

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 321 213**

51 Int. Cl.:

H04L 12/46 (2006.01)

H04L 29/06 (2006.01)

H04L 12/28 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA MODIFICADA
TRAS OPOSICIÓN

T5

96 Fecha de presentación y número de la solicitud europea: **13.06.2005 E 05757338 (8)**

97 Fecha y número de publicación de la concesión europea modificada tras oposición: **14.01.2015 EP 1753175**

54

Título: **Procedimiento para la implementación de Operación en Red Privada Virtual**

30

Prioridad:

11.06.2004 CN 200410048698

45

Fecha de publicación y mención en BOPI de la
traducción de la patente modificada:
27.04.2015

73

Titular/es:

**HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian,
Longgang District
Shenzhen, Guangdong 518129 , CN**

72

Inventor/es:

DONG, WEISI

74

Agente/Representante:

LEHMANN NOVO, María Isabel

ES 2 321 213 T5

DESCRIPCIÓN

Procedimiento para la implementación de Operación en Red Privada Virtual

5 Campo de la invención

La presente invención se refiere a una tecnología de Red Privada Virtual (VPN, por sus siglas en inglés), y más en particular, a un procedimiento para la implementación de una VPN basada en el protocolo de Conmutación de Etiquetas Multi-Protocolo (MPLS, por sus siglas en inglés).

10

Antecedentes de la Invención

Una VPN del Protocolo de Acceso Marginal (BGP, por sus siglas en inglés) / Conmutación de Etiquetas Multi-Protocolo (MPLS) fue propuesta en 1999, y ha constituido el estándar 2547 de Peticiones de Comentarios (RFC, por sus siglas en inglés).

15

Un modelo de VPN BGP/MPLS incluye tres partes: un dispositivo de Borde del Usuario (CE, por sus siglas en inglés), un enrutador de Borde del Proveedor (PE, por sus siglas en inglés) de red principal, y un enrutador del Proveedor (P) de red principal. De ellos, el dispositivo CE es un componente de una red de usuario y posee una interfaz que conecta con una red de operador directamente, el cual es normalmente un enrutador y no puede percibir la existencia de la VPN; el enrutador PE es un dispositivo de borde de la red del operador que conecta con un CE de un usuario directamente, y en la red MPLS, todo el procesamiento relacionado con la VPN se completa en el enrutador PE; y el enrutador P está situado en la red del operador a modo de enrutador principal, que no conecta con el enrutador de CE directamente, y que necesita disponer de capacidades básicas de señalización y envío de MPLS.

20

La división del CE y del PE se realiza principalmente en términos de ámbitos de gestión del operador y de los usuarios. El CE y el PE son los límites de los dos ámbitos de gestión. La información de enrutamiento puede ser conmutada entre el CE y el PE utilizando el BGP Externo (E-BGP), el Protocolo de Acceso Interior (IGP, por sus siglas en inglés), o rutas estáticas. No es necesario que el CE soporte el protocolo MPLS o que esté capacitado para percibir la VPN. Dentro de la VPN, se conmuta la información de enrutamiento entre los PEs en base al Protocolo de Acceso Marginal Multi-Protocolo (MP-BGP).

25

30

La VPN de BGP/MPLS definida por el RFC 2547 va a ser descrita en lo que sigue con detalle.

1. Una instancia de Enrutamiento/Envío de VPN (VRF, por sus siglas en inglés)

Una VPN de BGP/MPLS se compone de múltiples sitios de usuario. Múltiples VRFs están salvados en un PE. Cada VRF corresponde a un sitio de usuario, y el contenido de un VRF incluye principalmente: una tabla de rutas de IP (Protocolo de Internet), una tabla de envío de etiquetas, y una serie de información de interfaz y de información de gestión que hace uso de la tabla de envío de etiquetas. De estas, la información de interfaz y la información de gestión incluyen: un Distinguidor de Ruta (RD, por sus siglas en inglés), una política de filtrado de ruta, una lista de interfaz de miembros, etc. Un VRF de un sitio de usuario en la VPN, integra realmente la relación del miembro de la VPN y las normas de enrutamiento del sitio de usuario. La información de envío de mensajes se salva en la tabla de rutas de IP y en la tabla de envío de etiquetas de cada VRF. El sistema mantiene un conjunto independiente de tabla de enrutamiento y tabla de envío de etiquetas para cada VRF, evitando con ello que los datos escapen de la VPN e impidiendo que los datos de fuera de la VPN entren.

35

40

2. Una familia de direcciones de VPN-Protocolo de Internet versión 4 (VPN- IPv4)

En una VPN de BGP/MPLS, el BGP se utiliza para distribuir rutas de VPN entre los enrutadores de PE adoptando la nueva familia de direcciones de VPN-IPv4. En estas, una dirección de VPN- IPv4 contiene 12 bytes, empezando por un RD de 8 bytes, y terminando con una dirección IPv4 de 4 bytes. El operador puede distribuir un RD independiente, sin embargo, necesita hacer que su número privado de Sistema Autónomo (AS, por sus siglas en inglés) forme parte del RD para asegurar la unicidad global de cada RD. La dirección de VPN- IPv4, de la que el RD sea cero, es sinónima de la dirección IPv4 globalmente única. Tras este procesamiento, incluso la dirección IPv4 de 4 bytes contenida en la dirección de VPN-IPv4 se solapa, pudiendo la dirección de VPN-IPv4 mantener aún su unicidad global. Además, la ruta, que el enrutador de PE recibe desde el enrutador de CE, es una ruta IPv4, de modo que la ruta necesita ser introducida en la tabla de rutas de VRF con el fin de que un RD pueda ser vinculado a la ruta. En aplicaciones prácticas, todas las rutas del mismo sitio de usuario pueden estar configuradas con un RD idéntico.

45

50

55

3. Atributos de VPN-Objetivo

Los atributos de VPN-Objetivo determinan finalmente la división de la VPN en la red global. La VPN de MPLS/BGP no posee ninguna etiqueta explícita de VPN, por lo que depende principalmente del atributo de VPN-Objetivo para determinar las rutas de qué sitios entre los que un sitio puede recibir, y en qué sitio las rutas del sitio pueden ser recibidas. Existen dos conjuntos de atributos VPN-Objetivo en el enrutador de PE: un conjunto es para el comienzo vinculado a una ruta recibida desde un sitio, denominado Exportar VPN-Objetivos, mientras que el otro conjunto es para determinar qué ruta puede ser introducida en la tabla de rutas del sitio, denominado Importar VPN-Objetivos. Emparejando los atributos de Objetivo de Ruta transportados por la ruta, es posible obtener la relación de miembro de la VPN. Además, se puede utilizar también un emparejamiento de los atributos de Objetivo de Ruta para filtrar la

60

65

información de enrutamiento recibida por el enrutador de PE, es decir, cuando la información de enrutamiento entra en el enrutador de PE, si existen unidades de información idénticas entre el conjunto de Exportar Objetivos de Ruta y el conjunto de Importar Objetivos de Ruta, la ruta será aceptada, y si no existen unidades de información idénticas entre el conjunto de Exportar Objetivos de Ruta y el conjunto de Importar Objetivos de Ruta, la ruta será rechazada.

5

4. Envío de mensaje de VPN

Con el fin de implementar el envío de mensaje de VPN en la VPN de BGP/MPLS, se aplica un método de etiqueta de 2 capas al envío de un mensaje de VPN. La etiqueta de la primera capa, es decir, la etiqueta de la capa externa conmutada en el interior de la red principal, representa una Trayectoria Conmutada de Etiqueta (LSP) desde un PE hasta un PE PEER, y utilizando la etiqueta de la primera capa, los mensajes pueden alcanzar el PE PEER a lo largo de la LSP correspondiente a la etiqueta de la primera capa. La etiqueta de la segunda capa, es decir, una etiqueta interior, utilizada cuando se transmite un mensaje desde el PE PEER hasta el CE, indica el sitio al que debe llegar el mensaje, o más en particular, a qué CE debe llegar el mensaje, y de acuerdo con la etiqueta de capa, es posible encontrar la interfaz destinada a enviar el mensaje al usuario. Si el sitio origen y el sitio destino del mensaje de VPN conectan ambos con el mismo PE, no existirá más el problema de cómo el mensaje alcanza al PE PEER, y el problema que debe ser resuelto consiste solamente en cómo llegar al CE que conecta con un sitio de destino.

10

15

5. Distribución de información de enrutamiento de VPN a través del BGP

La información de enrutamiento es transmitida entre el CE y el PE por medio del IGP o del EBGp. El PE obtiene la tabla de rutas de la VPN y la salva en un VRF independiente. Varios PEs adoptan el IGP para asegurar la conectividad de la red de operador, transferir la información de construcción de la VPN y las rutas a través del BGP Interno (IBGP), y completar la actualización de sus propios VRFs, respectivamente. Y después, el PE actualiza la tabla de rutas de un CE conectando directamente con el PE mediante conmutación de las rutas con el CE, realizando con ello la conmutación de la ruta entre una diversidad de CEs.

20

25

Según se aprecia a partir de la descripción que antecede, en la técnica anterior, dos enrutadores de PE intercambian información de enrutamiento de la VPN ejecutando el protocolo MBGP, y emparejan los Objetivos de Exportación de Ruta y los Objetivos de Importación de Ruta configurados en cada VRF para determinar la introducción de ruta del VRF y a qué VRF, distinto del VRF, deben ser distribuidas las rutas del VRF. Por este medio, los VRFs correspondientes pueden apropiarse de las rutas necesarias, que contengan una etiqueta, de modo que se pueda establecer una relación lógica de la VPN que garantice una capa de ruta alcanzable.

30

En la capa de envío, la etiqueta de capa externa puede asegurar que un mensaje alcanza el enrutador de PE PEER correcto, es decir, el enrutador correspondiente a la dirección de salto siguiente de la ruta de VPN. Después de que el mensaje ha llegado al enrutador de PE PEER, puede ser enviado desde la interfaz de VPN designada de acuerdo con la etiqueta de capa portada en el mensaje, o cargado en el enrutador directamente. Con ello, la etiqueta de capa constituye una parte de la ruta de VPN distribuida a través del MBGP. Se debe apreciar que también es posible adoptar otras técnicas de túnel para asegurar que el mensaje llega al enrutador de PE PEER correcto, por ejemplo, el túnel de protocolo de Encapsulamiento de Ruta Genérica (GRE) y el túnel de Protocolo de Seguridad de IP (IPsec), etc.

35

40

Se puede ver que existen varios factores claves en la técnica anterior: el establecimiento de un túnel entre dos PEs y el intercambio de información de enrutamiento de VPN entre dos PEs mediante señalización de MBGP. Al igual que para el envío del mensaje, existen dos factores claves: uno consiste en que la etiqueta de capa externa garantiza que el mensaje VPN llegue al dispositivo de PE correcto, mientras que el otro consiste en que la etiqueta interna asegure que un mensaje sea enviado desde la interfaz correcta hasta el dispositivo de CE correspondiente. Solamente cuando se satisfacen ambos factores, los CEs que conectan los dos VRFs pueden acceder, respectivamente, cada uno al otro.

45

50

Como la técnica anterior descrita en lo que antecede es relativamente compleja, la necesidad de personal de gestión será más alta en aplicaciones prácticas, de modo que no se puede realizar una configuración y un ajuste de VPN que sean flexibles, especialmente para algunos requisitos en circunstancias especiales, por ejemplo:

55

En primer lugar, existen pocas rutas que necesiten ser intercambiadas entre los enrutadores de PE, pero es necesario operar el complicado protocolo MBGP por anticipado para intercambiar rutas de VPN de acuerdo con la técnica anterior, lo que hace que la operación sea demasiado compleja y dé lugar a una necesidad excesivamente alta de personal de gestión.

60

En segundo lugar, la relación de VPN requerida no ha sido establecida entre un VRF y otro VRF, es decir, los objetivos de Importar/Exportar no se emparejan uno con el otro, sino que es necesario que el VRF acceda a algunos enrutadores de CE que conecten con otro VRF, que no pueden ser implementados utilizando la solución existente.

65

En tercer lugar, la técnica anterior no puede regular dinámicamente los dispositivos correspondientes de los VRFs en otros PEs que sean accesibles para un dispositivo de CE de acuerdo con las demandas de los usuarios.

El documento EP 1 392 033 A1 proporciona una PVN PP expandible de 3 capas que consume menos recursos y

que requiere poca configuración. Esta permite resolver el problema de que los dispositivos de PE, en la arquitectura BGP/MPLS de la VPN, pueden ser un cuello de botella en despliegues a gran escala debido a que los mismos tienen que converger en rutas procedentes de una pluralidad de VPNs. Y, el objetivo se consigue mediante un PE jerárquico (HoPE) que está formado por múltiples dispositivos de PE.

5

Sumario

La presente invención consiste en proporcionar un procedimiento para la implementación de una VPN con el fin de transmitir rutas de VPN entre dos dispositivos de PE sin ejecutar el protocolo MBGP, y realizar el inter-acceso de los VRFs en los dos enrutadores de PE sin la relación de emparejamiento de Objetivos de Ruta.

10

La presente invención revela un procedimiento para la implementación de Operación en Red Privada Virtual (VPN), que incluye:

15

configurar una etiqueta estática para una instancia de Envío de Enrutamiento de VPN (VRF), correspondiente a un CE de Borde de Usuario conectado con un primer PE de Borde de Proveedor;

20

configurar, en un segundo PE, una o más rutas estáticas para alcanzar una entidad de red conectada con el CE, la dirección de destino de cualquiera de las una o más rutas estáticas es la dirección de la entidad de red conectada con el CE, la dirección de salto siguiente de cualquiera de las una o más rutas estáticas es la dirección del primer PE, y la etiqueta estática configurada para el VRF se toma como la etiqueta de cualquiera de las una o más rutas estáticas;

25

tras la recepción de un mensaje que ha de ser enviado, encontrar una ruta estática para el segundo PE que contenga la dirección de destino en el mensaje, insertar la etiqueta de la ruta estática encontrada en el mensaje como etiqueta de capa interna, y seleccionar un túnel para el envío del mensaje hasta el primer PE de acuerdo con la dirección de salto siguiente de la ruta estática; y

30

al recibir el mensaje, buscar el primer PE para el VRF, de acuerdo con la etiqueta de capa interna del mensaje, y enviar el mensaje a la entidad de red conectada con el CE de acuerdo con el VRF encontrado.

La solución anterior puede incluir además: transferir información de enrutamiento de la VPN entre los PEs por medio del protocolo de acceso marginal de extensión multi-protocolo.

35

En la solución anterior, la información de enrutamiento de la VPN puede ser la información contenida en las una o más rutas estáticas configuradas en el segundo PE.

40

En la solución anterior, cuando se encuentra una ruta estática que contiene la dirección de destino en el mensaje, puede incluir además: si se encuentra la ruta estática, continuar el procedimiento; en caso contrario, terminar el procedimiento.

En la solución anterior, el túnel puede ser un LSP, un túnel de Encapsulado de Enrutamiento Genérico, o un Túnel Seguro de Protocolo de Internet.

45

Un sistema para la implementación de Operación en Red Privada Virtual VPN, incluye:

un CE de Borde de Usuario, conectado a un primer PE de Borde de Proveedor;

50

una entidad de red, conectada con el CE;

el primer PE, configurado con una etiqueta para una instancia VRF de Envío de Enrutamiento de VPN correspondiente al CE; configurado para buscar el VRF de acuerdo con una etiqueta interna del mensaje, y enviar el mensaje a la entidad de red conectada con el CE de acuerdo con el VRF encontrado; y

55

un segundo PE, configurado con una o más rutas estáticas para alcanzar una entidad de red conectada con el CE, la dirección de destino en cualquiera de las una o más rutas estáticas es la dirección de la entidad de red conectada con el CE de acuerdo con el VRF encontrado; y

60

un segundo PE, configurado con una o más rutas estáticas para alcanzar una entidad de red conectada con el CE, la dirección de destino en cualquiera de las una o más rutas estáticas es la dirección de la entidad de red conectada con el CE, la dirección de salto siguiente de cualquiera de las una o más rutas estáticas es la dirección del primer PE, y una etiqueta configurada para el VRF se toma como la etiqueta de cualquiera de las una o más rutas estáticas; configurado para encontrar una ruta estática que contiene la dirección de destino en un mensaje y tras la recepción del mensaje, insertar la etiqueta, y seleccionar un túnel para enviar el mensaje hasta el primer PE de acuerdo con la dirección de salto siguiente de la ruta estática.

65

En la solución anterior, la dirección del primer PE puede ser la dirección pública del primer PE.

En la solución anterior, la dirección de la entidad de red puede ser la dirección del segmento de red de la entidad de red.

5 A partir de la descripción que antecede, queda claro que las diferencias entre las realizaciones de la presente invención y la técnica anterior, son como sigue: configurar una etiqueta para un VRF en un PE, y configurar una o más rutas estáticas en cualquier otro PE que necesite acceder al VRF, en el que, cada ruta estática configurada incluye una etiqueta del VRF de destino, y su dirección de salto siguiente es una dirección pública del PE donde se ubica el VRF de destino; cuando un mensaje se empareja con una o más rutas estáticas, insertar en el mensaje la etiqueta contenida en la ruta estática emparejada a modo de etiqueta interna, encontrar un túnel en base a la dirección de salto siguiente, y enviar el mensaje al PE en el que se ubica el VRF de destino; y envío por el PE del mensaje recibido hasta el VRF correspondiente a la etiqueta interna. Este procedimiento para la implementación de la VPN mediante configuración de etiquetas y de rutas estáticas, puede ser aplicado de manera independiente o con esquemas de implementación de VPN basados en MBGP.

20 Con el esquema de VPN simplificada de BGP/MPLS conforme a las realizaciones de la presente invención, es posible elegir no ejecutar el protocolo MBGP de acuerdo con el tamaño de red y con la capacidad de mantenimiento para la VPN de MPLS, simplificando con ello el protocolo de señalización de la red VPN de MPLS, y reduciendo la necesidad de personal de mantenimiento. Especialmente para una red de tamaño más pequeño, la utilización de las realizaciones de la presente invención resulta relativamente conveniente para implementar la VPN.

25 Además, en base a la relación de VPN desplegada de la red, los VRFs de dos enrutadores de PE que no tienen ninguna relación de emparejamiento de VPN, es decir, sus Objetivos de Ruta de importación/exportación no se emparejan entre sí, pueden soportar un inter-acceso, y la relación de acceso de los VRFs de los dos enrutadores de PE pueden ser ajustados de manera conveniente y dinámica según se requiera prácticamente, lo que mejora en gran medida la flexibilidad de configuración de la red.

Breve descripción de los dibujos

30 La Figura 1 es un diagrama esquemático de la operación en red implementada por la VPN simplificada de BGP/MPLS de acuerdo con una realización de la presente invención.

La Figura 2 es un diagrama de flujo esquemático de acuerdo con una realización de la presente invención.

Descripción detallada de las realizaciones preferidas

40 El procedimiento de las realizaciones de la presente invención incluye: configurar una etiqueta estática para un VRF en un PE; cuando se ha de ejecutar el protocolo MBGP entre dos PEs, la etiqueta estática es portada por una ruta de la VPN del VRF cuando la ruta de la VPN está siendo divulgada por el exterior; y, si se está enviando un mensaje, la etiqueta puede identificar globalmente a qué VPN será transmitido el mensaje.

45 En cualquier PE que tenga derecho a acceder a una entidad de red correspondiente al VRF, excepto el PE configurado con la etiqueta estática, se configura una ruta estática que llega a entidad de la red. El destino de la ruta estática puede ser una ruta por defecto o cualquier segmento de red de un dispositivo de CE conectado con el PE configurado con la etiqueta estática, y la dirección de destino de la ruta estática es la dirección de la entidad de red a la que debería llegar. La principal diferencia entre la ruta estática mencionada anteriormente y una ruta estática común de la técnica anterior consiste en que el siguiente salto de ruta estática mencionado anteriormente, no es la dirección de un dispositivo P del PE, sino la dirección pública de un PE del lado de destino a la que el usuario desea acceder; además, la ruta estática mencionada anteriormente puede estar configurada con una etiqueta, en la que la etiqueta es la etiqueta estática del VRF en el PE del lado de destino al que el usuario desea acceder. Después de que se ha generado la ruta estática, el PE en el que se ha configurado la ruta estática puede enviar un mensaje a un túnel que el PE del siguiente salto necesita alcanzar a través de la dirección configurada de salto siguiente, y a través del túnel, el mensaje puede alcanzar además el PE de salto siguiente, es decir, el PE del lado de destino. Entre estos, el túnel puede ser un LSP, un Encapsulamiento de Enrutamiento Genérico (GRE por sus siglas en inglés), una IPsec (Seguridad de IP), o cualquier otro túnel.

55 Esta realización para la implementación de la VPN mediante etiquetas de configuración y rutas estáticas, puede ser realizada de forma independiente o combinada con un procedimiento basado en MBGP para la implementación de VPN. Es decir, durante el envío del mensaje, la VPN puede ser implementada en base a la relación de emparejamiento de los Objetivos de Ruta de Exportación y los Objetivos de Ruta de Importación, utilizando ya sea las rutas estáticas configuradas o ya sea las rutas de VPN suministradas por medio del MBGP. Una realización preferida de la presente invención consiste en adoptar el MBGP para establecer la mayoría de las VPNs, y utilizar el procedimiento de rutas estáticas para configurar la minoría de las VPNs, con requisitos especiales, tal como una VPN temporal.

65 Con referencia al diagrama esquemático de operación en red implementado por la VPN de BGP/MPLS simplificada de acuerdo con una realización de la presente invención mostrada en la Figura 1, supóngase que la VPN

establecida debe realizar el inter-acceso entre la entidad de red conectada con un dispositivo CE-1 y las conectadas con un dispositivo CE-3, así como el inter-acceso entre la entidad de red que conecta con el dispositivo CE-1 y las que conectan con un dispositivo CE-2. La entidad de red mencionada es, en general, un dispositivo de terminal de usuario.

5 La dirección pública de PE-1 es addr1, el CE-1 conectado con PE-1 corresponde a VRF1, y la dirección del segmento de red de la entidad de red conectada con CE-1 es dest1; la dirección pública de PE-2 es addr2, el CE-2 conectado con PE-2 corresponde a VRF2, y la dirección del segmento de red de la entidad de red conectada con CE-2 es dest2; y la dirección pública de PE-3 es addr3, el CE-3 conectado con PE-3 corresponde a VRF3, y la
10 dirección del segmento de red de la entidad de red conectada con CE-3 es dest3.

Según se muestra en la Figura 2, el proceso incluye las siguientes etapas:

15 Etapa 201: configurar una o más rutas estáticas en cada PE.

En PE-3, configurar una etiqueta estática, L3, para VRF3, que corresponda al dispositivo CE-3; y en PE-2, configurar una etiqueta estática, L2, para VRF2, que corresponda al dispositivo CE-2.

20 Configurar dos rutas estáticas en PE-1: la dirección de destino de una ruta estática es la dirección del segmento de red de la entidad de red conectada con el dispositivo CE-2, dest2, la dirección de salto siguiente es la dirección pública de PE-2, addr2, y la etiqueta es la etiqueta estática de VRF2, L2; y la dirección de destino de la otra ruta estática es la dirección del segmento de red de la entidad de red conectada con el dispositivo CE-3, dest3, la dirección de salto siguiente es la dirección pública de PE-3, addr3, y la etiqueta es L3.

25 La configuración anterior permitirá que la entidad de red conectada con CE-1 acceda a las entidades de red conectadas con CE-2 y CE-3.

De forma similar, también es posible configurar en PE-2 y en PE-3, respectivamente, una ruta estática que alcance dest1, la dirección del segmento de red de la entidad de red conectada con CE-1 que conecta con PE-1, con el fin
30 de implementar el acceso de la entidad de red en CE-2 y CE-3 respecto a la entidad de red en CE-1, de lo que no se van a describir más detalles en lo que sigue.

Es evidente que, tal configuración de ruta estática no necesita ejecutar el protocolo MBGP entre PE-1, PE-2 y PE-3.

35 Después de esto, se puede implementar el envío del mensaje.

De acuerdo con el protocolo convencional, PE-1 puede estar equipado con túneles que alcancen addr2 y addr3, y de forma similar, ambos PE-2 y PE-3 pueden estar equipados con túneles que alcancen addr1.

40 Etapa 202: CE-1 envía a PE-1 el mensaje desde la entidad de red con la que conecta CE-1.

Después de recibir el mensaje, de acuerdo con la dirección del segmento de red de destino portada en el mensaje, supóngase que es dest2, PE-1 busca las rutas estáticas que contienen la dirección de dest2 en posición local; si no se encuentra ninguna ruta estática, se puede determinar entonces que la entidad de red de destino está fuera del
45 alcance de la VPN, y terminar el procedimiento; si se encuentra una ruta estática, insertar la etiqueta L2, configurada para la ruta estática, como etiqueta interna en el mensaje, y de acuerdo con la dirección de salto siguiente de addr2 contenida en la ruta estática, buscar un túnel adecuado para enviar el mensaje a un PE-2 que corresponda con addr2.

50 Etapa 203: Después de recibir el mensaje, PE-2 extrae la etiqueta interna de L2 contenida en el mensaje.

Puesto que la etiqueta interna de L2 está también configurada para VRF2 en PE-2, es posible encontrar VRF2, cuya etiqueta estática es también L2, en base a la etiqueta de L2, para encontrar la tabla de envío correspondiente a VRF2 por medio de la técnica anterior para obtener la información de enrutamiento de addr2, y para enviar el
55 mensaje a CE-2 correctamente de acuerdo con la información de enrutamiento de addr2, y a continuación CE-2 envía el mensaje a la entidad de red de destino correspondiente a dest2.

El procedimiento de configuración de ruta estática de la Etapa 201, se describe con detalle en el ejemplo que sigue:

60 Supóngase que existen tres dispositivos: PE1, P y PE2; se configura una VPN en PE1, denominada vpn1, y se configura una etiqueta bajo la VPN denominada 20; de forma similar, hay también una VPN existente en PE2, denominada vpn2, y una etiqueta configurada bajo la VPN es 30. Con el fin de permitir el inter-acceso de estas dos VPNs, se pueden configurar rutas como sigue:

65 La ruta estática configurada en PE2 es el salto siguiente de la "ip ruta vpn vpn2 10.0.0.0/8" (la dirección en PE1): "PE1, etiqueta 20", y

la ruta estática configurada en PE1 es el salto siguiente de "ip ruta vpn vpn1 20.0.0.0/8" (la dirección en PE2): "PE2, etiqueta 30".

- 5 Lo que se ha descrito en lo que antecede son solamente realizaciones de la presente invención, pero que no limitan el alcance de protección de la presente invención.

REIVINDICACIONES

1. Un procedimiento para la implementación de Operación en Red Privada Virtual, abreviada en lo que sigue como VPN, que se caracteriza por comprender:
- 5
- configurar una etiqueta estática para una instancia de Envío de Enrutamiento de VPN, abreviada en lo que sigue como VRF (VRF2, VRF3), correspondiente a un Borde de Usuario, abreviado en lo que sigue como CE (CE-2, CE-3), conectado con un primer Borde de Proveedor, abreviado en lo que sigue como PE (PE-2, PE-3) (201);
 - 10 - configurar en un segundo PE (PE-1), una o más rutas estáticas para alcanzar una entidad de red conectada con el CE (CE-2, CE-3), siendo la dirección de destino de cualquiera de las una o más rutas estáticas la dirección (dest2, dest3) de la entidad de red conectada con el CE (CE-2, CE-3), siendo la dirección de salto siguiente de cualquiera de las una o más rutas estáticas la dirección (addr2, addr3) del primer PE (PE-2, PE-3), y siendo la etiqueta estática configurada para el VRF (VRF2, VRF3) tomada como la etiqueta para cualquiera de las una o más rutas estáticas (201); donde el segundo PE es un PE que tiene el derecho a acceder a la entidad de red conectada con el CE;
 - 15 - tras la recepción de un mensaje que ha de ser enviado, encontrar por parte del segundo PE (PE-1) una ruta estática que contenga la dirección de destino en el mensaje, insertar la etiqueta de la ruta estática encontrada en el mensaje como etiqueta interna, y seleccionar un túnel para enviar el mensaje hasta el primer PE (PE-2, PE-3) de acuerdo con la dirección de salto siguiente de la ruta estática (202); y
 - 20 - con la recepción del mensaje, buscar mediante el primer PE (PE-2, PE-3) el VRF (VRF-2, VRF-3) de acuerdo con la etiqueta interna del mensaje, y enviar el mensaje hasta la entidad de red conectada con el CE (CE2, CE3) de acuerdo con el VRF (VRF2, VRF3) encontrado (203).
- 25 2. El procedimiento de acuerdo con la reivindicación 1, que se caracteriza por que comprende además: transferir información de enrutamiento de VPN entre los PEs (PE-1, PE-2, PE-3) por medio de un protocolo de acceso marginal de extensión de multi-protocolo.
- 30 3. El procedimiento de acuerdo con la reivindicación 2, que se caracteriza por que la información de enrutamiento de VPN es la información contenida en una o más rutas estáticas configuradas en el segundo PE (PE-1).
4. El procedimiento de acuerdo con la reivindicación 1, que se caracteriza por que, cuando se encuentra una ruta estática que contiene la dirección de destino (dest2, dest3) en el mensaje, dicho procedimiento comprende además: si se encuentra la ruta estática, continuar el procedimiento; en otro caso, terminar el procedimiento.
- 35 5. El procedimiento de acuerdo con la reivindicación 1, que se caracteriza por que el túnel es un LSP, un túnel de Encapsulamiento de Enrutamiento Genérico, o un Túnel Seguro de Protocolo de Internet.
- 40 6. El procedimiento de acuerdo con la reivindicación 1, que se caracteriza por que la dirección del primer PE (PE-2, PE-3) es una dirección pública del primer PE (PE-2, PE-3).
7. El procedimiento de acuerdo con la reivindicación 1, que se caracteriza por que la dirección (addr2, addr3) de la entidad de red es la dirección del segmento de red de la entidad de red.
- 45 8. Un sistema para la implementación de Operación en Red Privada Virtual, abreviada en lo que sigue como VPN, que se caracteriza por comprender:
- un Borde de Usuario, abreviado en lo que sigue como CE (CE-2, CE-3), conectado con un Borde de Proveedor, abreviado en lo que sigue como PE (PE-2, PE-3);
 - 50 - una entidad de red, conectada con el CE (CE-2, CE-3);
 - correspondiendo el primer PE (PE-2, PE-3), configurado con una etiqueta para una instancia de Envío de Enrutamiento de VPN, abreviada en lo que sigue como VRF (VRF2, VRF3), con el CE (CE-2, CE-3); configurado para buscar el VRF (VRF-2, VRF-3) de acuerdo con una etiqueta interna del mensaje al recibir el mensaje, y para enviar el mensaje a la entidad de red conectada con el CE (CE2, CE3) de acuerdo con el VRF (VRF2, VRF3) encontrado (203); y
 - 55 - un segundo PE (PE-1), configurado con una o más rutas estáticas para alcanzar una entidad de red conectada con el CE (CE-2, CE-3), siendo la dirección de destino de cualquiera de las una o más rutas estáticas la dirección (dest2, dest3) de la entidad de red conectada con el CE (CE-2, CE-3), siendo la dirección de salto siguiente de cualquiera de las una o más rutas estáticas la dirección (addr2, addr3) del primer PE (PE-2, PE-3), y siendo la etiqueta configurada para el VRF (VRF2, VRF3) tomada como la etiqueta de cualquiera de las una o más rutas estáticas; donde el segundo PE es un PE que tiene el derecho a acceder a la entidad de red conectada con el CE; estando configurado para encontrar una ruta estática que contenga la dirección de destino en un mensaje tras la recepción del mensaje, insertar la etiqueta en la ruta estática encontrada en el mensaje como etiqueta interna, y seleccionar un túnel para enviar el mensaje al primer PE (PE-2, PE-3) de acuerdo con la dirección de salto siguiente de la ruta estática.
 - 60
 - 65

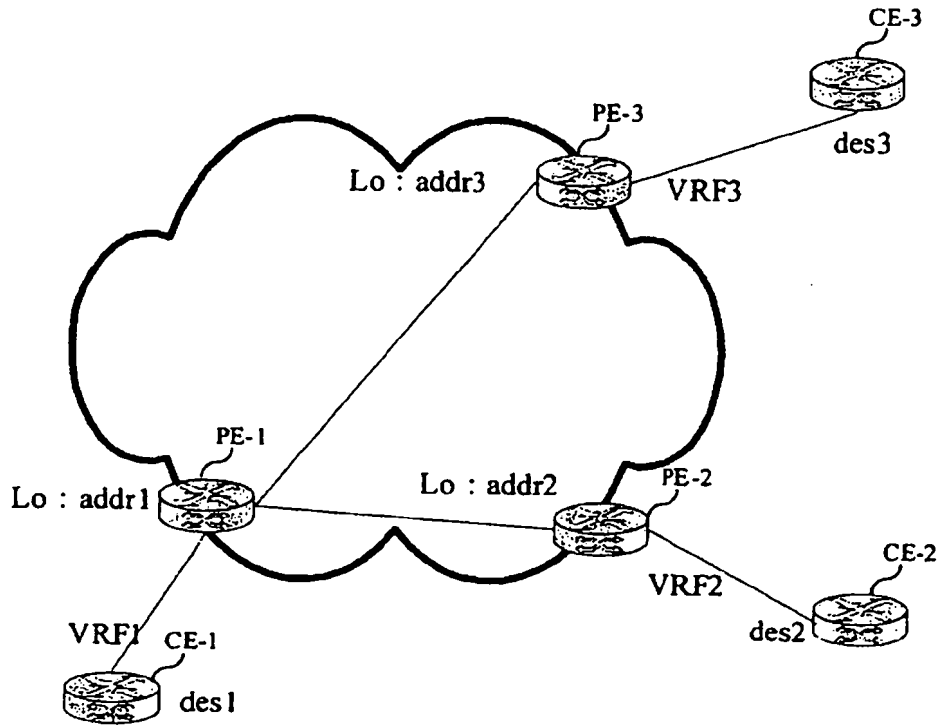


Fig.1

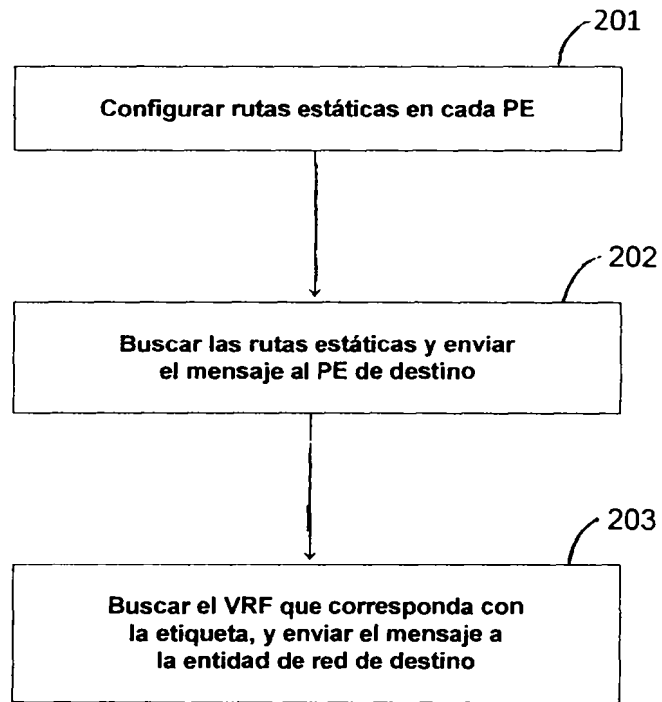


Fig. 2