Yn-Z), en donde n = 1, 2, 3, …

En el primer salto el UE/HGW asocia la “sesión BFD” con una “sesión IPv6” correspondiente de acuerdo con el valor del campo “discriminador” en el mensaje BFD.

La “sesión BFD” de un solo salto adoptada por el segundo salto ejecuta la interacción “activa” con la dirección de la BNG o la dirección del “mandatario”, en donde la dirección del “mandatario” puede ser una dirección de un puerto WAN de la HGW, y el campo “discriminador” del mensaje BFD se ajusta a un valor correspondiente al “prefijo Yn” (n = 1, 2, 3, …). Por ejemplo, se utilizan los últimos 32 bits del “prefijo Yn” como valor del campo “discriminador”, o bien el valor es (Yn-Z), en donde n = 1, 2, 3, …

En el segundo salto la BNG/HGW asocia la “sesión BFD” con una “sesión IPv6” correspondiente de acuerdo con la dirección/prefijo IP de origen y/o el valor del campo “discriminador” en el mensaje BFD. El “mandatario” corresponde a UEs o sesiones IPv6 diferentes adoptando diferentes puertos WAN, y la BNG/HGW distingue “sesiones IPv6” de diferentes usuarios de acuerdo con el valor del campo “discriminador” en el mensaje BFD.

Opcionalmente, la “sesión BFD” de un solo salto utiliza el “prefijo Z” como identificador de la “sesión”; y la “sesión BFD” multisalto utiliza el “prefijo Z” o el “prefijo Yn” como identificador de la “sesión”.

Tomando la figura 6 como ejemplo, una “sesión IP 0” puede identificarse con un “prefijo Z” y adoptar una “sesión BFD 0” para soportar el estado “activo”, y el campo “discriminador” del mensaje BFD se ajusta a “0” o “0xFFFF”; y el BNG/UE asocia la “sesión BFD 0” con una “sesión IPv6 0” correspondiente de acuerdo con el prefijo de dirección IP de origen “prefijo Z” del mensaje BFD.

Una “sesión IP 1” puede identificarse con un “prefijo Y1” y adoptar una “sesión BFD 11” y una “sesión BFD 21” para soportar el estado “activo” y el campo “discriminador” del mensaje de la “sesión BFD 21” se ajusta a (Y1-Z); la BNG/HGW asocia la “sesión BFD 21” con una “sesión IPv6 1” correspondiente de acuerdo con el prefijo de dirección IP de origen “prefijo Y1” del mensaje BFD; y el HGW/UE asocia la “sesión BFD 11” con una “sesión IPv6 1” correspondiente de acuerdo con el prefijo de dirección IP de origen “prefijo Y1” del mensaje BFD.

Una “sesión IP n” puede identificarse con un prefijo Yn y adoptar una “sesión BFD 1n” y una “sesión BFD 2n” para soportar el estado “activo”, y el campo “discriminador” del mensaje BFD de la “sesión BFD 2n” se ajusta a (Yn-Z); y el campo “discriminador” del mensaje BFD de la “sesión BFD 1n” se ajusta a los últimos 32 bits del “prefijo Yn”. La BNG/HGW asocia la “sesión BFD 2n” con una “sesión IPv6 n” correspondiente de acuerdo con el prefijo de dirección IP de origen “prefijo Yn” del mensaje BFD; y el HGW/UE asocia la “sesión BFD 1n” con una sesión IPv6 n” correspondiente de acuerdo con el prefijo de dirección IP de origen “prefijo Yn” del mensaje BFD.

En el procedimiento de reenvío del mensaje de detección y de vigilancia del estado activo de la “sesión IPv6”, la HGW ejecuta, además, una operación de sincronización de estado de homólogos de sesión. La operación puede incluir: El “mandatario” recoge un código de diagnóstico (código de diagnóstico BFD) o un estado NUD, tal como un vecino inalcanzable de un salto en la “sesión IP”, y ejecuta una expresión sobre el otro salto a través del código de diagnóstico (código de diagnóstico BFD) o la NUD.

Por ejemplo, cuando tanto el primer salto como el segundo salto son la “sesión BFD”, el “mandatario” se encarga de replicar un valor de “código de diagnóstico” del mensaje “BFD” de un salto convirtiéndolo en un campo de “código de diagnóstico” del mensaje BFD del otro salto, o bien el “mandatario” se encarga de diagnosticar un estado activo de un homólogo de sesión 1 (homólogo1) de un salto, generar luego un código de diagnóstico correspondiente (código de diagnóstico BFD) para el estado activo del homólogo de sesión 1 (homólogo1) y notificarlo a un homólogo de sesión 2 (homólogo2) a través de un mensaje BFD.

Cuando un salto es la NUD, mientras que el otro salto es la “sesión BFD”, en la dirección de enlace ascendente el “mandatario” se encarga de diagnosticar el estado activo del homólogo de sesión 1 (homólogo1) del primer salto a través de un mecanismo NUD, generar luego un código de diagnóstico correspondiente (código de diagnóstico BFD) para el estado activo del primer salto y notificarlo al homólogo de sesión 2 (homólogo2) a través de un mensaje BFD; y, por ejemplo, después de enviar un mensaje NS al homólogo 1, si el “mandatario” no recibe un mensaje NA respondido por el homólogo 1 en un tiempo dado, el “mandatario” genera un código de diagnóstico correspondiente (código de diagnóstico BFD), tal como un “código de diagnóstico = 1” indicando tiempo de detección de control expirado, un “código de diagnóstico = 2”, indicando función de eco fallida o un “código de diagnóstico = 3” indicando sesión señalada de vecino caída del homólogo 1, y luego lo notifica al homólogo2 a través de un mensaje BFD.

Alternativamente, cuando un salto es la NUD, mientras el otro salto es la “sesión BFD”, en la dirección de enlace descendente el “mandatario” se encarga de generar una acción NUD correspondiente en el primer salto de acuerdo con el valor del “código de diagnóstico” del mensaje BFD del segundo salto. Por ejemplo, cuando el “código de

diagnóstico” del mensaje BFD del segundo salto indica sesión señalada de vecino caída del homólogo 2, ruta caída, tiempo de detección de control expirado, función de eco fallida, plano de reenvío repuesto o administrativamente caído, el “mandatario” indica vecino inalcanzable al homólogo 1 a través de la NUD; por ejemplo, después de recibir el mensaje NS del homólogo 1, el “mandatario” puede no retornar el mensaje NA al homólogo 1 o bien el “mandatario” deja de iniciar activamente el mensaje NS para el homólogo 1.

En el método de vigilancia del estado activo de una sesión IP de acuerdo con la realización de la presente invención se utiliza una “BFD multisalto” como mecanismo de vigilancia del estado activo de una “sesión IPv6 multisalto” o bien un “mandatario de sesión IPv6 activa” está dispuesto en la HGW, de modo que se puede establecer una “sesión IPv6” entre el UE siguiente a la HGW y el nodo de borde IP, y se puede extender una “sesión IP de un solo salto” a una “sesión IP multisalto”, realizando así una vigilancia del estado activo de la “sesión IPv6 de múltiples saltos”.

Los expertos ordinarios en la materia pueden comprender que la totalidad o parte de los pasos del método según las realizaciones puede implementarse con un programa que dé instrucciones al hardware relevante. El programa puede almacenarse en un medio de almacenaje legible por ordenador. Cuando se ejecuta el programa, se llevan a cabo los pasos del método según las realizaciones. El medio de almacenaje puede ser cualquier medio que sea capaz de almacenar códigos de programa, tal como una memoria de solo lectura (ROM), una memoria de acceso aleatorio (RAM), un disco magnético o un disco óptico.

La figura 7 es un diagrama estructural esquemático de una HGW según una realización de la presente invención. Como se muestra en la figura 7, la HGW incluye un primer módulo de recepción 11 y un primer módulo de reenvío 12, en donde el primer módulo de recepción 11 está configurado para recibir un mensaje BFD enviado por un UE o un nodo de borde IP; y el primer módulo de reenvío 12 está configurado para enviar el mensaje BFD, incluyendo un primer valor de campo discriminador, al nodo de borde IP o al UE de acuerdo con el mensaje BFD recibido por el primer módulo de recepción, en donde el primer valor del campo discriminador es una diferencia entre un prefijo de dirección IP del UE y un prefijo de dirección IP de la HGW. Específicamente, el primer módulo de recepción 11 recibe el mensaje BFD enviado por el UE o una BNG, y si el primer valor del campo discriminador en el mensaje BFD es la diferencia entre el prefijo de dirección IP del UE y el prefijo de dirección IP de la HGW, el mensaje BFD es reenviado directamente al UE o a la BNG; y si el primer valor del campo discriminador en el mensaje BFD no es la diferencia entre el prefijo de dirección IP del UE y el prefijo de dirección IP de la HGW, se modifica el primer valor del campo discriminador convirtiéndolo en la diferencia entre el prefijo de dirección IP del UE y el prefijo de dirección IP de la HGW, y se reenvía el mensaje BFD modificado al UE o a la BNG.

La HGW según esta realización incluye, además, un módulo de mandatario 13 configurado para modificar el primer valor del campo discriminador en el mensaje BFD recibido por el primer módulo de recepción 11. Específicamente, para habilitar la HGW como “enrutador” a fin de realizar la vigilancia del estado activo de la “sesión IP” entre el UE conectado a la HGW y el nodo de borde IP, tal como la BNG, se añade una función de mandatario en la HGW y la retransmisión del primer salto al segundo salto se realiza a través del mandatario. El primer módulo de recepción 11 recibe un mensaje de detección BFD enviado por el UE o la BNG y el módulo de mandatario 13 modifica un valor del campo discriminador en el mensaje de detección de acuerdo con la situación real de modo que el mensaje sea adecuado para ser transportado en un salto siguiente, consiguiendo así el propósito de una vigilancia del estado activo. Después de modificar el valor del campo discriminador, el módulo de mandatario 13 envía el mensaje de detección, incluyendo el valor modificado del campo discriminador, a un extremo de destino – que puede ser el UE o la BNG – de un salto siguiente a través del primer módulo de reenvío 12.

La HGW según esta realización, incluye, además, un módulo de emisión 14 configurado para enviar un mensaje de detección, incluyendo un segundo valor del campo discriminador, a la BNG, en donde el segundo valor del campo discriminador es “0” o “0xFFFF”. La HGW realiza la vigilancia del estado activo de la sesión entre la HGW y la BNG a través del módulo de emisión 14.

En la HGW según esta realización está dispuesto un “mandatario de sesión IPv6 activa” en la HGW, de modo que se puede establecer una “sesión IPv6” entre el UE siguiente a la HGW y el nodo de borde IP, y se puede extender una “sesión IP de un solo salto” a una “sesión IP multisalto”, realizando así una vigilancia del estado activo de la “sesión IPv6 de múltiples saltos”.

La figura 8 es un diagrama estructural esquemático de un dispositivo de red según una realización de la presente invención. Como se muestra en la figura 8, el dispositivo de red incluye un segundo módulo de recepción 21 y un módulo de procesamiento 22. El dispositivo de red recibe, a través del segundo módulo de recepción 21, un mensaje BFD enviado por una HGW, en donde un primer valor del campo discriminador incluido en el mensaje BFD es una diferencia entre un prefijo de dirección IP de un UE y un prefijo de dirección IP de la HGW; y luego vigila, a través del módulo de procesamiento 22, si una sesión IP entre un nodo de borde IP y el UE está activa de acuerdo con el primer valor del campo discriminador en el mensaje BFD. El módulo de procesamiento está configurado, además, para determinar si una sesión BFD correspondiente al primer valor del campo discriminador está activa de acuerdo con el primer valor del campo discriminador en el mensaje BFD, y para determinar si una sesión IP asociada con la sesión BFD está activa de acuerdo con si la sesión BFD está activa.

El dispositivo de red según esta realización puede ser el UE o una BNG, el cual realiza la vigilancia del estado activo en una “sesión IPv6” entre el UE y la BNG a través de un mensaje BFD enviado por la HGW.

La figura 9 es un diagrama estructural esquemático de un sistema de vigilancia del estado activo de una sesión IP de acuerdo con una realización de la presente invención. Como se muestra en la figura 9, el sistema de vigilancia del estado activo de una sesión IP incluye una HGW 1 y un dispositivo de red 2. La HGW 1 está configurada para enviar un mensaje BFD al dispositivo de red, en donde un primer valor del campo discriminador en el mensaje BFD es una diferencia entre un prefijo de dirección IP de un UE y un prefijo de dirección IP de la HGW; y el dispositivo de red 2 está configurado para recibir el mensaje BFD enviado por la HGW y vigilar si una sesión IP entre un nodo de borde IP y el UE está activa de acuerdo con el primer valor del campo discriminador en el mensaje BFD.

La HGW y el dispositivo de red implicados en el sistema de vigilancia del estado activo de una sesión IP de acuerdo con esta realización pueden adoptar las premisas de la HGW y el dispositivo de red según las realizaciones anteriores, y no se describen aquí nuevamente los detalles.

En el sistema de vigilancia del estado activo de una sesión IP según esta realización se dispone un “mandatario de sesión IPv6 activa” en la HGW, de modo que puede establecerse una “sesión IPv6” entre el UE siguiente a la HGW y el nodo de borde IP, y se puede extender una “sesión IP de un solo salto” a una “sesión IP multisalto”, realizando así una vigilancia del estado activo de la “sesión IPv6 de múltiples saltos”.

Finalmente, deberá hacerse notar que las realizaciones anteriores se proporcionan meramente para describir las soluciones técnicas de la presente invención, pero no están destinadas a limitar la presente invención. Deberá entenderse por los expertos ordinarios de la materia que, aunque se ha descrito en detalle la presente invención con referencia a las realizaciones, se pueden hacer modificaciones en las soluciones técnicas descritas en las reivindicaciones o se pueden efectuar sustituciones equivalentes en algunas características técnicas de las soluciones técnicas.

REIVINDICACIONES

1. Un método de vigilancia del estado activo de sesiones de protocolo de Internet, IP, **caracterizado** porque comprende:

recibir, por un equipo de usuario, UE, o un nodo de borde IP, un mensaje de detección de reenvío bidireccional, BFD, enviado por una pasarela doméstica, HGW, en donde un primer valor de campo discriminador comprendido en el mensaje BFD es una diferencia entre un prefijo de dirección IP del UE y un prefijo de dirección IP de la HGW; y

vigilar, por el UE o el nodo de borde IP, si una sesión IP entre el nodo de borde IP y el UE está activa de acuerdo con el primer valor del campo discriminador en el mensaje BFD;

en donde el UE se conecta al nodo de borde IP a través de la HGW.

2. El método de vigilancia del estado activo de sesiones IP según la reivindicación 1, en el que la vigilancia de si una sesión IP entre el nodo de borde IP y el UE está activa comprende:

determinar si una sesión BFD correspondiente al primer valor del campo discriminador está activa de acuerdo con el primer valor del campo discriminador en el mensaje BFD, y determinar si la sesión IP asociada con la sesión BFD está activa de acuerdo con si la sesión BFD está activa.

3. El método de vigilancia del estado activo de sesiones IP según la reivindicación 1 ó 2, en el que el mensaje BFD comprende, además, un segundo valor del campo discriminador, y el segundo valor del campo discriminador es “0” o “0xFFFF”.

4. El método de vigilancia del estado activo de sesiones IP según la reivindicación 3, que comprende además:

vigilar, por la HGW o el nodo de borde IP, si una sesión IP entre el nodo de borde IP y la HGW está activa de acuerdo con el segundo valor del campo discriminador en el mensaje BFD.

5. El método de vigilancia del estado activo de sesiones IP según la reivindicación 1 ó 2, en el que, antes de recibir, por el UE o el nodo de borde IP, el mensaje BFD enviado por la HGW, el método comprende además:

modificar, por la HGW, el primer valor del campo discriminador comprendido en el mensaje BFD convirtiéndolo en la diferencia entre el prefijo de dirección IP del UE y el prefijo de dirección IP de la HGW, y reenviar después el mensaje BFD modificado al UE o al nodo de borde IP.

6. Una pasarela doméstica, HGW, que comprende:

un módulo de recepción (11) configurado para recibir un mensaje de detección de reenvío bidireccional, BFD, enviado por un equipo de usuario, UE, o un nodo de borde de protocolo de Internet, IP, en donde el UE está conectado al nodo de borde IP a través de la HGW; y

caracterizada porque incluye un módulo de reenvío (12) configurado para enviar un mensaje BFD que comprende un primer valor de campo discriminador al nodo de borde IP o al UE de acuerdo con el mensaje BFD recibido por el módulo de recepción, en donde el primer valor del campo discriminador es una diferencia entre un prefijo de dirección IP del UE y un prefijo de dirección IP de la HGW.

7. La HGW según la reivindicación 6, que comprende además:

un módulo mandatario (13) configurado para modificar el mensaje BFD recibido por el módulo de recepción convirtiéndole en el módulo BFD que comprende el primer valor del campo discriminador.

8. La HGW según la reivindicación 6 ó 7, que comprende además:

un módulo de emisión (14) configurado para enviar un mensaje BFD, que comprende un segundo valor del campo discriminador, al nodo de borde IP, en donde el segundo valor del campo discriminador es “0” o “0xFFFF”.

9. La HGW según la reivindicación 7, en la que:

el módulo de mandatario (13) está configurado, además, para recoger un código de diagnóstico o un estado de detección de vecino inalcanzable, NUD, en un salto de una sesión IP y para enviar el código de diagnóstico o el estado NUD a un homólogo de sesión en otro salto de la sesión IP a través del mensaje BFD.

10. Un dispositivo de red **caracterizado** porque comprende:

un módulo de recepción (21) configurado para recibir un mensaje de detección de reenvío bidireccional, BFD, enviado por una pasarela doméstica, HGW, en donde un primer valor de campo discriminador comprendido en el

mensaje BFD es una diferencia entre un prefijo de dirección de protocolo de Internet, IP, de un equipo de usuario, UE, y un prefijo de dirección IP de la HGW; y

un módulo de procesamiento (22) configurado para vigilar si una sesión IP entre un nodo de borde IP y el UE está activa de acuerdo con el primer valor del campo discriminador en el mensaje BFD;

en donde el dispositivo de red es un nodo de borde IP y el UE está conectado al nodo de borde IP a través de la HGW.

11. El dispositivo de red según la reivindicación 10, en el que el módulo de procesamiento (22) está configurado, además, para determinar si una sesión BFD correspondiente al primer valor del campo discriminador está activa de acuerdo con el primer valor del campo discriminador en el mensaje BFD, y para determinar si una sesión IP asociada con la sesión BFD está activa de acuerdo con si la sesión BFD está activa.

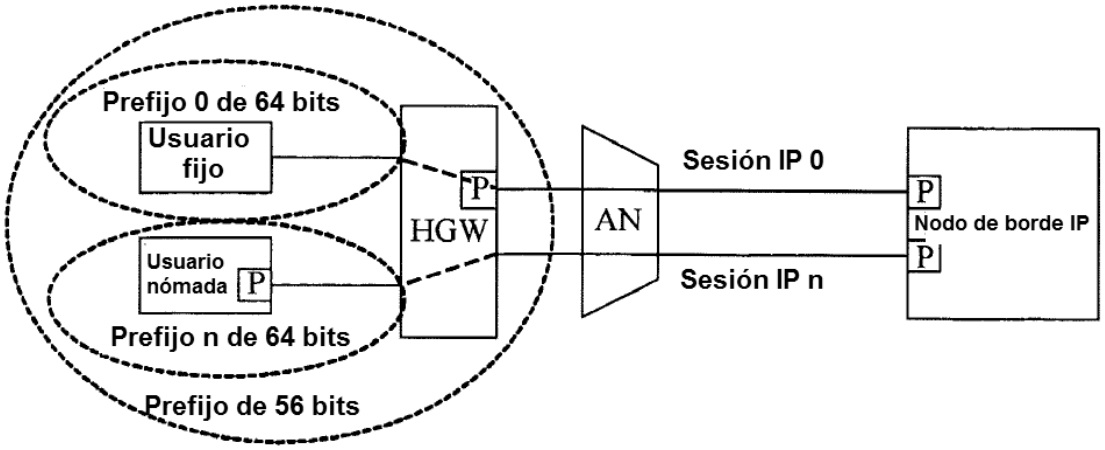

FIG. 1

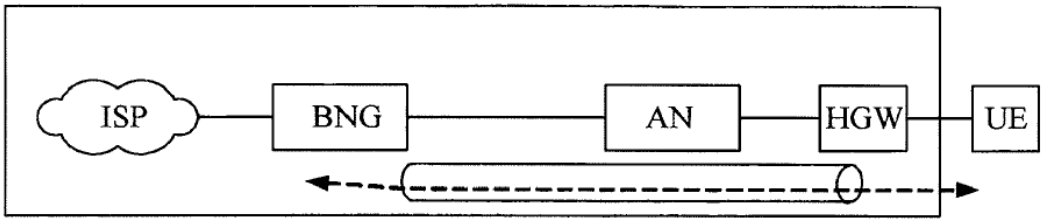

FIG. 2

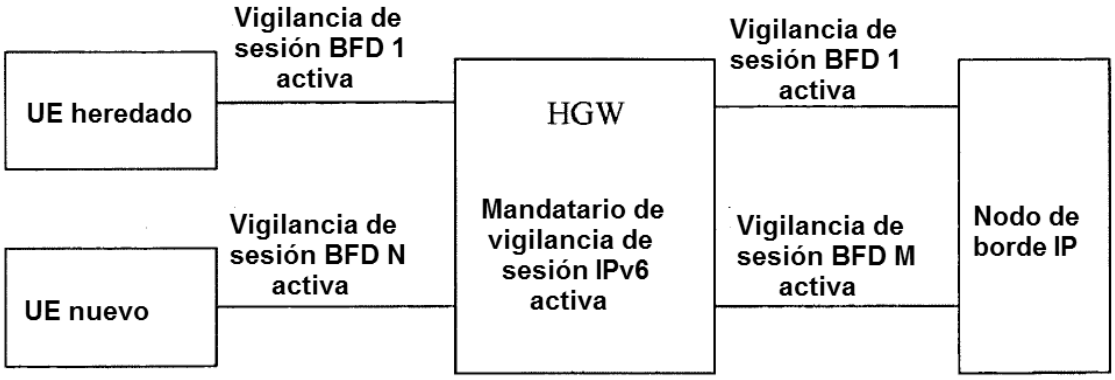

FIG. 3

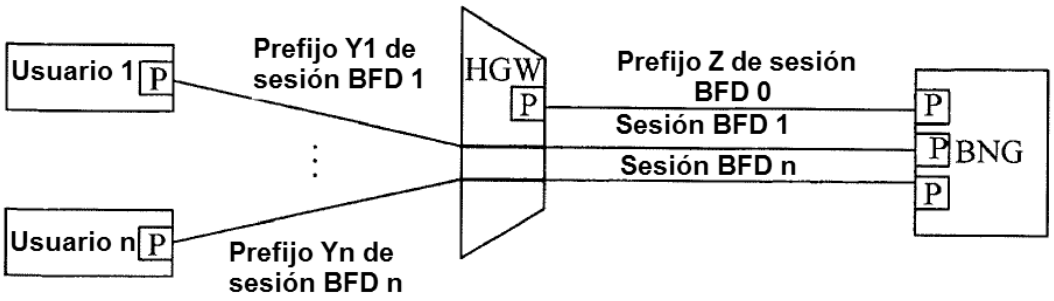

FIG. 4

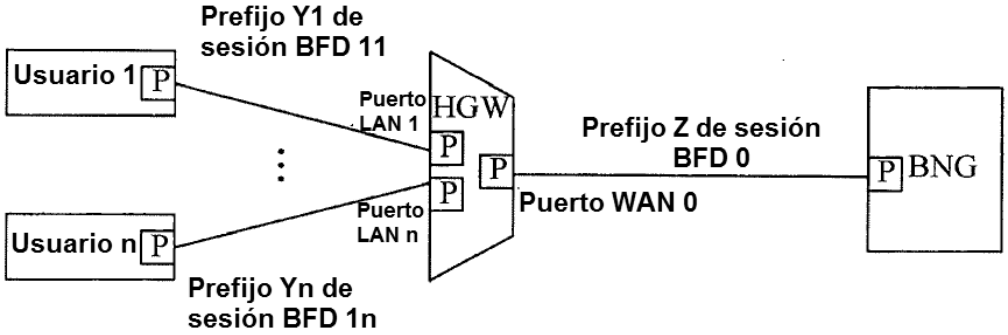

FIG. 5

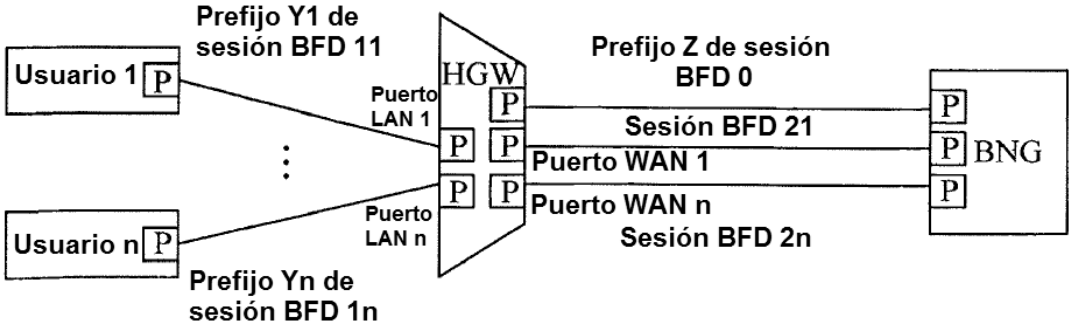

FIG. 6

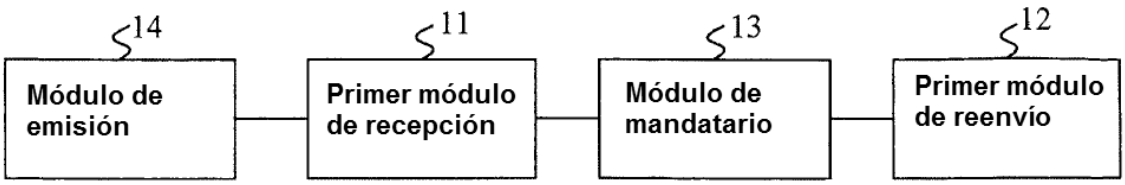

FIG. 7

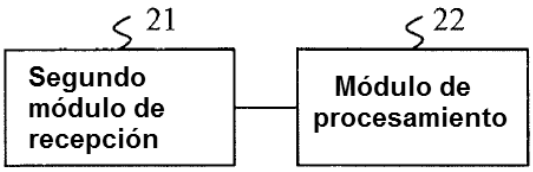

FIG. 8

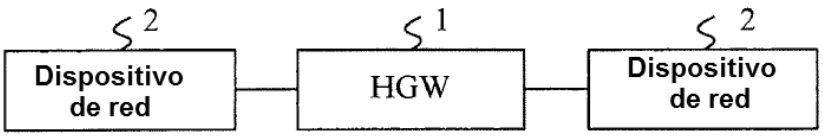

FIG. 9