(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 485 307**

(51) Int. CI.:

H04L 12/773 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.10.2006 E 11190180 (7)**

(97) Fecha y número de publicación de la concesión europea: **04.06.2014 EP 2424178**

(54) Título: **Formación de puentes de estado de enlaces de proveedores**

(30) Prioridad:

05.10.2005 US 723479 P
14.11.2005 US 735884 P
21.04.2006 US 745330 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.08.2014

(73) Titular/es:

NORTEL NETWORKS LIMITED (100.0%)
2351 Boulevard Alfred-Nobel
St Laurent, Québec H4S 2A9, CA

(72) Inventor/es:

ALLAN, DAVID y
BRAGG, NIGEL

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

DESCRIPCIÓN

Formación de puentes de estado de enlaces de proveedores

Campo técnico

La presente invención se refiere al campo de los protocolos de encaminamiento de tráfico de Ethernet y, en particular, a la configuración de la conectividad en una red Ethernet mallada.

Antecedentes de la invención

En las arquitecturas de red Ethernet los dispositivos conectados a la red compiten en la capacidad de uso de la trayectoria de las telecomunicaciones compartidas en cualquier momento determinado. Allí donde se utilizan múltiples puentes o nodos para interconectar los segmentos de red, existirán múltiples trayectorias potenciales hacia el mismo destino dentro de una arquitectura de red mallada. La ventaja de esta arquitectura es que proporciona redundancia de trayectorias entre puentes y permite que se añada una capacidad a la red bajo la forma de enlaces adicionales. Sin embargo, el paradigma de Ethernet, de inundación y aprendizaje, significa que habitualmente la anchura de la conectividad que existe en una red mallada no puede ser explotada en cualquier instante determinado en el tiempo debido a la exigencia de asegurar que ninguna trayectoria replicante pueda establecer un bucle. Debe destacarse que los puentes pueden estar interconectados mediante simples enlaces o mediante segmentos de LAN (Red de Área Local) compartidos o mediante segmentos de LAN Virtual compartidos. Desde el punto de vista del presente documento, segmento, segmento virtual y enlace son efectivamente intercambiables.

Cada nodo de puente en una red Ethernet aprende cuáles son los dispositivos o la estación a los que se puede llegar a través de qué segmento de Ethernet local mediante la observación de por cuál segmento llegan paquetes desde un dispositivo determinado. Al efectuar un envío hacia un dispositivo desconocido (uno para el cual no existe ninguna información de remisión en la base de información de remisión (FIB)), un puente replicará el mensaje sobre todos los segmentos adjuntos (esto se conoce como inundación). Esto tiene dos efectos: los puentes que observan el paquete inundado aprenden la información de accesibilidad hacia el dispositivo de origen, y hay una expectativa de que en algún momento en el futuro se observará una contestación solicitada por el mensaje, o por un mensaje posterior no solicitado, desde el dispositivo de destino concebido, a partir de la cual pueda apreciarse por medio de qué segmento el dispositivo contestó al mensaje. De manera gradual, el puente construye una imagen para sí mismo de cuál es el siguiente segmento apropiado para alcanzar dispositivos específicos en la red. Cuando se envían mensajes posteriores, el puente puede utilizar su FIB para determinar a qué segmento localmente adjunto remitirlos. El enfoque de permitir que los puentes aprendan la red por medio de la experiencia es conocido como formación transparente de puentes. Una ventaja clave de la técnica es que la formación de puentes no requiere su configuración por un administrador.

En una malla, cuando un paquete es remitido entre dispositivos homólogos es posible que el paquete pase a través de múltiples puentes por medio de una pluralidad de trayectorias. Sin embargo, si el paquete tuviera que ser enviado por múltiples rutas de manera simultánea, la congestión de la red aumentaría y podrían producirse posibles condiciones de formación de bucles. Este escenario surge en una malla para el tráfico de multidifusión y / o inundado, puesto que el número de copias de un paquete determinado crecería de manera exponencial si no se controlara. Un algoritmo del Protocolo de Árbol de Recubrimiento (STP) es utilizado para eliminar la duplicación de paquetes mediante la elección de manera iterativa de un árbol de recubrimiento que conecte de forma lógica el conjunto de nodos participantes. El algoritmo está específicamente construido para evitar bucles de puentes (múltiples trayectorias que enlazan un segmento con otro, provocando una situación de formación de bucles infinitos). El algoritmo habitualmente calcula la trayectoria más corta desde todos los segmentos hasta un puente raíz elegido. Si la mejor trayectoria falla, el algoritmo vuelve a calcular la red y encuentra la siguiente mejor ruta. Si la raíz falla, se elige una nueva raíz y el algoritmo se re-ejecuta. Al mismo tiempo, toda la información de MAC aprendida con respecto a la accesibilidad del dispositivo es descartada y las FIB son repobladas de manera gradual mediante inundación y aprendizaje una vez que se establece el nuevo árbol de recubrimiento.

El STP proporciona la conectividad impidiendo al tiempo la formación de bucles no deseables en una red que se producirían si existieran múltiples trayectorias activas entre nodos o dispositivos. Si se permitiera la formación de bucles, los paquetes que entraran en el bucle circularían hasta que un nodo adoptara la medida de suprimir el paquete o que el bucle se rompiera. Si los puentes en el bucle se inundan, o el paquete es un paquete de multidifusión, se generarán copias adicionales del paquete en cada recorrido del bucle, un resultado sumamente indeseable. Para establecer una conectividad exenta de bucles, el STP crea un árbol que abarca todos los puentes existentes en una red extendida, forzando a las trayectorias redundantes a un estado de espera, o de bloqueo. El STP permite solo una trayectoria activa cada vez entre dos puntos cualesquiera en la red, lo cual impide la formación de bucles pero la capacidad adicional asociada con la conectividad de la malla física no se utiliza. El STP fue diseñado para nodos sin memoria de estados, para simplificar los puentes. Sin embargo, este enfoque simplista de la conectividad exenta de bucles puede traducirse en un exceso de capacidad no utilizada de la red debido a la necesidad de podar la topología física en un único árbol de recubrimiento exento de bucles.

La elección de la raíz durante la convergencia del STP está determinada por el conjunto de puentes que determinan qué puente presenta el Identificador más bajo y, a continuación, mediante la determinación por parte de cada puente del siguiente salto sobre la trayectoria de coste más bajo hasta el puente con el Identificador más bajo, o "raíz". Los puentes inicialmente anuncian su propio Identificador y un coste nulo, en los intercambios del protocolo del árbol de recubrimiento. Cuando reciben un anuncio con un Identificador más bajo, dejan de anunciar su propio Identificador y anuncian el Identificador más bajo y el coste. De manera similar, cuando aprecian un segmento con un coste más bajo que el del Identificador actual más bajo, modifican, en la medida correspondiente, tanto sus anuncios re-irradiados como su estado interno. En último término, la red convergerá a una vista común del Identificador más bajo, y cada puente que conoce el segmento siguiente sobre la trayectoria de coste más bajo hacia la raíz. Si los costes se modifican, o si un segmento de red del árbol de recubrimiento resulta inalcanzable, el algoritmo del STP calcula de manera iterativa una nueva topología del árbol de recubrimiento para ofrecer una conectividad que utilice el conjunto revisado de segmentos. Mientras que los puentes de la red no converjan, los puertos quedan bloqueados deteniendo el tráfico de la red con el fin de impedir la formación de bucles y la replicación.

La Fig. 1 muestra un ejemplo de la forma en que un algoritmo del protocolo de árbol de recubrimiento, dentro de una red mallada, afecta a la remisión de un paquete a través de la red. A partir de un dispositivo de origen A, el algoritmo del STP ha elaborado un mapa de una trayectoria a través de la red, determinando los enlaces existentes entre cada nodo que consiguen el coste más bajo (mostrada como ruta de multidifusión). Esta ruta determina las trayectorias disponibles para todo el tráfico que atraviesa la red. El dispositivo A, asociado al puente 110, envía un paquete al dispositivo B, que es nuevo en la red. Los puentes de la red no incorporan tablas de remisión rellenadas para este dispositivo. La red es inundada por el paquete, hasta cada nodo de puente, por la trayectoria definida por el árbol de recubrimiento. A continuación, los paquetes del árbol de recubrimiento son remitidos desde el puente 110 a través del puente 112. Los enlaces desde el puente 110 hacia los puentes vecinos 116 y 120 no son utilizados porque han sido inhabilitados o bloqueados y no forman parte del árbol de recubrimiento. Desde el puente 112 el paquete es remitido a los demás nodos de la red, los puentes 120, 122, 124 y 114. El puente 114, a su vez, remite el paquete a los puentes 116 y 118. El dispositivo B recibe una copia inundada del paquete a través del puente 122. Todos los puentes intermedios advertirán el segmento de llegada para el origen "A" y actualizarán en consecuencia sus FIB. Una respuesta enviada por el dispositivo B recorrerá entonces la red directamente hacia el dispositivo A sin ser inundada, en cuanto la ruta de retorno es conocida por los puentes intermedios de la red. En lo esencial, una inundación de paquetes entra en la red con una respuesta de retorno desde el dispositivo B hasta el dispositivo A y, de modo similar a la manera en que los puentes intermedios aprendían la remisión óptima hacia "A" observando el mensaje inicial, aprenden la remisión óptima hacia "B" observando la respuesta.

La utilización del STP en una red Ethernet limita la eficacia de la utilización de los enlaces o de los segmentos de la LAN en la red. Los segmentos y los enlaces no seleccionados por el algoritmo STP están inhabilitados y no forman esencialmente parte de la topología de red activa hasta que se produzca algún cambio en la topología física de la red, de forma que el enlace constituya parte del árbol de recubrimiento resultante. Esto atora la capacidad de estos enlaces. En un entorno de LAN pequeña, ello puede no constituir un problema, sin embargo, en una WAN o en una red de proveedores una capacidad no utilizada afecta por un lado al cambio de escala y también representa una inversión infrautilizada. Además, cuando se produce un fallo, el rendimiento de la red entera resulta afectado durante el tiempo requerido para re-converger el STP y estabilizar todos los puentes en la red. La trayectoria adoptada por un paquete determinado que utiliza el árbol de recubrimiento no es habitualmente la trayectoria más corta entre el origen y el destino, en cuanto la raíz del árbol de recubrimiento actual no está necesariamente sobre la trayectoria física más corta. Por ejemplo, si el dispositivo C estuviera conectado al puente vecino 116, los paquetes procedentes del dispositivo A seguirían teniendo que atravesar los puentes 112 y 114 en base al actual árbol de recubrimiento, que no proporciona necesariamente la trayectoria más corta hacia el puente 116. Por último, en una red de proveedores puede haber muchas pequeñas comunidades de interés, bajo la forma de redes virtuales privadas, y contener la inundación de información dentro de esas comunidades de interés requiere habitualmente un árbol de recubrimiento específico por cada comunidad.

Se han propuesto diversos procedimientos para mejorar el rendimiento del STP y mitigar la formación de bucles en una red Ethernet mallada. Algunas propuestas actuales requieren una etiqueta tipo MPLS o el agregado del campo de tiempo de vida (TTL) al paquete Ethernet para limitar el impacto de la formación de bucles. Sin embargo, se requieren modificaciones fundamentales de los planos de los datos para implementar estas soluciones, lo que limita su utilidad. Además, limitar únicamente el número de veces que un paquete puede replicarse es una solución demostrablemente incompleta al problema de la formación de bucles.

Con el fin de ajustar Ethernet a escala desde el espacio de una LAN al de una WAN, o al espacio de una red de proveedores, se requiere un mecanismo mejorado para la creación de redes Ethernet eficaces carentes de bucles. Este es uno que hace una utilización superior de la conectividad mallada, restringe el impacto de los fallos o los cambios de topología (por ejemplo, no interrumpe, o reduce al mínimo las interrupciones de conectividad), y suprime los bucles o mitiga el efecto de la formación de bucles. Por consiguiente, existe la necesidad de una red Ethernet con una utilización de red mejorada que al tiempo evite los escollos de los bucles transitorios o persistentes.

En una presentación titulada "Formación de puentes con la trayectoria más corta", realizada para la norma IEEE 802.1 en Garden Grove, California, el 22 de septiembre de 2005, Norman Finn describe modificaciones del protocolo

802.1s del Árbol de Recubrimiento, para habilitar puentes en una red Ethernet, para generar un conjunto de SPI (Interfaces de Proveedores de Servicios) simétricas, una para cada puente.

En un Borrador de Internet titulado “Estado de enlaces de multidifusión para Rpuentes” (Borrador de trabajo de normas IETF), Fuerza de Tareas de Ingeniería de Internet, IETF, CH, 17 de octubre de 2005), S. Hare revela varios enfoques para el cálculo de multidifusión.

Sumario de la invención

La presente invención proporciona un sistema y un procedimiento para crear redes Ethernet exentas de bucles mediante la utilización de una Formación de Puentes de Estado de Enlaces de Proveedores (PLSB). La PLSB expande la configuración estática de las tablas de remisión del MAC (Control de Acceso al Medio) de Ethernet mediante un plano de control, y utiliza la manipulación directa de la remisión de Ethernet mediante un sistema de encaminamiento del estado de los enlaces. Al menos dos direcciones de MAC están asociadas con cada puente, una para la remisión individual y otra para la remisión de multidifusión desde el puente. El MAC de unidifusión es utilizado por puentes homólogos, al enviar paquetes hacia el puente, como la dirección de destino para un paquete, e identifica el puente como el origen del tráfico de unidifusión o de multidifusión desde el puente a sus homólogos. La dirección de multidifusión es utilizada por el puente al enviar tráfico de manera simultánea a múltiples puentes homólogos para identificar el árbol de multidifusión específico configurado por el sistema de encaminamiento.

Los puentes intercambian la información de estado mediante un protocolo de estado de enlaces y mantienen una base de datos de estados utilizada para determinar las trayectorias más cortas entre puentes homólogos mediante un algoritmo de trayectorias más cortas. En condiciones de Trayectorias Múltiples de Igual Coste entre dos puentes cualesquiera, se efectúa una elección coherente de trayectoria por parte de todos los puentes, de tal manera que las trayectorias de unidifusión de “ida” y “vuelta” y los segmentos relevantes de los dos árboles de multidifusión sean encaminados de forma simultánea. Las tablas de remisión o la base de información de remisión (FIB) luego son rellenadas con las direcciones adecuadas de unidifusión y de multidifusión. Luego se crean árboles únicos de distribución de unidifusión y de multidifusión en cada puente, que proporcionan una utilización más eficaz de los enlaces.

La supresión de los bucles está proporcionada por un control de remisión de trayectoria inversa (RPFC), llevado a cabo sobre los paquetes recibidos en cada puente. El RPFC determina si el paquete ha llegado al puerto o interfaz correctos, según lo identificado en la FIB, desechándose los paquetes que no llegan al puerto correcto. Esto es posible debido a la propiedad de co-encaminamiento de todas las trayectorias entre dos puntos cualesquiera (como *supra*). Durante el periodo de inestabilidad de la red, como por ejemplo en el curso de un fallo de un puente o de un enlace, en los que puede producirse potencialmente la formación de bucles y la topología de la red no ha convergido, el RPFC puede ser inhabilitado para paquetes de unidifusión, para reducir al mínimo el impacto sobre el tráfico. Cuando la topología re-converge en cada puente, el RPFC puede ser rehabilitado. Para el tráfico de multidifusión, el RPFC nunca es inhabilitado, para reducir la posibilidad de una replicación ilimitada.

Las redes privadas virtuales (VPN) pueden ser correlacionadas encima de la red de PLSB, haciendo posible que un árbol de multidifusión único sea correlacionado para cada VPN, para cada puente de frontera, para que el tráfico sea solo dirigido hacia la comunidad única específica de interés. El tráfico de multidifusión de las VPN es solo suministrado a aquellos puentes que participan en la VPN mediante la instalación de las direcciones de multidifusión grupales de la VPN para las trayectorias que sean comunes.

Las redes pueden ser ajustadas a escala mediante la utilización de otras técnicas, tales como, por ejemplo, la técnica de Transporte Troncal de Proveedores (PBT) (tal y como se describe en la solicitud US20050220096 transferida al modo común) y los Puentes Troncales de Proveedores (PBB) del Estándar 802.1ah en combinación con la PLSB. Un PBB puede ser utilizado para ligar entre sí áreas de PLSB como, por ejemplo, los dominios de WAN de la PLSB y los dominios metropolitanos de la PLSB, o para extender la conectividad utilizando el PBT.

Por tanto, de acuerdo a un aspecto de la presente invención, se proporciona un procedimiento de operación de un puente de Ethernet en una red, de acuerdo a la reivindicación 1.

Un aspecto adicional de la presente invención proporciona una formación de puentes de Ethernet de acuerdo a la reivindicación 11.

Otros aspectos y características distintivas de la presente invención se pondrán de manifiesto para los medianamente expertos en la materia, tras el análisis de la descripción siguiente de realizaciones específicas de la invención, en combinación con las figuras que se acompañan.

Breve descripción de los dibujos

Las características y ventajas adicionales de la presente invención se pondrán de manifiesto a partir de la siguiente descripción detallada, considerada en combinación con los dibujos adjuntos, en los cuales:

La FIG. 1 es una representación esquemática de una red mallada que utiliza el protocolo del árbol de recubrimiento (STP);

la FIG. 2a es una representación esquemática de una red mallada que implementa la PLSB, mostrada desde un dispositivo A;

la FIG. 2b es una representación esquemática de una red mallada que implementa la PLSB, mostrada desde un dispositivo B;

la FIG. 3 es un diagrama esquemático de un escenario de formación de bucle de paquetes;

la FIG. 4 es una representación esquemática de un bloqueo de puertos durante la convergencia;

la FIG. 5 es una representación esquemática de un puente de PLSB;

la FIG. 6 es un diagrama de flujo de un procedimiento para la configuración de un puente de PLSB;

la FIG. 7 es un diagrama de flujo de un procedimiento para operar un puente de PLSB;

la FIG. 8 es una representación esquemática de una superposición de una VPN que utiliza la PLSB; y

la FIG. 9 es un esquema de red de una PLSB en combinación con redes híbridas de PBB y PBT.

Se hace notar que a lo largo de los dibujos adjuntos, las mismas características se identifican mediante los mismos números de referencia.

Descripción detallada de la forma de realización preferente

A continuación se describen formas de realización de la presente invención, solo a modo de ejemplo, con referencia a las Figs. 2 a 9. La presente invención proporciona un sistema, un procedimiento y un dispositivo para la conexión en redes Ethernet exentas de bucles.

La Formación de Puentes de Estado de Enlaces de Proveedores (PLSB) permite que las redes Ethernet sean ajustadas a escala, desde el espacio de una LAN al espacio de una WAN, o al espacio de redes de proveedores, mediante la provisión de un uso más eficaz de la capacidad de las redes, con remisión por la trayectoria más corta exenta de bucles. Más que utilizar una visión de red aprendida en cada nodo mediante la utilización del algoritmo del Protocolo de Árbol de Recubrimiento (SPT), combinado con la formación transparente de puentes, en una red basada en la PLSB los puentes que constituyen la red mallada tienen una visión sincronizada de la topología de la red. Esto se consigue por medio del mecanismo, bien comprendido, de un sistema de encaminamiento de estados de enlaces. Los puentes en la red tienen una visión sincronizada de la topología de la red, tienen conocimiento de la conectividad de la unidifusión y la multidifusión requeridas, pueden calcular una conectividad de la trayectoria más corta entre cualquier par de puentes en la red y pueden, de forma individual, rellenar las bases de información de remisión (FIB) de acuerdo con la visión calculada de la red. Cuando todos los nodos han calculado su papel dentro de la visión sincronizada y rellenado sus FIB, la red tendrá un árbol de unidifusión exento de bucles hacia cualquier puente determinado, desde el conjunto de puentes homólogos; y un árbol de multidifusión de punto a multipunto (p2mp) tan congruente como exento de bucles, desde cualquier puente determinado hacia el mismo conjunto de puentes homólogos. El resultado es que la trayectoria entre un par determinado de puentes no queda constreñida a transitar por el puente de raíz de un árbol de recubrimiento, y el resultado global puede utilizar mejor la amplitud de conectividad de una malla.

La PLSB proporciona el equivalente de la conectividad por puentes de Ethernet, pero lo consigue por medio de la configuración de la FIB y no mediante la inundación y el aprendizaje. En cuanto tal, puede ser utilizada por los estándares incipientes, como por ejemplo el estándar en borrador 802.1ah del IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) titulado Puentes Troncales de Proveedores (PBB) o el MAC-en-MAC con remisión configurada de los B-MAC (MAC Troncales) y modificaciones triviales de la función de adaptación de los PBB, para correlacionar el comportamiento de difusión del cliente con la multidifusión de la PLSB, de tal manera que las Ethernet clientes puedan utilizar la conectividad ofrecida por la red de PLSB sin modificación.

El funcionamiento de la PLSB puede ser combinada con otros planos de control o con la formación transparente de puentes, mediante la división de la red, mediante el empleo de LAN virtuales (WLAN). El Identificador de la VLAN puede ser utilizado para definir una instancia de la malla en el nivel del plano de control; en el caso de la PLSB, esto es controlado mediante un sistema distribuido de encaminamiento de estados de enlaces. Cuando se utiliza la división de las VLAN de la función de red, la PLSB es compatible codo con codo con otras tecnologías de redes Ethernet, como por ejemplo el Transporte Troncal de Proveedores (PBT), tal y como se divulga en la solicitud de patente estadounidense transferida al modo común Nº US20050220096, depositada el 4 de abril de 2004.

La PLSB utiliza métricas simétricas, de tal manera que la conectividad entre dos puentes cualesquiera siga la misma trayectoria en ambas direcciones, y utiliza métricas comunes para la conectividad de unidifusión y multidifusión, de tal manera que exista congruencia de remisión entre paquetes que sean de multidifusión y paquetes que sean de

unidifusión. Hay una serie de razones por las que esto es deseable cuando la PLSB sea utilizada para transportar clientes Ethernet:

La imposibilidad de un reordenamiento de paquetes dentro de un flujo allí donde los paquetes iniciales inundan la trayectoria de multidifusión y la información de remisión es aprendida durante el flujo para permitir la remisión por la trayectoria de unidifusión.

Una probabilidad mucho más elevada de que los fallos sean simétricos, para contrarrestar el problema conocido por los clientes que utilizan el árbol de recubrimiento, cuando los fallos asimétricos pueden provocar bucles.

La congruencia de la remisión de los paquetes clientes de la Gestión de Fallos de Conectividad (CFM) de multidifusión del estándar 802.1ag del IEEE y la correspondiente trayectoria de unidifusión a través de la red de la PLSB.

Congruencia similar de los paquetes de la CFM del nivel de la PLSB.

Las métricas simétricas se traducen en unos retardos de transporte de “ida” y “vuelta” iguales, lo que mejora en gran medida la efectividad y robustez de los esquemas de distribución de reloj de la capa 2 para diseminar la información de temporización dentro de la red.

Tal y como se analiza con mayor detalle en la descripción que sigue, con independencia de las exigencias de servicio de los clientes de Ethernet, las métricas simétricas facilitan además la supresión de bucles.

La PLSB utiliza una configuración de MAC para construir la conectividad exenta de bucles de la trayectoria más corta (con fines tanto de unidifusión como de multidifusión) entre un conjunto de puentes troncales de proveedores del estándar 802.1ah (ligeramente modificados) con el fin de proporcionar un servicio de LAN transparente a la capa C-MAC (MAC de Cliente) o a otras redes con capas que puedan utilizar un servicio de LAN transparente. Esto requiere el funcionamiento de un protocolo de encaminamiento de estados de enlaces dentro de la red troncal con puentes de los proveedores en lugar de un STP para la(s) LAN(s) asociada(s) y el remolque de la información de MAC sobre los anuncios del sistema de encaminamiento.

Cuando un puente de tránsito no necesita terminar la conectividad de unidifusión o de multidifusión, puede escoger no ofrecer la información de MAC, pero procesará los anuncios de direcciones de MAC procedentes de otros puentes. En el caso del estándar 802.1ah, los puentes de frontera conocidos como puentes troncales de proveedores (PBB) casi siempre ofrecerán la información de MAC, mientras que no lo harán los puentes puramente de tránsito.

Al menos dos direcciones de MAC están asociadas con cada puente, una para la remisión por unidifusión hacia el puente y al menos una para la remisión por multidifusión desde el puente. El MAC de unidifusión es utilizado por puentes homólogos al enviar paquetes hacia el puente, como la dirección de destino de un paquete, e identifica el puente como el origen del tráfico de unidifusión o de multidifusión desde el puente a sus homólogos. La dirección de multidifusión es utilizada por el puente al enviar tráfico hacia múltiples puentes homólogos de manera simultánea, para identificar el árbol de multidifusión específico configurado por el sistema de encaminamiento. El árbol de multidifusión puede ser configurado para suministrar un paquete a cada puente en el dominio de la PLSB, implementando así la función de difusión respecto del puente de origen específico. De manera optativa, puede identificar un subconjunto estricto del árbol de difusión para restringir la distribución únicamente a aquellos puentes que pertenecen a una comunidad de interés concreta, habitualmente, una VPN de la capa cliente.

Cuando la PLSB utiliza la información configurada y habilita todos los segmentos en una red mallada determinada, la inundación asociada con la formación transparente de puentes no se requiere y resulta indeseable. Por consiguiente, cualquier división de la LAN asignada al comportamiento de la PLSB debe además hacer que sea modificado el comportamiento de remisión para tratar los paquetes con direcciones de MAC de destino “desconocidas” de manera diferente a la de la formación transparente de puentes. Para la PLSB, los paquetes con direcciones de destino desconocidas son descartados de manera silenciosa.

La Fig. 2a es una representación esquemática de una red que utiliza la PLSB. A partir de la topología de red compartida, cada nodo calcula las trayectorias óptimas más cortas hacia otros puentes troncales de proveedores (PBB) o hacia nodos existentes en la red, utilizando un algoritmo de la trayectoria más corta. El resultado de la aplicación del algoritmo de la trayectoria más corta a través de la red, y el correspondiente rellenado de la FIB de los puentes, proporciona un árbol único a través de la malla desde cada puente hacia los puentes miembros de la red. Por ejemplo, el árbol de multidifusión calculado utilizando la trayectoria más corta desde el dispositivo A de la Fig. 2a es distinto al árbol de recubrimiento mostrado en la Fig. 1, en particular, por cuanto no existe ninguna elección de conmutación de raíz como en el STP. Tal y como se muestra en la Fig. 2a, la utilización de un algoritmo de la trayectoria más corta hace posible que un paquete de un dispositivo A recorra una ruta más directa hacia los puentes adyacentes 120 y 116, mientras que, utilizando el STP, las rutas de la trayectoria más corta pueden estar inhabilitadas tal y como se muestra en la Fig. 1.

Las operaciones de formación transparente de puentes, de inundación y aprendizaje, pueden ser correlacionadas con los PBB del estándar 802.1ah que implementan la PLSB. Por ejemplo, si el emplazamiento del dispositivo cliente B es desconocido para el puente 110 en la red de la PLSB, los paquetes dirigidos a B desde A serán encapsulados por MAC-en-MAC en un paquete de multidifusión por el puente 110, utilizando la dirección del grupo asignada a ese puente y con una dirección de origen del puente 110. El mensaje de multidifusión recorre la red por medio del árbol de la PLSB y una copia llega en última instancia al nodo 122 donde la encapsulación de MAC-en-MAC es eliminada y la copia es remitida al dispositivo B. La función de formación transparente de puentes de MAC-en-MAC en el puente 122 observa la dirección de B-MAC de origen en la encapsulación de MAC-en-MAC y deduce que para llegar hasta A se debe atravesar el puente 110. EL dispositivo B, al contestar al mensaje, envía entonces un mensaje dirigido a “A” al puente 122. El puente 122 advierte que el destino de MAC-en-MAC para A es el puente 110 y envuelve el mensaje en un paquete de unidifusión dirigido al puente 110. El paquete es enviado a través del puente 112 al puente 110, el cual, a continuación, elimina la encapsulación de MAC-en-MAC y remite el paquete por el puerto correcto para alcanzar el dispositivo A. De modo similar, el puente 110 observa que para llegar a B dentro de la red de la PLSB se debe atravesar el puente 122. Cualquier mensaje futuro enviado desde el dispositivo A al dispositivo B, y viceversa, puede ahora utilizar la remisión por unidifusión aprendida a través de la red de la PLSB.

Se requiere que los árboles de unidifusión y de multidifusión para cada puente sean congruentes, y este será un resultado directo del uso de métricas simétricas de enlaces. Cuando haya que afrontar trayectorias múltiples de igual coste, se requiere un medio distribuido para conseguir una clasificación común de las trayectorias, y es un problema bien sabido con muchas soluciones potenciales. Una solución ejemplar consiste en identificar los dos puentes donde las trayectorias de igual coste se dividen y vuelven a emerger, seleccionar el número de puente más alto, y escoger la trayectoria desde / hacia ese puente con el puente adyacente con el número más alto sobre los segmentos de la trayectoria de igual coste. Otros procedimientos resultarán evidentes para los expertos en la materia. La trayectoria más corta clasificada entre dos puentes cualesquiera es simétrica, por lo que se consigue la congruencia de la remisión, tanto de unidifusión como de multidifusión, entre dos puentes cualesquiera.

Para un nodo de puente determinado, a fin de determinar si está sobre la trayectoria más corta entre un par determinado de puentes, pueden ser utilizados diversos algoritmos de la trayectoria más corta, para calcular las trayectorias óptimas. Un algoritmo basado en gráficos como, por ejemplo, el algoritmo de Floyd [R. Floyd: Algoritmo 97 (trayectoria más corta), Comunicaciones de la ACM, 7:345, 1962] o el algoritmo de Dijkstra [E. W. Dijkstra: una nota sobre dos problemas con relación a los gráficos, Matemática Numérica, 1:269-271, 1959], puede ser implementado en el puente de la PLSB para calcular la trayectoria más corta entre nodos homólogos. Debería entenderse que también podría ser utilizado cualquier algoritmo adecuado de la trayectoria más corta. El algoritmo de Floyd calcula una matriz de distancias a partir de una matriz de costes, en donde, como el algoritmo de Dijkstra, computa las distancias más cortas desde un vértice a todos los demás vértices. Debería destacarse que el número de árboles no incide en la complejidad de cálculo del algoritmo básico de Floyd. El algoritmo genera una visión diferente de la trayectoria que el algoritmo del STP, en el sentido de que las trayectorias no tienen que extenderse a partir de una trayectoria de puente raíz. El STP genera una estructura de “árbol” más restringida utilizada para todas las trayectorias posibles, mientras que un procedimiento de trayectorias más cortas no está limitado por la selección de las rutas de la misma manera.

El algoritmo de la trayectoria más corta puede ser modificado para tener en cuenta la información de la ingeniería del tráfico. Por ejemplo, la trayectoria más corta puede incluir una medida del coste como, por ejemplo, la capacidad, la velocidad, el uso y la disponibilidad. La preservación del MAC de Origen entre puentes significa que la matriz de tráfico efectiva puede ser observada y utilizada como entrada para el sistema de encaminamiento. y reducir al mínimo la desviación estándar de la carga por enlace y facilitar el equilibro de las cargas. También debería destacarse que un efecto colateral de los algoritmos de la trayectoria más corta es que las “alternativas exentas de bucles”, el término industrial aceptado para un salto siguiente que se sabe más próximo al destino que el nodo actual, para el re-encaminamiento rápido sin conexión, pueden ser calculadas como parte del cálculo de la conectividad de la red.

Tal y como se muestra en la Fig. 2b, mirando desde el dispositivo B al puente 122, el árbol resultante del algoritmo de la trayectoria más corta es distinto al árbol desde el dispositivo A al puente 110 mostrado en la Fig. 2a. El tráfico desde el dispositivo B puede llegar a su destino por la trayectoria más corta desde el puente 122 de conexión y el árbol creado puede ser único si se observa desde el puente. Los árboles únicos desde cada puente hacen posible la utilización eficaz de los enlaces de la red. Sin embargo, la trayectoria entre dos dispositivos (A y B) o entre puentes asociados será simétrica y, por consiguiente, la misma en cada dirección.

Con referencia de nuevo a la Fig. 2a, si en cualquier punto hay un fallo de un enlace en la red, por ejemplo, si fallara el enlace entre el puente 116 y el puente 118, el único impacto afectaría al tráfico que transita por ese enlace. El fallo es anunciado por el sistema de encaminamiento, y se ejecuta el algoritmo de la trayectoria más corta. En este punto, el único cambio será para las trayectorias que transitaron por el enlace fallido, dado que las trayectorias más cortas no afectadas no se modificarán. El resultado neto es que la nueva FIB será en gran medida idéntica a la antigua, lo que significará que no hubo ningún impacto efectivo con respecto a la remisión de paquetes sobre trayectorias no afectadas. Con referencia a la Fig. 2b, el fallo en el enlace entre el puente 116 y el puente 118 no afectaría al árbol de encaminamiento, dado que no forma parte de la trayectoria más corta. Los expertos en la materia advertirán que no hay técnicas para reducir al mínimo el cálculo efectuado en escenarios de fallos que se sitúan al margen del

alcance de la invención. La descripción expuesta en lo que antecede simplemente ilustra el supuesto más sencillo al analizar las acciones de un sistema de encaminamiento, tales como la recepción de la notificación de un cambio de la topología, el cálculo de una nueva tabla de remisión y el rellenado de la FIB.

Las direcciones de MAC asociadas con un puente (de unidifusión o de multidifusión) son globales con respecto a la sub-red Ethernet controlada de estados de enlaces, y se utilizan para la remisión en base al destino. Esto significa que simplemente pueden inundar en los anuncios del sistema de encaminamiento y, tras la convergencia local del sistema de encaminamiento, pueden ser instanciadas en la base de datos de remisión (o FIB) del puente local, según instrucciones del sistema de encaminamiento. De esta manera, el cálculo distribuido de la conectividad de la capa 2 puede ser aplicado a los puentes de Ethernet sin que sea necesario un sistema de señalización diferenciado para asociar la conectividad con la topología. En su forma más simple, cuando un puente ha calculado que está en la trayectoria más corta entre dos nodos de puente determinados, simplemente instala las direcciones de MAC asociadas con esos puentes en la FIB, las direcciones de MAC de unidifusión que apuntan a cada uno de los puentes de interés y la(s) dirección(es) de MAC que apuntan desde los puentes de interés. Perfeccionamientos ulteriores pueden añadir información de la comunidad de interés a los anuncios de encaminamiento, de tal manera que un puente determine que, cuando está en la trayectoria más corta entre dos nodos, si presentan intersección de comunidad de intereses, puede, en consecuencia, modificar lo que está rellenado en las tablas de remisión.

Una malla única puede ser configurada por cada VLAN utilizando el mecanismo de la PLSB. Normalmente, una sola malla sería suficiente, sin embargo, en el caso de trayectorias iguales puede ser deseable distribuir el tráfico de manera que puedan ser utilizadas trayectorias de coste igual. Allí donde se requieran múltiples permutaciones de conectividad (por ejemplo, una utilización eficiente de las trayectorias de coste igual), esto puede conseguirse mediante la delegación de más de una VLAN a la operación de la PLSB, utilizando a la vez, sin embargo, una sola instancia del protocolo de encaminamiento. Al calcular las trayectorias más cortas, la operación se repite para cada VLAN, al tiempo que se tiene asignado un algoritmo de clasificación específico para cada VLAN, para resolver empates, y la distribución de las cargas en la frontera por toda la gama de las VLAN delegadas en esta modalidad de funcionamiento. No se requieren direcciones adicionales de MAC, dado que su función es identificar sin ambigüedades los puntos terminales, y la VLAN determina el algoritmo de clasificación para la selección de la ruta.

Deberá entenderse que, aunque se describe una sola dirección de MAC de unidifusión por puente, nada impide el uso de una granularidad más precisa, y una dirección de MAC de unidifusión puede referirse a una tarjeta de línea, a una instancia de conmutación virtual (VSI) o a un puerto de UNI (Interfaz de Red de Usuario). Esto puede ser deseable para simplificar el demultiplexado de flujos en un puente de destino.

La supresión de bucles se requiere en la red para mantener la conectividad (si bien de una forma potencialmente degradada) durante periodos de inestabilidad (el periodo entre un cambio de topología, el anuncio de la misma por el sistema de encaminamiento a todos los puentes de la red, y la re-convergencia en una visión común de la nueva topología y la actualización correspondiente de la información de remisión). La inestabilidad en un sistema distribuido frecuentemente significa que, al menos de forma temporal, la visión global de la red no estará sincronizada.

El direccionamiento de Ethernet es plano y no conglomerable, lo que implica un dominio de encaminamiento único, por lo que los bucles de unidifusión transitorios son locales y relativamente inofensivos, y únicamente necesitan afrontarse los bucles de unidifusión persistentes y cualquier bucle de multidifusión. Dado que las métricas son simétricas y comunes para la remisión, tanto por unidifusión como por multidifusión, entonces la trayectoria más corta en cada dirección será la misma entre dos dispositivos cualquiera, para las trayectorias tanto de unidifusión como de multidifusión. Si es la misma, entonces, en una red convergida, cada puente conoce la interfaz por la cual cabe esperar cualquier MAC de Origen determinado, porque en la FIB el puerto, para apuntar hacia el cual debe estar configurado cada MAC, es la trayectoria de retorno. Debería destacarse además que la dirección de origen de un paquete es común tanto para los paquetes de unidifusión como para los paquetes de multidifusión, esto es, la dirección de origen de unidifusión del remitente.

En cualquier sistema distribuido los bucles transitorios aparecerán conjuntamente con los cambios de la topología. En casos excepcionales también pueden producirse bucles permanentes, como consecuencia de errores de implementación, o de problemas de hardware. Esto es también cierto para una red que comprenda múltiples dominios de encaminamiento debidos a problemas de configuración o de criterio; sin embargo, únicamente se toma en consideración un único dominio o una jerarquía estricta en la PLSB (frente a una malla homóloga de dominios de encaminamiento). Los bucles se forman cuando algunos nodos conocen información acerca de la red y cuando otros no la conocen. Esto se producirá debido a los retardos de propagación de la información de la red, lo cual con frecuencia significa que no todos los nodos convergen al mismo tiempo. Para que funcione el encaminamiento distribuido, hay una hipótesis de que a la postre todos los nodos sanos tendrán una visión sincronizada y habrán calculado un resultado común.

Como se ha indicado con anterioridad, las métricas simétricas se utilizan de tal manera que la trayectoria más corta entre dos nodos cualesquiera sea idéntica en ambas direcciones. Cuando se combina con la configuración de la base de datos de remisión, mediante el encaminamiento de estados de enlaces, existirá información suficiente en la base de datos de remisión para permitir que se modifiquen los procedimientos tradicionales de aprendizaje de MAC,

para que constituyan una auditoría acerca de si los paquetes son o no recibidos por las interfaces esperadas (el segmento de llegada procedente de un origen determinado se corresponde con el segmento dispuesto sobre la trayectoria más corta con respecto a ese origen), mediante la ejecución lo que se denomina un Control de Remisión de Trayectoria Inversa (RPFC). Esto permite la auditoria, paquete por paquete, de la ausencia de bucles sin tener que bloquear los puertos o interrumpir groseramente de otro modo la conectividad de la red. Esto produce una conectividad absoluta de Ethernet exenta de bucles sin el uso del STP.

El puente lleva a cabo un control de saneamiento sobre los paquetes, en base a una comparación de la dirección de MAC de Origen, contenida en el paquete y en el segmento por el que llega el paquete, con lo que está configurado para esa misma dirección de MAC como destino en la base de datos de remisión. Cuando se habilita la vigilancia del RPFC, si el segmento aprendido para la dirección de MAC de origen modificará una entrada estática, o si no hay ninguna entrada estática, entonces el paquete se descarta. Por ejemplo, con referencia a la Fig. 2a, si un paquete que incorpora el MAC de Origen del puente 110 llega al puente 112 a través de los puertos asociados con los otros enlaces de conexión a los puentes 114, 118, 120, 122 o 124, el paquete es descartado, dado que los puertos no tendrían una entrada asociada con el MAC de Origen para el puente 110. El RPFC supone una implementación exenta de errores y coherente del sistema de encaminamiento de estados de enlaces dentro de la sub-red.

Como se ha indicado con anterioridad, una red correctamente convergida presentará una trayectoria bidireccional más corta entre cualquier par de puentes de la red. El encaminamiento de la PLSB, por definición, asigna un “peso igual” a ambas direcciones de un enlace. Una vez habilitado el RPFC, un paquete que va desde el puente A hasta el puente B es el “Y” lógico de la convergencia correcta de todos los nodos intermedios para ambas direcciones. Cualquier paquete que encuentre trayectorias incorrectas o no convergentes será descartado, antes que incurrir en el riesgo de que forme un bucle.

La Fig. 3 es una representación esquemática de la forma en que puede producirse la formación de un bucle en una red. El ejemplo empieza con un sistema en funcionamiento que remite desde el dispositivo B al dispositivo A, y viceversa, en la etapa 301. Tal y como se muestra en la etapa 302, para iniciar un posible bucle transitorio, por ejemplo, el enlace desde el nodo Y al dispositivo A debe fallar Y el dispositivo A debe tener origen doble sobre el bucle, de forma que el nodo Y siga intentando suministrar el paquete a través del segundo enlace. La creación de un bucle en una red de PLSB presupone que de alguna manera han fallado los mecanismos de supresión del bucle.

Como se muestra en la etapa 303, para mantener el bucle en marcha en el puente Z, el puente Z debe creer que la ruta más corta hacia el puente Y es en sentido contrario al de las agujas del reloj, a través del puente X, en directa contradicción con el puente Y, el cual ha decidido ir directamente del puente Y al puente Z, lo cual solo es coherente con el puente Z hacia el puente Y, O el puente Z hacia el dispositivo A.

Para mantener el bucle en marcha en el puente X, debe entonces existir un segundo fallo, tal y como se muestra en la etapa 304. Sin embargo, cuando se emplea el RPFC, se requiere un bucle, de manera simultánea en ambas direcciones directa e inversa. Es fácil imaginar desde el punto de vista conceptual un bucle en una dirección hacia delante pero es menos fácil imaginar que ello suceda en ambas direcciones. Un bucle es específico para una trayectoria más corta entre dos dispositivos. Por tanto, un bucle para una dirección de MAC específica no significa que todo el tráfico hacia esa dirección forme un bucle, sino solo aquél para el cual la trayectoria de retorno esté también en un bucle congruente.

La inexistencia garantizada de bucles puede ser consolidada mediante una prueba informal intuitiva. Dos direcciones contra-rotativas en un bucle no pueden existir de manera simultánea: las condiciones para crear una tal estructura de remisión presentan de manera inherente una paradoja si las condiciones para producir un bucle en una dirección son duplicadas en espejo. El RPFC requiere que un bucle sea congruente tanto en la dirección directa como en la inversa. La esencia de la prueba intuitiva es que, en un sistema sano, esto no puede ser verdad de manera simultánea para ambas direcciones. Para que haya una trayectoria más corta entre un par determinado de nodos sobre una trayectoria distinta a la actualmente en funciones, se necesita añadir enlaces o recursos, y el conocimiento de eso necesita ser confinado en una sola dirección para que efectivamente se forme un bucle. Requerir que el conocimiento del recurso añadido sea simétrico (en ambas direcciones) de manera simultánea para frustrar el RPFC es inherentemente una paradoja.

Deberá también destacarse que si una combinación de fallos o una implementación insana efectivamente formaran un bucle, el bucle tendría la propiedad de que, una vez formado, ningún tráfico adicional podría entrar en el bucle, por lo que los paquetes solo podrían salir del mismo si acertaran con un punto de replicación. Tal y como se muestra de manera ilustrativa en la Fig. 4, cuando un bucle 402 se forma entre múltiples puentes, debido al RPFC la única fuente válida para los paquetes en un bucle es el propio bucle. Los paquetes en bucle están constreñidos a aquellos paquetes ya atrapados en el bucle. Ningún tráfico adicional desde los puentes externos al bucle, desde los nodos 404, 406, 408 y 410, puede entrar en el bucle. Esto significa que solo se pueden formar bucles sencillos, si es que se forma alguno. Un paquete duplicado no puede volver a fundirse en el flujo original, dado que es imposible que un bucle acepte más de una interfaz como origen válido para una dirección de origen determinada.

El RPFC puede, por consiguiente, ser utilizado como mecanismo de prevención de bucles que lleva a cabo una vigilancia, paquete por paquete, de la inexistencia de bucles (frente al TTL o bloqueo de puertos). Es también

importante destacar que la granularidad de un bucle está significativamente restringida en cuanto tiene que existir para un par de origen / destino.

El RPFC tiene la ventaja de que no requiere modificaciones en el paquete de Ethernet y modificaciones mínimas en la implementación de un puente. El RPFC es agresivo para vigilar, ya que puede haber otras causas de que un paquete llegue por una interfaz inesperada; por consiguiente, es deseable la capacidad de no emplearlo en circunstancias selectivas. La multidifusión de la PLSB se produce exclusivamente sobre la base de las direcciones de MAC de Ethernet (por ejemplo, por oposición a la inundación en una VLAN). Las direcciones de MAC de multidifusión de Ethernet incluyen una indicación de multidifusión explícita sobre la dirección de MAC de destino que permite que sea aplicado un tratamiento de vigilancia única a los paquetes de unidifusión o de multidifusión (obsérvese que, de modo similar al PBT, la inundación de paquetes desconocidos está prohibida). Para la remisión de unidifusión configurada, un bucle transitorio no es catastrófico, dado que la red simplemente almacena en memoria intermedia los paquetes en el bucle hasta el momento en el que el bucle se desenrede o se sobrepase la capacidad de almacenamiento en memoria intermedia, lo que da como resultado el descarte del tráfico adicional recibido. Esto significa que durante la convergencia de la red, la supresión de bucles puede ser desactivada, dado que los bucles transitorios son inofensivos y no replicantes (la red simplemente almacena en memoria intermedia hasta que se despejen los bucles); cuando la red sea estable, la supresión de la unidifusión es activada de nuevo para sofocar instantáneamente cualquier bucle persistente.

Pueden considerarse otras estrategias, tales como la habilitación de forma periódica del RPFC para la unidifusión, simplemente para controlar si existe una condición de bucle persistente (detectada a través del descarte de tráfico) y, si no es así, desactivarla de nuevo. Las consecuencias de la formación de bucles son considerablemente diferentes para el tráfico de multidifusión: un bucle transitorio podría dar como resultado una replicación ilimitada; por consiguiente, el RPFC nunca está inhabilitado para paquetes con direcciones de MAC de destino de multidifusión. Para la multidifusión, la supresión de bucles debe mantenerse activa todo el tiempo, de manera que la remisión por multidifusión no convergente descarte paquetes de manera agresiva e impida los bucles.

Los árboles no afectados por un cambio de topología continuarán funcionando normalmente, ya que no hay ningún cambio en la FIB o inestabilidad para aquellas trayectorias asociadas, no asociadas con el cambio de la topología, pero aquellas afectadas por el cambio pueden experimentar interrupciones en la conectividad, dado que el RPFC descarta paquetes para trayectorias de multidifusión no convergentes. En términos de la red global, esto será algo análogo a un “semi-apagado” temporal del servicio. Las entradas aprendidas no sustituyen las entradas configuradas, por lo que la habilitación / inhabilitación de la vigilancia no tendrá como resultado la corrupción de la configuración instanciada por el sistema de encaminamiento.

La Fig. 5 es una representación esquemática de una posible implementación de un nodo 500 de puente para la implementación de la PLSB. El módulo 502 del sistema de encaminamiento intercambia información con los puentes homólogos en la red con respecto a la topología de la red, utilizando un encaminamiento del protocolo de estados de enlaces. Tal y como se analizó con anterioridad, el intercambio de información hace posible que los puentes generen una visión sincronizada de la topología de la red, lo cual puede entonces permitir que el módulo del sistema 502 de encaminamiento calcule el árbol de las trayectorias más cortas (utilizando un algoritmo analizado con anterioridad) durante la convergencia. La FIB 504 es rellenada con las entradas adecuadas para dirigir el tráfico a través de la red en base a las trayectorias determinadas. Un módulo 506 de control de origen de RPFC procesa los paquetes entrantes 500 y lleva a cabo una consulta en la FIB 504 para determinar si el puerto recibido coincide con el puerto identificado en la FIB 504 para el MAC de Origen específico. Si el puerto / MAC de Origen recibido no se corresponde con el puerto / MAC de origen esperado, el paquete es descartado. De modo similar, si el sistema 502 de encaminamiento identifica, para el control 506 de origen de RPFC, que la red está en el proceso de convergencia, la supresión de bucles es inhabilitada para la unidifusión. Cuando la red ha convergido, la supresión de bucles es rehabilitada para los paquetes de unidifusión. Para los paquetes de multidifusión, tal y como han sido identificados por la dirección de destino de multidifusión, el control 506 de origen de RPFC nunca es inhabilitado durante la convergencia. Si el paquete pasa el módulo 506 de control de origen de RPFC, o si el control es inhabilitado, el módulo de consulta 508 de destino determina a partir de la FIB 504 por qué puerto debe ser remitido el paquete a la dirección de MAC de destino de unidifusión o de multidifusión. Si no hay una entrada válida, el paquete puede entonces ser descartado. Si el puente está en la frontera de la red, la encapsulación MAC-en-MAC del paquete puede producirse (no mostrada) utilizando direcciones únicas de unidifusión o de multidifusión antes de la remisión de los paquetes salientes. También debería entenderse que los módulos descritos tienen únicamente finalidad ilustrativa y pueden ser implementados mediante la combinación o distribución de funciones entre los módulos de un nodo de puente, como debería advertir una persona experta en la materia.

La Fig. 6 muestra una forma de realización de un procedimiento de configuración de un puente 500 de la PLSB para su funcionamiento. Cuando se produce un cambio en la topología de la red en la etapa 602, como por ejemplo un fallo de un puente o de un enlace, la información del estado es intercambiada entre los puentes en la red en la etapa 604 por el módulo 502 del sistema de encaminamiento. El módulo 502 del sistema de encaminamiento construye una visión sincronizada de la configuración de red mediante el almacenamiento de la información de la topología en una base de datos residente en el puente. El puente puede entonces determinar las trayectorias más cortas entre puentes homólogos en la etapa 606 utilizando un algoritmo de la trayectoria más corta, de acuerdo con lo descrito anteriormente. La FIB 504 es luego rellenada en la etapa 608 con las entradas de encaminamiento adecuadas para

posibilitar la conectividad. Los paquetes pueden ser procesados luego por el puente. Si se produce un cambio en la topología de la red, el proceso es reiniciado.

La Fig. 7 muestra una forma de realización de un nodo 500 de puente que procesa los paquetes recibidos. Un paquete es recibido en un puerto del puente en la etapa 702. En la etapa 704 la dirección de destino se utiliza para determinar si el paquete es un paquete de multidifusión o un paquete de unidifusión. Si el paquete es de unidifusión (SÍ en la etapa 704), el sistema de encaminamiento está convergido, el RPFC, por consiguiente, es habilitado (SÍ en la etapa 706) y se lleva a cabo en la etapa 708. Si el RPFC es satisfactorio (SÍ en la etapa 708), es decir, el paquete llegó al puerto esperado para la dirección de MAC de origen asociada, se produce una consulta en la FIB del puerto saliente para el MAC de destino, en la etapa 710. Si el RPFC no es habilitado (NO en la etapa 706), es decir, existen condiciones de formación de bucles y la red no es convergente, el RPFC es omitido y se establece una consulta directamente para la remisión del paquete en la etapa 710. Si hay una entrada para la dirección de MAC asociada (SÍ en la etapa 710), el paquete se remite entonces a su destino en la etapa 714. Si el RPFC no es satisfactorio (NO en la etapa 708), es decir, el paquete no llegó al puerto esperado en base a la dirección de origen, el paquete es descartado en la etapa 712. De modo similar, si el paquete no presenta una entrada adecuada (NO en la etapa 710), el paquete es descartado en la etapa 712.

Si el paquete es un paquete de multidifusión (NO en la etapa 704), el RPFC es siempre habilitado y se lleva a cabo en la etapa 708. Si el RPFC es satisfactorio (SÍ en la etapa 708), es decir, el paquete llegó al puerto esperado para la dirección de MAC asociada, se produce una consulta en la FIB del puerto saliente para el MAC de destino, en la etapa 710. Si hay una entrada para la dirección de MAC asociada (SÍ en la etapa 710), el paquete se remite luego a su destino, en la etapa 714. Si el RPFC no es satisfactorio (NO en la etapa 708), es decir, el paquete no llegó al puerto esperado en base a la dirección de origen, el paquete es descartado en la etapa 712. De modo similar, si el paquete no presenta una entrada apropiada (NO en la etapa 710), el paquete es descartado en la etapa 712. Tal y como se ha indicado con anterioridad, el RPFC puede ser habilitado de forma periódica para unidifusión, simplemente para controlar si existe una condición de bucle persistente (detectada por medio de un descarte de tráfico) y, en caso contrario, desactivarlo de nuevo.

Hasta ahora, se ha descrito una red con puentes de estados de enlaces de proveedores que da soporte a una única comunidad de interés; sin embargo, también es posible dar soporte a múltiples comunidades de interés, en donde cualquier comunidad individual únicamente requiere la conectividad con un subconjunto de los puertos y, por consiguiente, con puentes en la red de PLSB. Lo que se requiere es conectividad de multidifusión restringida al conjunto de puentes que participan en la comunidad de interés, y conectividad de unidifusión común, y un mecanismo para la asociación de un paquete determinado con una comunidad de interés. El campo I–SID (Identificador de servicio extendido) del estándar 802.1ah del IEEE es un ejemplo de un mecanismo que asocia un paquete con una comunidad de interés, El identificador de la comunidad de interés (por ejemplo, I–SID) puede también ser incorporado a los anuncios del sistema de encaminamiento, para que los nodos puedan identificar el interés en las comunidades de interés identificadas con el I–SID; finalmente, cada puente asocia una dirección única de multidifusión grupal con cada I–SID anunciado. Un puente que se encuentre en la trayectoria más corta entre dos puentes instala la(s) dirección(es) de MAC de unidifusión asociada(s) con cada puente, y las direcciones de MAC de multidifusión para todos los I–SID comunes a los dos puentes. La consecuencia de esto es que un puente de frontera determinado presentará conectividad de unidifusión para todos los puentes homólogos, y conectividad de multidifusión única para cada comunidad de interés identificada por I–SID. Esto tendrá la forma de ser una hoja en un árbol de unidifusión de multipunto a punto (mp2p) para cada homólogo, y ser la raíz de un árbol de multidifusión de punto a multipunto (p2mp) (S, G), donde S es la dirección del origen y G es la dirección del grupo de multidifusión, para el conjunto de nodos homólogos para cada comunidad de interés. Si el par de puentes no tiene ningún I–SID en común, un perfeccionamiento ulterior podría ser que no se instalara ninguna dirección de MAC de unidifusión. De modo similar, el par de puentes pueden ser puentes de tránsito y haber escogido no ofrecer ninguna información de MAC para flujos, ya sean terminados u originados por el nodo. De esta manera, no solo queda la conectividad de multidifusión confinada a grupos específicos de interés, sino que el enfoque es frugal en cuanto al consumo del espacio de las tablas de remisión para la conectividad de unidifusión.

La Fig. 8 muestra la forma en que las redes privadas virtuales (VPN) pueden ser correlacionadas por encima de la red de PLSB, haciendo posible que un árbol de multidifusión único sea correlacionado por cada VPN, por cada puente de frontera. En el escenario de VPN de multidifusión, el tráfico de multidifusión es solo suministrado a los puentes que participan en la VPN. Las direcciones de multidifusión de grupos de VPN están instaladas para las trayectorias que son comunes. Cuatro redes VPN están identificadas como V1, V2, V3 y V4. Múltiples VPN pueden ser alojadas por un puente como, por ejemplo, el puente 110 y pueden ser dispositivos terminales de VPN individuales. Para cada VPN, por ejemplo, V1 y V3, se crean árboles de multidifusión únicos. Solo son identificadas las rutas a los puentes que contienen puntos terminales de la VPN correspondiente. Por ejemplo, se requieren un árbol de encaminamiento para la V1, trayectorias hacia el puente 116 y entre el puente 112 hacia el puente 122 y el puente 124. De manera similar, se requieren un árbol de encaminamiento para V3, trayectorias hacia los puentes 112 y sobre los puentes 118 y 124. Esto elimina la posibilidad de que el tráfico de VPN desde V1 sea suministrado a puentes que no alberguen los dispositivos terminales de la VPN V1 o la VPN V3. Cada VPN puede tener un árbol por puente de frontera, único para la VPN en base al algoritmo de la trayectoria más corta.

La conectividad asimétrica puede ser construida de modo similar a la capacidad para definir las VPN. Normalmente, la PLSB genera conectividad de multidifusión (*, G), donde * significa todos los orígenes, y la G representa el grupo de multidifusión, como una malla completa de árboles de multidifusión (S, G), donde la S indica un origen dentro de un grupo “G”. También puede ser deseable, para una instancia de un servicio determinado, limitar la conectividad a (S, G). Esto puede llevarse a cabo con facilidad para la multidifusión mediante la adición de atributos al anuncio que indica el deseo de ser un origen, un sumidero o tanto un origen como un sumidero, para un grupo de multidifusión determinado. Los puentes que establecen que están en la trayectoria más corta entre otros dos puentes utilizan los atributos de origen / sumidero para determinar qué direcciones del grupo de multidifusión deberían ser instaladas. Puede ser construida una conectividad más compleja mediante la repetición de instancias de ésta con configuraciones de atributos diferentes. Por ejemplo, se pueden contemplar dos conjuntos de dispositivos en una red, participando ambos en dos VPN. Como cuestión de criterio, la conectividad solo se permite entre los conjuntos y no dentro de los conjuntos (constituyendo una instanciación práctica la conectividad entre la oficina central y una oficina sucursal). Por lo que la primera VPN presenta un atributo de origen para el conjunto A, y un atributo de sumidero para el conjunto B. La segunda VPN tiene un atributo de sumidero para el conjunto A y un atributo de origen para el conjunto B. Cuando se considera una superposición de puentes transparentes, la imposición de dichas restricciones significa que la inundación desconocida desde el conjunto A está limitada al conjunto B, y viceversa. Por tanto, los dos conjuntos nunca pueden aprender conectividad dentro del conjunto, y los dispositivos del conjunto A solo se comunican con el conjunto B, y viceversa.

Como se muestra en la Fig. 9, las redes pueden ser ajustadas a escala mediante la utilización de otras tecnologías tales como el PBT (tal y como se describe en la solicitud US20050220096 transferida por el procedimiento común) y el PBB del estándar 802.1ah. El PBB 904 puede ser utilizado como un equivalente aproximado de los Encaminadores de Fronteras de Áreas (ABR) para vincular entre sí áreas de la PLSB tales como los dominios 902 de las WAN de la PLSB y los dominios metropolitanos 906 de la PLSB, o extender la conectividad utilizando el PBT 908. La inspección de la información de cliente en las fronteras de las áreas permite que un área homóloga sea simplemente modelada como una dirección de MAC única en el sistema de encaminamiento de las áreas adyacentes, o cooperar con los dominios de concurrencia del PBT que aparecen como un único MAC–B a los homólogos, y cualquiera de estas técnicas suministra la sumarización. Para asegurar la carencia de bucles entre los dominios, la red es una jerarquía estricta de dominios y una malla de dominios de encaminamiento no puede disponer de soporte.

En el extremo alejado de la red, se aprecia el MAC–B de origen para un MAC–C de origen determinado, de modo similar a la forma en que opera el aprendizaje del origen con el MAC–B de origen suplantando al Identificador de puerto. Este procedimiento es modificado trivialmente para que opere con la formación de puentes de estados de enlaces. El procedimiento de aprendizaje del MAC–C al MAC–B queda sin modificación. Allí donde un MAC–B no ha sido aprendido para un MAC–C, se utiliza la dirección adecuada de multidifusión del puente para la comunidad de interés (habitualmente, la VPN cliente), y esto proporciona la emulación requerida en el espacio de la PLSB de una difusión de MAC–C.

La PLSB proporciona una red con puentes MAC–en–MAC, eliminándose la mayoría de los lados inferiores del Protocolo de Árbol de Recubrimiento. Esto se traduce en una mucho mejor utilización de la conectividad de malla, y una convergencia mucho más rápida, dado que cada dispositivo incorpora una base de datos de estados de enlaces. La conectividad de unidifusión no es perturbada durante la re-convergencia de la red. Además, la PLSB proporciona la capacidad de operar codo con codo con el PBT (utilizando una gama distinta de VID) o concatenada con el PBT (en una implementación de concentrador), y los atributos de Ethernet están completamente preservados, proporcionando una emulación perfecta para las capas clientes.

Las formas de realización de la invención descritas con anterioridad pretenden ser únicamente ilustrativas.

Las realizaciones de la invención pueden resumirse según lo siguiente:

Un nodo de Ethernet con puentes de estados de enlaces de proveedores, comprendiendo el nodo: al menos una dirección asociada de control de acceso al medio (MAC) de unidifusión; al menos una dirección asociada de MAC de multidifusión; un módulo de encaminamiento para intercambiar información de encaminamiento de estados de enlaces entre los nodos, en base a la respectiva dirección de MAC de unidifusión y una pluralidad de direcciones de MAC de multidifusión de nodos homólogos, y para determinar la conectividad de la trayectoria más corta entre nodos homólogos, y en donde, cuando se dispone de múltiples trayectorias de igual coste, la trayectoria más corta seleccionada se dispone para que sea congruente para todos los puentes que participan en el intercambio de información de encaminamiento; una base de información de remisión (FIB) rellenada con información de remisión recibida desde el módulo de encaminamiento para identificar la conectividad desde el nodo a los nodos puente homólogos, en donde las direcciones de MAC de unidifusión apuntan a nodos homólogos y las direcciones de multidifusión apuntan desde nodos homólogos; un módulo de control de remisión de trayectoria inversa (RPFC) para inspeccionar los paquetes entrantes y determinar si los paquetes llegaron o no por el mismo puerto de ingreso que se usará como puerto de egreso, según lo determinado por la FIB, para remitir un paquete con una dirección de MAC de destino igual a la dirección de MAC de origen del ingreso; y un módulo de remisión para determinar, a partir de la FIB, si un puerto de egreso del nodo está asociado a la dirección de MAC de destino de un puente homólogo, y remitir el paquete.

El módulo de RPFC puede desechar el paquete si se determina que el paquete no llegó por el puerto de ingreso correcto.

El módulo de RPFC puede ser inhabilitado para el tráfico de unidifusión cuando la topología de la red y el módulo de encaminamiento no son convergentes.

El módulo de RPFC puede ser habilitado periódicamente para paquetes de unidifusión, para comprobar si existe una condición de bucle persistente, detectando el desecho de paquetes.

El módulo de remisión puede desechar el paquete si un puerto de egreso no está identificado en la FIB para la dirección de MAC de destino del paquete.

Dichas (al menos una) direcciones de MAC de unidifusión pueden estar asignadas a uno entre una tarjeta de línea, una instancia de conmutación virtual (VSI) o un puerto de UNI, u otra nomenclatura arbitraria de terminaciones en un puente, o ser representativas de terminaciones de MAC más allá del puente.

El módulo de salida puede determinar la trayectoria más corta por el algoritmo de Floyd o el algoritmo de Dijkstra.

El módulo de la FIB puede ser rellenado en base a información referida solamente a nodos en la trayectoria más corta.

La información de estado de enlace puede incluir información de comunidades de interés dentro de los anuncios de encaminamiento, de modo que cada puente pueda determinar, cuando está en la trayectoria más corta entre dos nodos, si los dos nodos tienen comunidades de intereses intersecantes; el puente modifica en consecuencia lo que se rellena en las tablas de remisión.

La información de estado de enlace puede comprender además la inclusión de una pluralidad de identificadores de LAN virtual (VLAN), en donde cada identificador se usa para definir una instancia de la malla en el plano de control.

La pluralidad de identificadores de VLAN puede ser usada para dividir la red, a fin de facilitar la dispersión del tráfico en la malla, de modo que puedan ser utilizadas múltiples trayectorias de igual coste.

El módulo de encaminamiento puede determinar las trayectorias más cortas para cada VLAN, habiendo asignado a la vez un algoritmo individual de clasificación a cada VLAN, para el desempate entre múltiples trayectorias de igual coste, para cargar la distribución entre una gama de las VLAN.

La información de estado de enlace puede incluir un Identificador de servicio extendido (I-SID) incorporado en los anuncios de encaminamiento de estados de enlaces, para identificar un grupo único de multidifusión, en donde un puente que está en la trayectoria más corta entre dos puentes instala la dirección de MAC de unidifusión asociada a cada puente, y las direcciones de MAC de multidifusión para todos los I-SID comunes a los dos puentes.

Un procedimiento de configuración y operación de un nodo de Ethernet con puentes de estados de enlace de proveedores en una red mallada, comprendiendo el procedimiento: intercambiar información de estado de enlaces con nodos homólogos, en donde cada nodo tiene al menos una dirección asociada de control de acceso al medio (MAC) de unidifusión y al menos una dirección de MAC de multidifusión; determinar las trayectorias más cortas hasta los nodos homólogos, por medio de un algoritmo de trayectoria más corta, en base a la información intercambiada de estados de enlace, y en donde, cuando se dispone de trayectorias múltiples de igual coste, la trayectoria más corta seleccionada se dispone para que sea congruente para todos los puentes que participan en el intercambio de información de encaminamiento; rellenar una base de información de remisión (FIB) con las trayectorias más cortas determinadas, utilizando las direcciones asociadas de MAC de unidifusión que apuntan a los nodos homólogos y las direcciones de MAC de multidifusión que apuntan desde los nodos homólogos; realizar un control de remisión de trayectoria inversa (RPFC), determinando, por la inspección de la dirección de MAC de origen de un paquete entrante, si el paquete llegó o no por el mismo puerto de ingreso del nodo, que se usará como un puerto de egreso del nodo para remitir un paquete con una dirección de MAC de destino igual a la dirección de MAC de origen de ingreso, en donde el paquete es desechado si el RPFC falla; y remitir el paquete a un puente homólogo, si el RPFC tiene éxito, mediante un puerto de egreso del nodo asociado al MAC de destino del paquete, según lo identificado por la FIB.

La etapa de ejecutar el RPFC puede ser omitida selectivamente para el tráfico de unidifusión cuando la topología de la red y, por lo tanto, el módulo de encaminamiento no son convergentes.

La etapa de la determinación de las trayectorias más cortas puede utilizar un algoritmo de Floyd o el algoritmo de Dijkstra.

El algoritmo de la trayectoria más corta puede incluir además una medida del coste, seleccionada entre un grupo que comprende la capacidad, la velocidad, el uso y la red de disponibilidad de otras aplicaciones que utilizan la red.

El módulo de encaminamiento puede utilizar métricas comunes para la conectividad de unidifusión y de multidifusión, de modo que haya congruencia de remisión entre paquetes de cualquier tipo.

La etapa del relleno de la FIB puede estar basada solamente en información referida solamente a nodos en la trayectoria más corta.

El paquete puede ser la encapsulación MAC-en-MAC, según la norma 802.1ah.

La etapa de intercambio de información de estados de enlace puede comprender adicionalmente la inclusión de información de comunidades de interés dentro de los anuncios de encaminamiento, de modo que cada puente pueda determinar, cuando está en la trayectoria más corta entre dos nodos, si los dos nodos tienen comunidades de intereses intersecantes; el puente modifica en consecuencia lo que está rellenado en las tablas de remisión.

La etapa de intercambiar información de estados de enlace puede comprender adicionalmente la inclusión de una pluralidad de identificadores de LAN virtual (VLAN), en donde cada identificador se usa para definir una instancia de la malla en el plano de control.

La pluralidad de identificadores de VLAN puede ser usada para dividir la red, a fin de facilitar la dispersión del tráfico en la malla, de modo que puedan utilizarse las múltiples trayectorias de igual coste.

La etapa de la determinación de las trayectorias más cortas puede ser repetida para cada VLAN, habiendo asignado a la vez un algoritmo individual de clasificación a cada VLAN, para el desempate entre múltiples trayectorias de igual coste, para cargar la distribución entre una gama de las VLAN.

La etapa de intercambio de información de estados de enlace puede comprender adicionalmente la inclusión de un Identificador de servicio extendido (I-SID), incorporado en los anuncios de encaminamiento de estados de enlace, para identificar un grupo único de multidifusión, en donde un puente que está en la trayectoria más corta entre dos puentes instala la dirección de MAC de unidifusión asociada a cada puente, y las direcciones de MAC de multidifusión para todos los I-SID comunes para los dos puentes.

La etapa de intercambio de información de estados de enlace puede comprender adicionalmente proporcionar conectividad asimétrica de VPN, añadiendo atributos al anuncio de estado de enlace, indicando el deseo del puente de ser un origen, un sumidero, o tanto un origen como un sumidero, para un grupo determinado de multidifusión, estableciendo el puente que está en la trayectoria más corta entre otros dos puentes, usando los atributos de origen / sumidero para determinar cuáles direcciones de grupos de multidifusión deberían ser instaladas.

Una red con puentes de Ethernet que comprende: una pluralidad de puentes, teniendo cada uno una base de información de remisión (FIB) que contiene información de remisión para puentes homólogos en la red, siendo cada puente capaz de realizar un control de remisión de trayectoria inversa (RPFC), para determinar si un paquete entrante llegó por el mismo puerto de ingreso del puente, que será usado como un puerto de egreso del puente para remitir un paquete con una dirección de MAC de destino igual a la dirección de MAC de origen del paquete entrante, interconectando una pluralidad de trayectorias los puentes y formando la red mallada; y en donde la FIB se rellena en base a la información de estado de enlace intercambiada entre la pluralidad de puentes, y es usada para determinar la trayectoria más corta entre puentes homólogos, en donde la determinación de las trayectorias escogidas, cuando se dispone de múltiples trayectorias de igual coste, se dispone para que sea congruente para los puentes homólogos.

Dichos uno o más puentes pueden tener al menos una dirección asociada de control de acceso al medio (MAC) de unidifusión y al menos una dirección asociada de MAC de multidifusión, que es utilizada al rellenar los puentes homólogos en la FIB.

El RPFC puede ser inhabilitado selectivamente para paquetes de unidifusión, según lo identificado por la dirección de destino del paquete, y habilitado para paquetes de multidifusión cuando la topología de la red no sea convergente entre puentes.

Los subconjuntos de puentes pueden formar dominios individuales de formación de puentes de estados de enlaces de proveedores (PLSB), que pueden estar interconectados mediante un MAC que identifique dominios homólogos de PLSB.

Las redes del Transporte Troncal de Proveedores (PBT) pueden estar interconectadas con puentes de frontera de la red puente, mediante identificadores de MAC del PBT.

El Puente Troncal de Proveedores de la norma 802.1ah de proveedores puede ser superpuesta sobre la red puente.

Un mecanismo de criterios de conectividad puede ser construido utilizando uno, entre la pluralidad de puentes, como una hoja en un árbol de unidifusión multipunto a punto (mp2p) hasta cada puente homólogo, y la raíz de un árbol de multidifusión punto a multipunto (p2mp) (S, G) hasta el conjunto de nodos homólogos para cada comunidad de interés.

REIVINDICACIONES

1. Un procedimiento de operación de un puente (500) de Ethernet en una red, comprendiendo el procedimiento:

intercambiar (604) información de estado de enlaces con puentes homólogos, en donde la información de estado de enlaces comprende identificadores de comunidades de interés, asociados a puentes homólogos; y
determinar (606) las trayectorias más cortas entre puentes homólogos, en base a la información de estado de enlaces intercambiada, usando un algoritmo de trayectoria más corta;
estando el procedimiento **caracterizado por:**

rellenar (608) al menos una base de información de remisión, FIB, con direcciones de MAC de multidifusión, en asociación con puertos de egreso determinados usando las trayectorias más cortas y los identificadores de comunidades de interés asociados a puentes homólogos, identificando unívocamente cada dirección de MAC de multidifusión un respectivo puente homólogo y una respectiva comunidad de interés, siendo el puente homólogo una raíz de un respectivo árbol de multidifusión para la comunidad de interés; y
remitir (714) paquetes de multidifusión en base a sus respectivas direcciones de MAC de multidifusión, de acuerdo a la FIB, por lo cual la conectividad de multidifusión para cada comunidad de interés está confinada a esa comunidad de interés.

2. El procedimiento de la reivindicación 1, en el cual el algoritmo de la trayectoria más corta es operable, cuando se dispone de múltiples trayectorias más cortas de igual coste entre dos puentes, para seleccionar una de las trayectorias más cortas de igual coste entre los dos puentes, congruente con las selecciones de trayectoria en los puentes homólogos.

3. El procedimiento de la reivindicación 1, adicionalmente **caracterizado por** desechar el paquete de multidifusión entrante cuando no hay ninguna entrada en dicha al menos una FIB para la dirección de MAC de multidifusión del paquete entrante.

4. El procedimiento de la reivindicación 1, adicionalmente **caracterizado por** realizar un control de remisión de trayectoria inversa para determinar si el paquete de multidifusión entrante llega o no por un puerto que no coincide con un puerto de egreso asociado, en dicha al menos una FIB, a una dirección de MAC de origen de unidifusión del paquete entrante.

5. El procedimiento de la reivindicación 1, adicionalmente **caracterizado por** desechar un paquete de multidifusión entrante cuando el paquete de multidifusión entrante llega por un puerto que no coincide con un puerto de ingreso asociado, en dicha al menos una FIB, a la dirección de MAC de multidifusión del paquete entrante.

6. El procedimiento de la reivindicación 1, adicionalmente **caracterizado por** determinar al menos un árbol de multidifusión en base a la información de estados de enlace intercambiada antes de rellenar la base de información de remisión con direcciones de MAC de multidifusión.

7. El procedimiento de la reivindicación 1, en el cual los identificadores de comunidades de interés son los I-SID.

8. El procedimiento de la reivindicación 1, adicionalmente **caracterizado por:**

comprender adicionalmente la información de estados de enlace intercambiada un atributo de origen para cada nodo y cada comunidad de interés con soporte por parte de ese nodo, indicando el atributo de origen si ese nodo ha de actuar o no como un nodo de origen para esa comunidad de interés;
comprender adicionalmente la información de estados de enlace intercambiada un atributo de sumidero para cada nodo y cada comunidad de interés con soporte por parte de ese nodo, indicando el atributo de sumidero si ese nodo ha de actuar o no como un nodo sumidero para esa comunidad de interés; y
rellenar dicha al menos una base de información de remisión con direcciones de MAC de multidifusión correspondientes a respectivos puentes homólogos y respectivas comunidades de interés, para que sean congruentes con los atributos de origen y sumidero de cada nodo para las comunidades de interés correspondientes a las direcciones de MAC de multidifusión.

9. El procedimiento de la reivindicación 1, en el cual:

el intercambio de información de estados de enlace con puentes homólogos comprende intercambiar información de estados de enlace, que comprende direcciones de MAC de unidifusión con soporte por parte de cada puente homólogo; y
rellenar dicha al menos una base de información de remisión comprende rellenar la base de información de remisión con direcciones de MAC de unidifusión con soporte por parte de los nodos homólogos, usando las trayectorias más cortas determinadas;
comprendiendo adicionalmente el procedimiento remitir paquetes entrantes con direcciones de MAC de unidifusión, usando la base de información de remisión.

10. El procedimiento de la reivindicación 9, que comprende adicionalmente:

realizar un control de remisión de trayectoria inversa para paquetes entrantes con direcciones de MAC de unidifusión, considerándose un fallo del control de remisión de trayectoria inversa cuando un paquete entrante llega por un puerto de ingreso que no coincide con un puerto de egreso asociado, en la base de información de remisión, a una dirección de MAC de origen del paquete entrante; y
desechar paquetes entrantes para los cuales el control de remisión de trayectoria inversa se considera un fallo.

11. Un puente (500) de Ethernet, que comprende:

un módulo (502) de encaminamiento, operable:

para intercambiar información de estados de enlace con puentes homólogos, en donde la información de estados de enlace comprende identificadores de comunidades de interés asociados a puentes homólogos; y
para determinar las trayectorias más cortas entre puentes homólogos, en base a la información de estados de enlace intercambiada, usando un algoritmo de trayectoria más corta; al menos una base de información de remisión, FIB (504); y
un módulo (508) de remisión;
estando el puente **caracterizado por**:

estar dicha al menos una FIB rellenada con direcciones de MAC de multidifusión, en asociación con puertos de egreso determinados usando las trayectorias más cortas y los identificadores de comunidades de interés asociados a puentes homólogos, identificando unívocamente cada dirección de MAC de multidifusión un respectivo puente homólogo y una respectiva comunidad de interés, siendo el puente homólogo una raíz de un respectivo árbol de multidifusión para la comunidad de interés; y
ser el módulo de remisión operable para remitir paquetes de multidifusión en base a sus respectivas direcciones de MAC de multidifusión, de acuerdo a la base de información de remisión (FIB), por lo que la conectividad de multidifusión para cada comunidad de interés está confinada a esa comunidad de interés.

12. El puente de la reivindicación 11, en el cual el algoritmo de trayectoria más corta es operable, cuando se dispone de múltiples trayectorias de igual coste entre dos puentes, para seleccionar una de las trayectorias más cortas de igual coste entre los dos puentes, congruente con las selecciones de trayectoria en puentes homólogos.

13. El puente de la reivindicación 11, en el cual el módulo de remisión es adicionalmente operable para desechar el paquete de multidifusión entrante cuando no hay ninguna entrada en dicha al menos una FIB para la dirección de MAC de multidifusión del paquete entrante.

14. El puente de la reivindicación 11, en el cual el módulo de remisión es adicionalmente operable para realizar un control de remisión de trayectoria inversa, a fin de determinar si el paquete de multidifusión entrante llega o no por un puerto que no coincide con un puerto de egreso asociado, en dicha al menos una FIB, a una dirección de MAC de origen de unidifusión del paquete entrante.

15. El puente de la reivindicación 11, en el cual el módulo de remisión es adicionalmente operable para desechar un paquete de multidifusión entrante cuando el paquete de multidifusión entrante llega por un puerto que no coincide con un puerto de ingreso asociado, en dicha al menos una FIB, a la dirección de MAC de multidifusión del paquete entrante.

16. El puente de la reivindicación 11, en el cual el módulo de encaminamiento es adicionalmente operable para determinar al menos un árbol de multidifusión, en base a la información de estados de enlace intercambiada antes de rellenar la base de información de remisión con direcciones de MAC de multidifusión.

17. El puente de la reivindicación 11, en el cual los identificadores de comunidades de interés son los I-SID.

18. El puente de la reivindicación 11, en el cual:

el módulo de encaminamiento es operable para el intercambio de información de estados de enlace, que comprende adicionalmente un atributo de origen para cada nodo y cada comunidad de interés con soporte por parte de ese nodo, indicando el atributo de origen si ese nodo ha de actuar o no como un nodo de origen para esa comunidad de interés;
el módulo de encaminamiento es operable para intercambiar información de estados de enlace, que comprende adicionalmente un atributo de sumidero para cada nodo y cada comunidad de interés con soporte por parte de ese nodo, indicando el atributo de sumidero si ese nodo ha de actuar o no como un nodo sumidero para esa comunidad de interés; y
dicha al menos una base de información de remisión está rellenada con direcciones de MAC de multidifusión correspondientes a respectivos puentes homólogos y respectivas comunidades de interés, para que sea congruente con los atributos de origen y de sumidero de cada nodo para las comunidades de interés correspondientes a las direcciones de MAC de multidifusión.

19. El puente de la reivindicación 11, en el cual:

el módulo de encaminamiento es operable para intercambiar información de estados de enlace, que comprende adicionalmente una dirección de MAC de unidifusión con soporte por parte de cada puente homólogo; y
dicha al menos una base de información de remisión está adicionalmente rellenada con direcciones de MAC de unidifusión con soporte por parte de puentes homólogos, que usan las trayectorias más cortas determinadas; y
el módulo de remisión es adicionalmente operable para remitir paquetes entrantes con direcciones de MAC de unidifusión, usando la base de información de remisión.

20. El puente de la reivindicación 19, en el cual el módulo de remisión es adicionalmente operable:

para realizar un control de remisión de trayectoria inversa para los paquetes entrantes con direcciones de MAC de unidifusión, siendo considerado el control de remisión de trayectoria inversa un fallo cuando un paquete entrante llega por un puerto de ingreso que no coincide con un puerto de egreso asociado, en la base de información de remisión, a una dirección de MAC de origen del paquete entrante; y
para desechar paquetes entrantes para los cuales el control de remisión de trayectoria inversa es considerado un fallo.

21. Una red Ethernet que comprende una pluralidad de puentes de Ethernet, siendo al menos uno de los puentes un puente según lo definido por la reivindicación 11.

22. La red de la reivindicación 21, en la cual cada puente de la red es un puente según lo definido en la reivindicación 11.

23. Un procedimiento de operación de una red Ethernet que comprende una pluralidad de puentes de Ethernet, comprendiendo el procedimiento la operación de al menos uno de los puentes de acuerdo al procedimiento definido en la reivindicación 1.

24. El procedimiento de la reivindicación 23, que comprende la operación de cada puente de la red de acuerdo al procedimiento definido en la reivindicación 1.

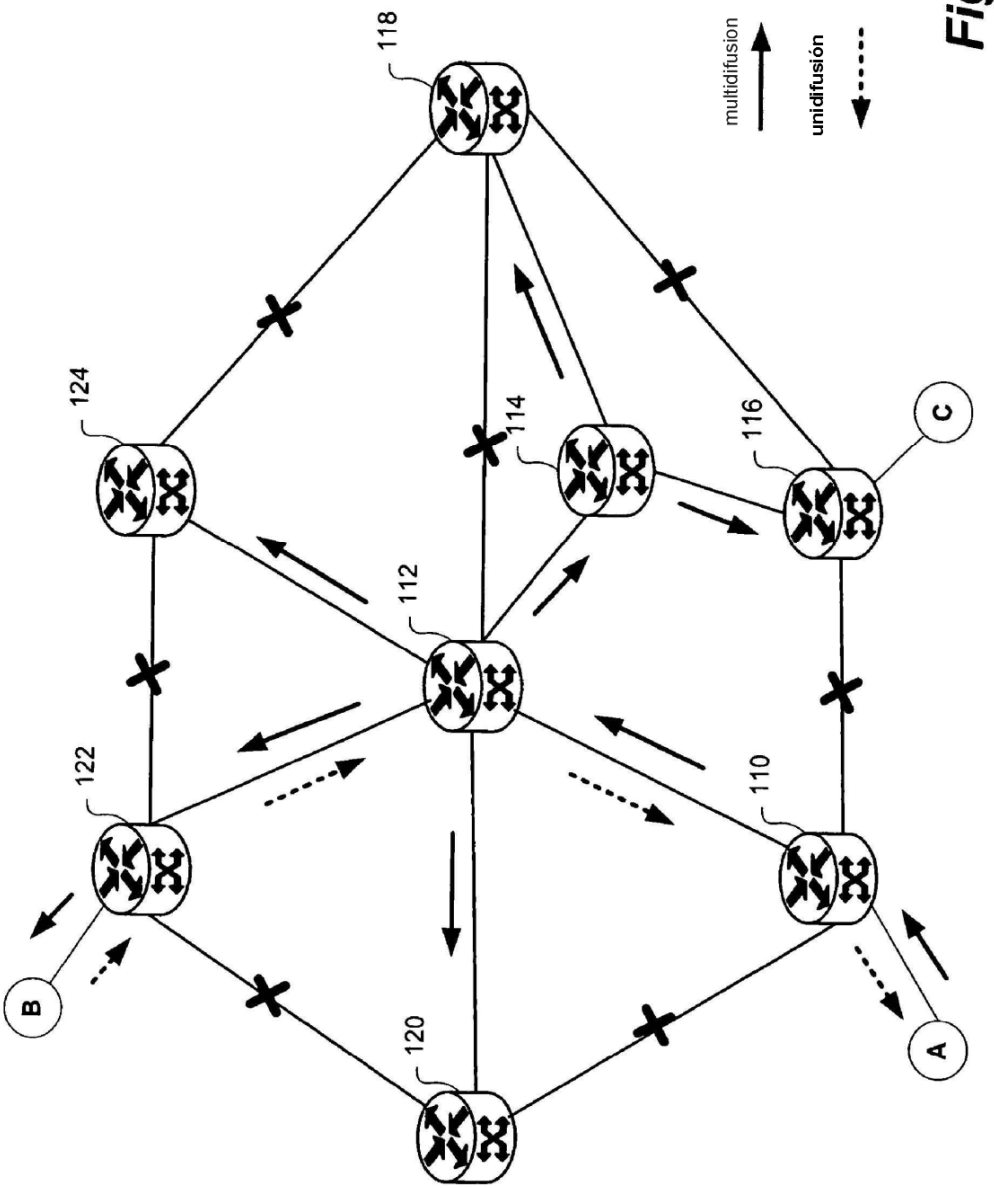
multidifusion
unidifusión
118
124
114
116
C
112
122
110
B
120
A

Fig. 1

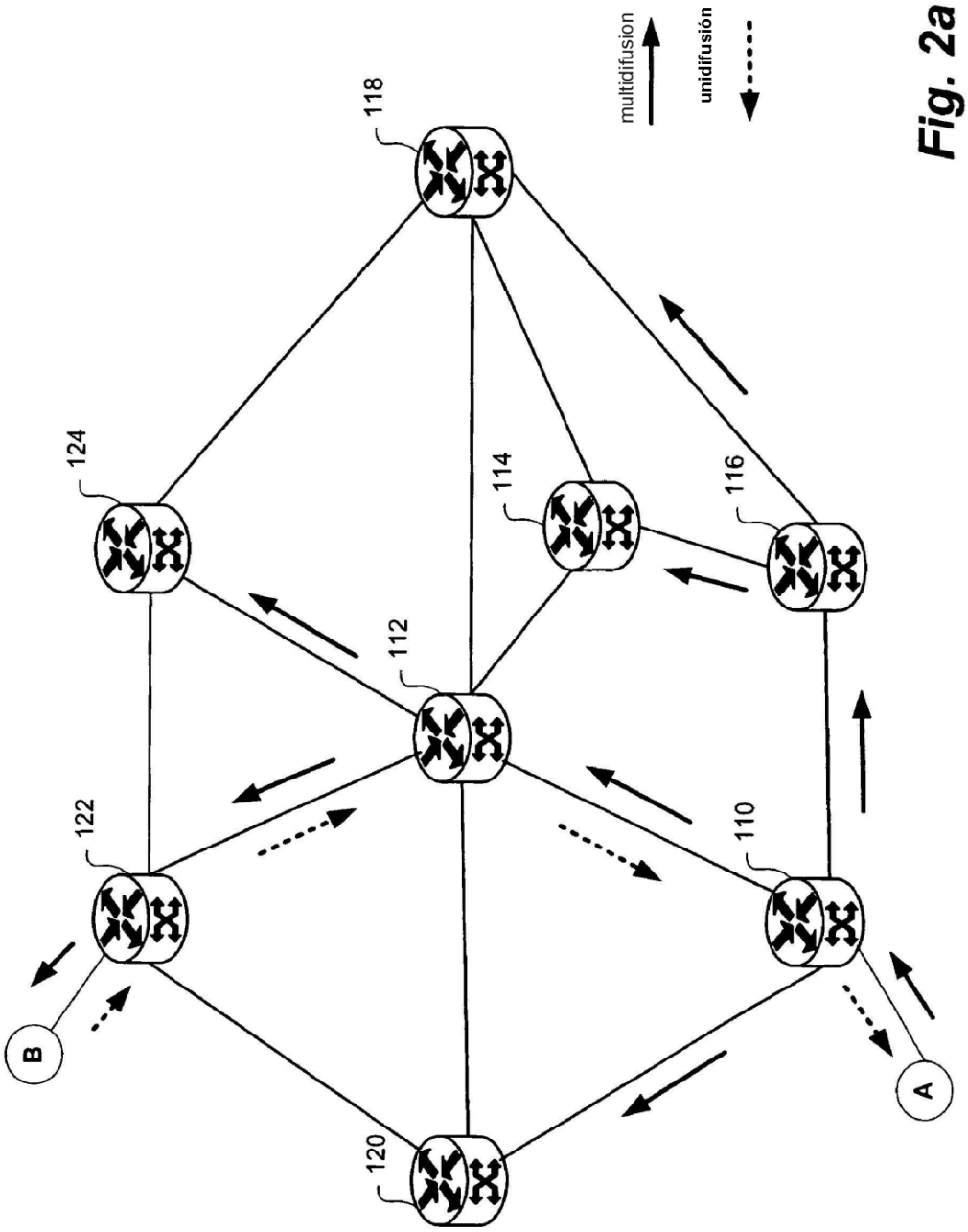
multidifusion
unidifusión
118
124
114
116
112
122
110
B
A
120

Fig. 2a

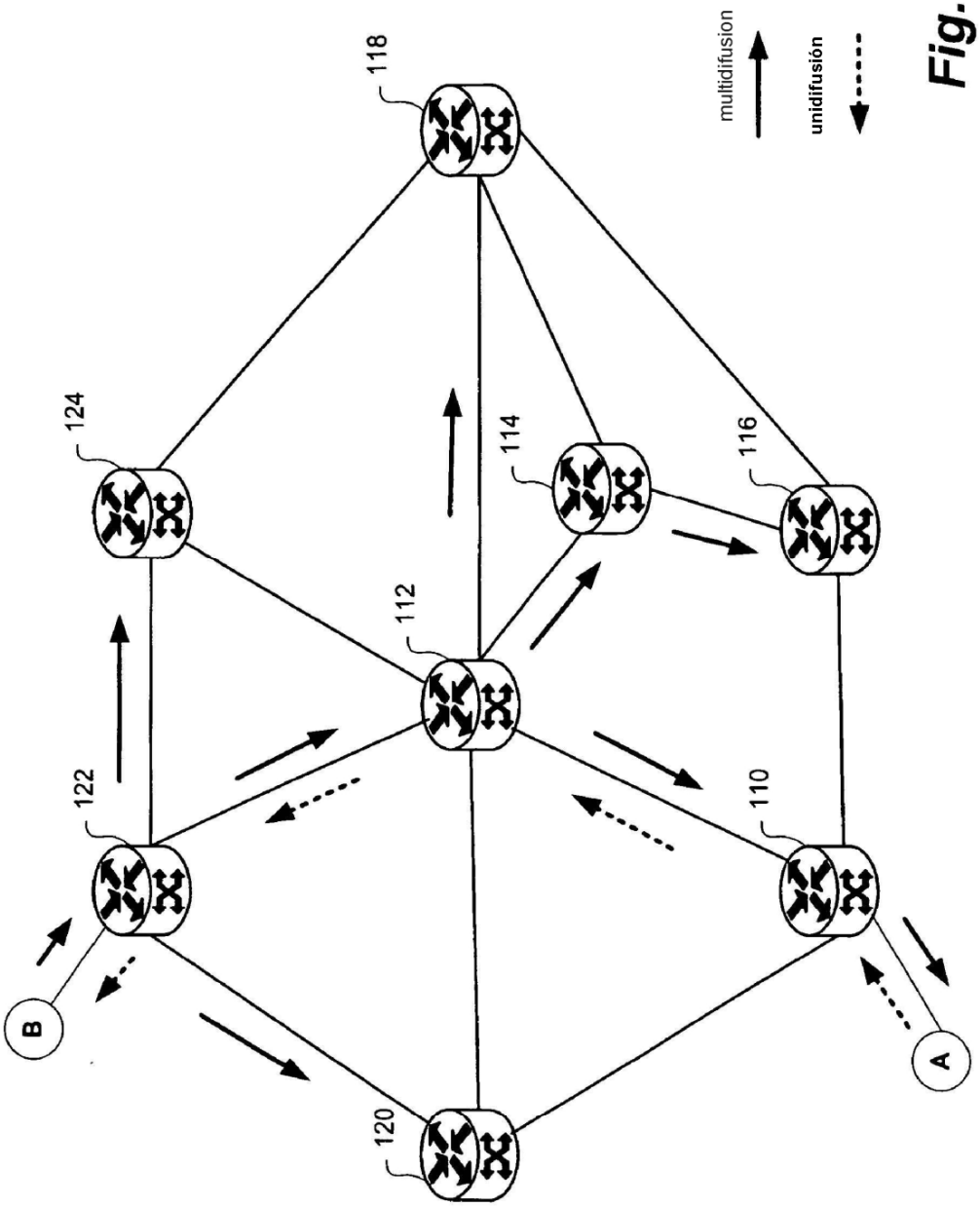
multidifusion
unidifusión
118
124
114
116
112
122
110
B
A
120

Fig. 2b

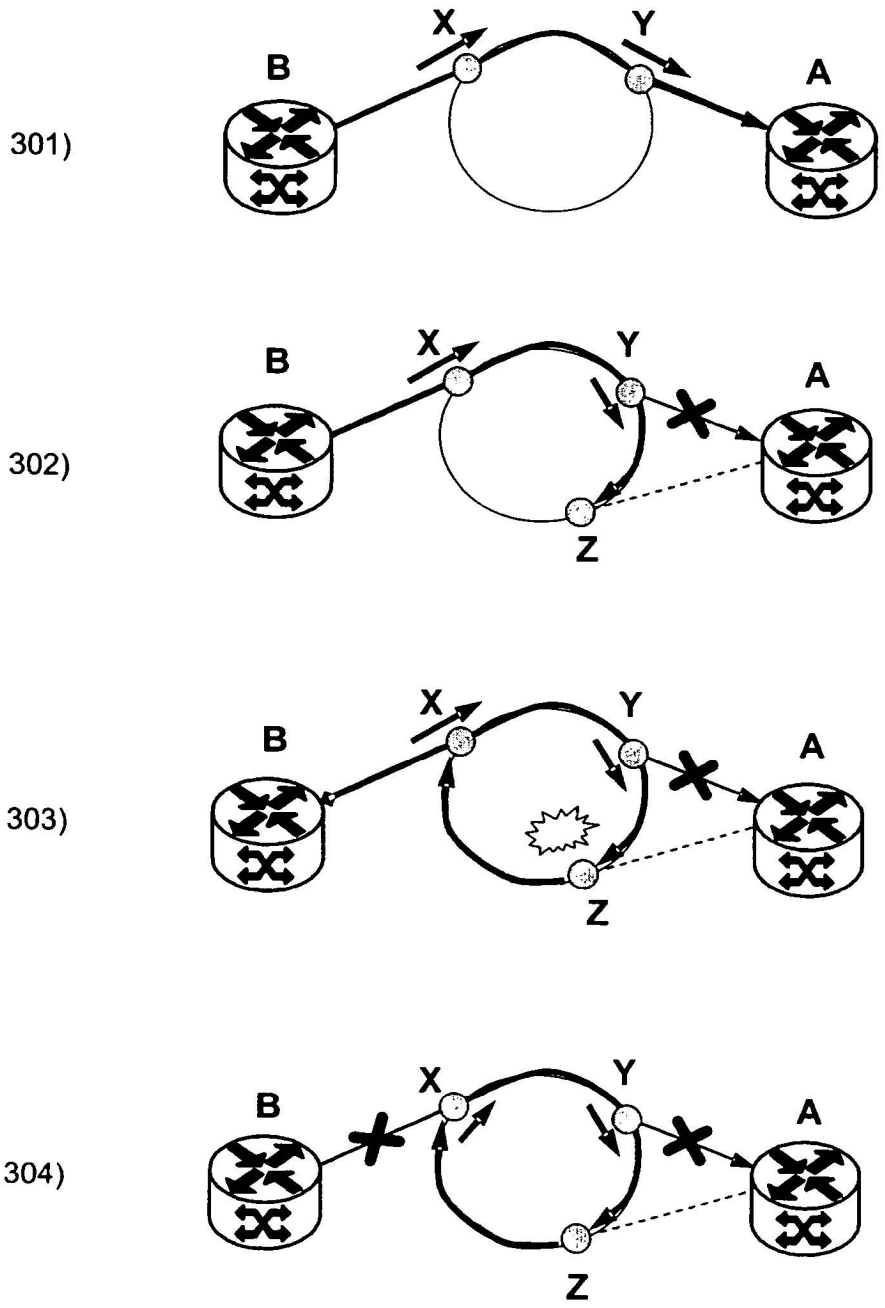

Fig. 3

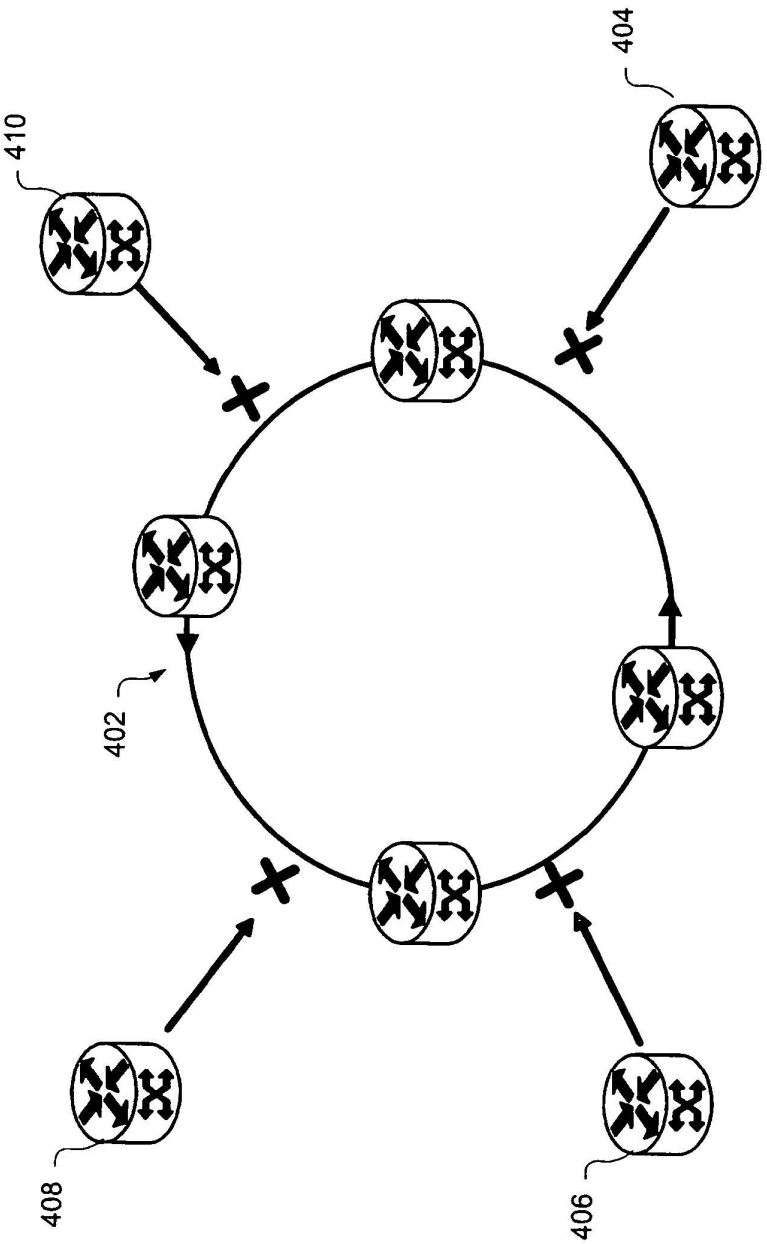

Fig. 4

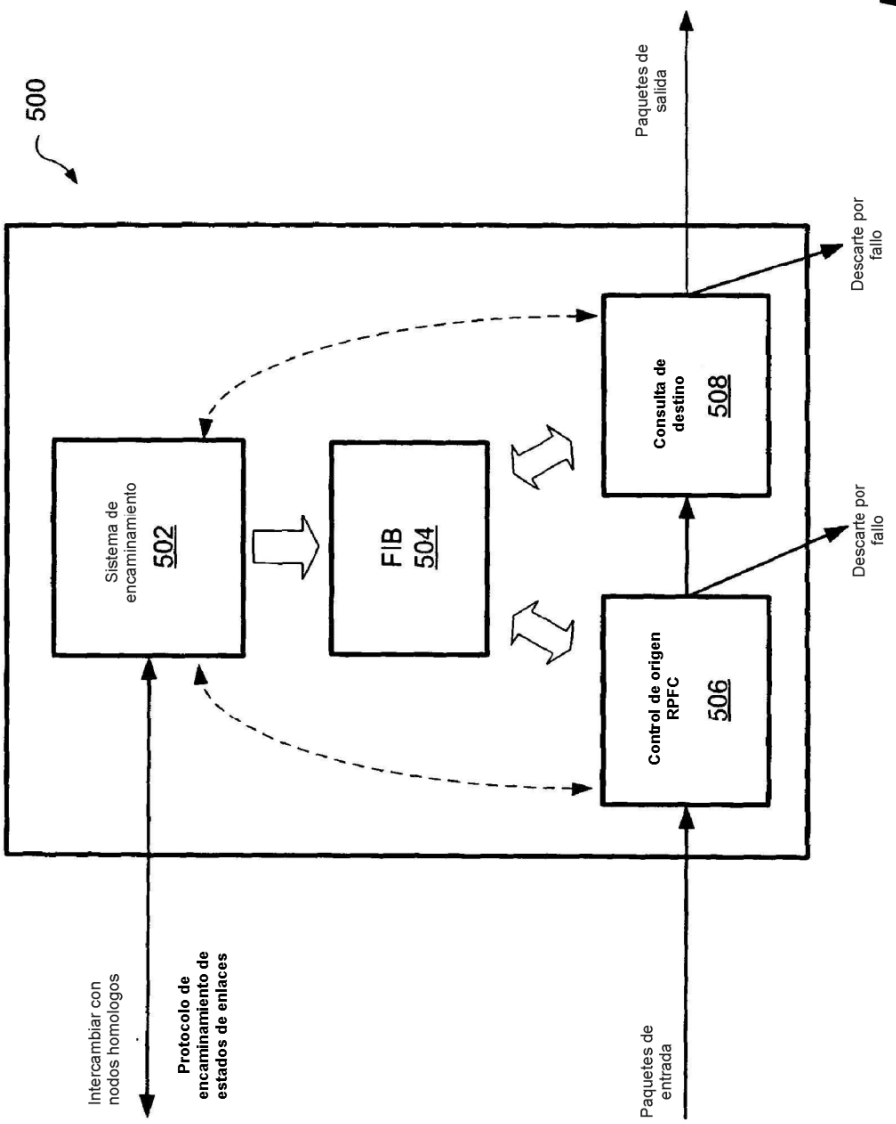
500
Paquetes de salida
Descarte por fallo
Consulta de destino
508
Sistema de encaminamiento
502
FIB
504
Descarte por fallo
Control de origen RPFC
506
Intercambiar con nodos homologos
Protocolo de encaminamiento de estados de enlaces
Paquetes de entrada

Fig. 5

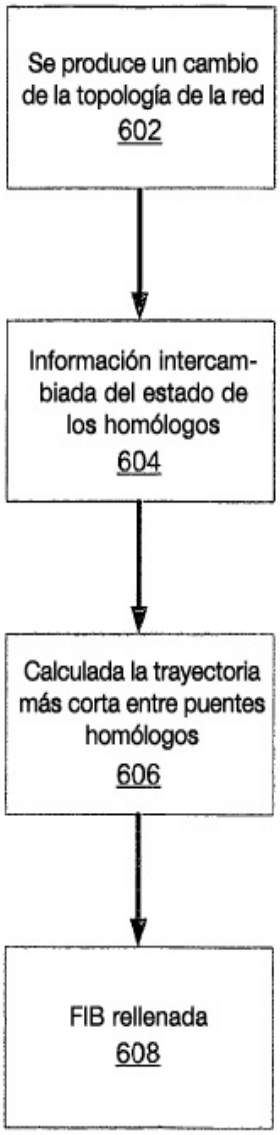
Se produce un cambio de la topología de la red
602
Información intercambiada del estado de los homólogos
604
Calculada la trayectoria más corta entre puentes homólogos
606
FIB rellenada
608

Fig. 6

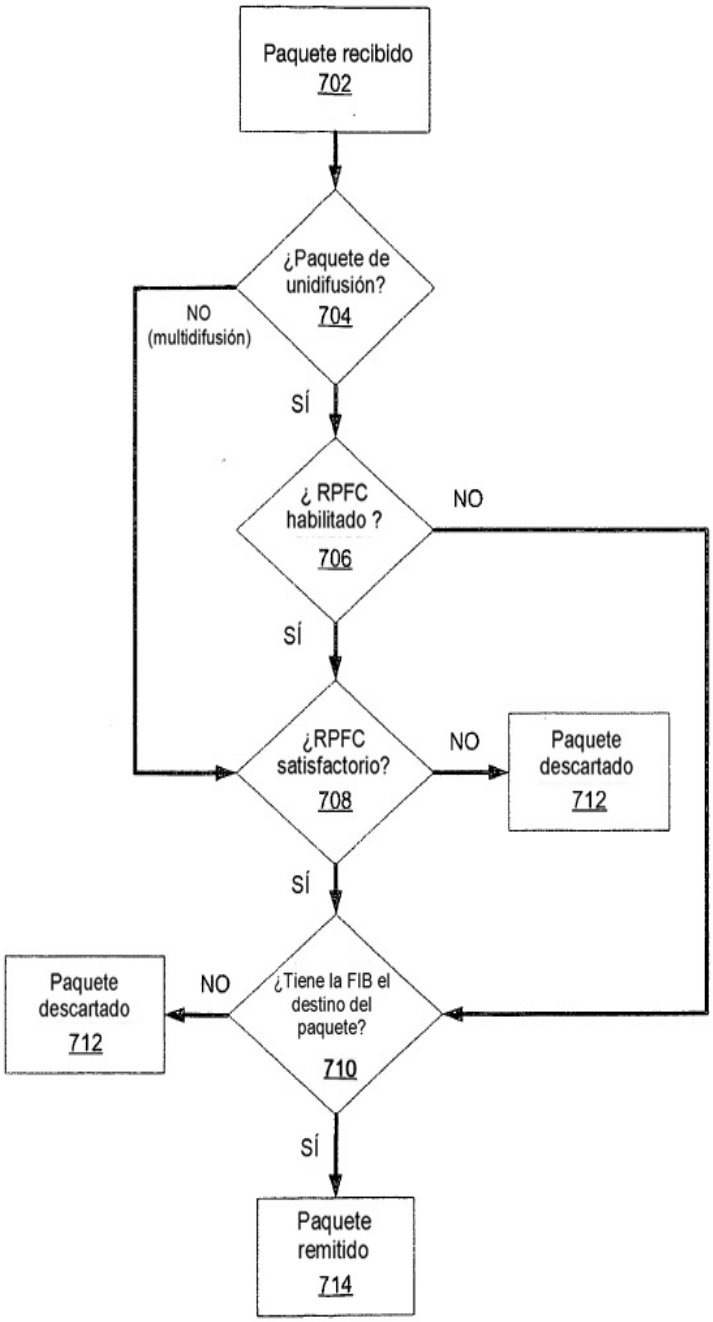
Paquete recibido
702
¿Paquete de unidifusión?
704
NO
(multidifusión)
SÍ
¿ RPFC habilitado ?
706
NO
SÍ
¿RPFC satisfactorio?
708
NO
Paquete descartado
712
SÍ
Paquete descartado
712
NO
¿Tiene la FIB el destino del paquete?
710
SÍ
Paquete remitido
714

Fig. 7

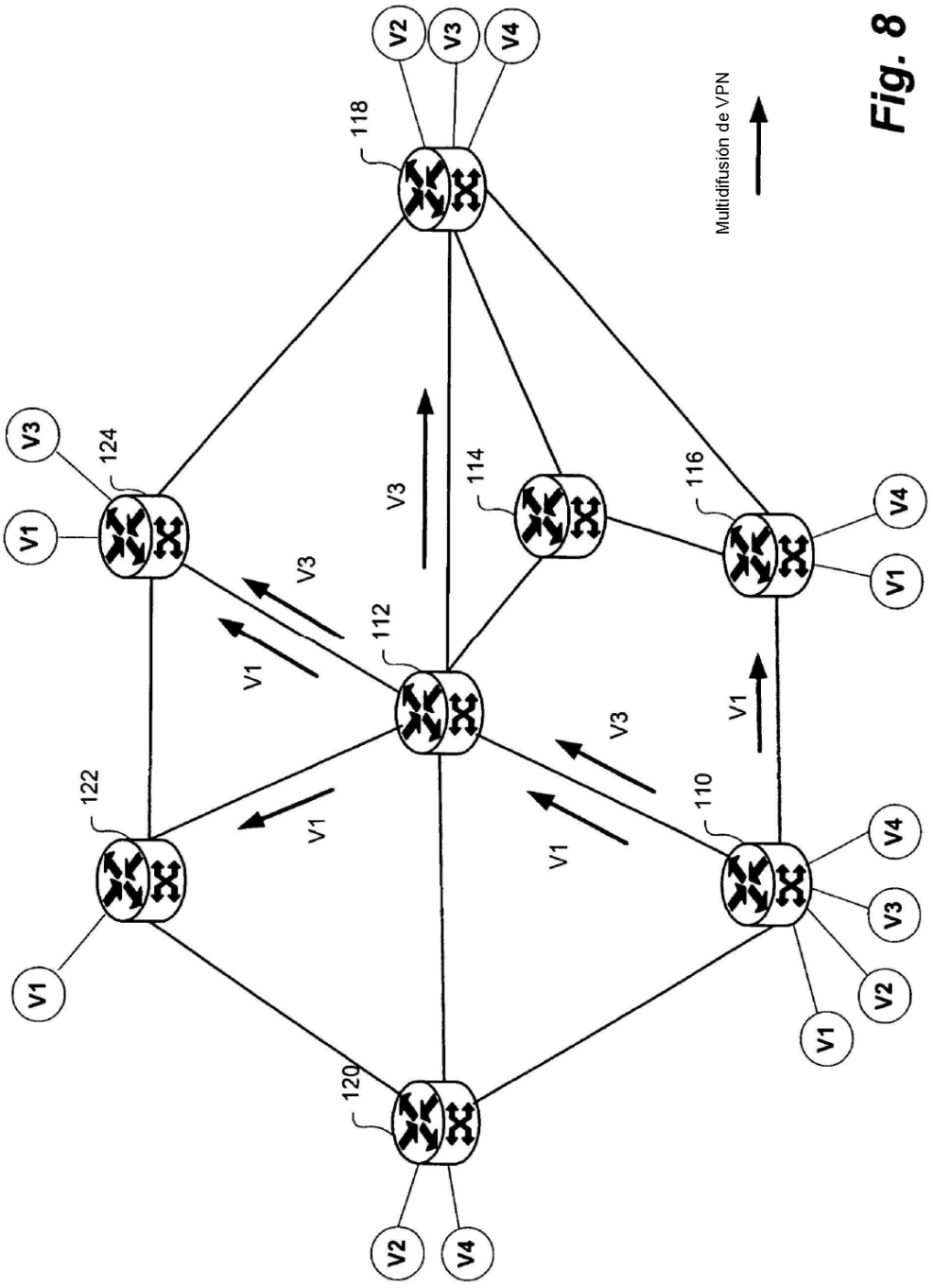
Multidifusión de VPN
118
V2
V3
V4
124
V3
V1
114
116
V4
V1
V3
V3
V1
112
V1
V3
V1
122
110
V1
V1
V4
V3
V2
V1
120
V2
V4

Fig. 8

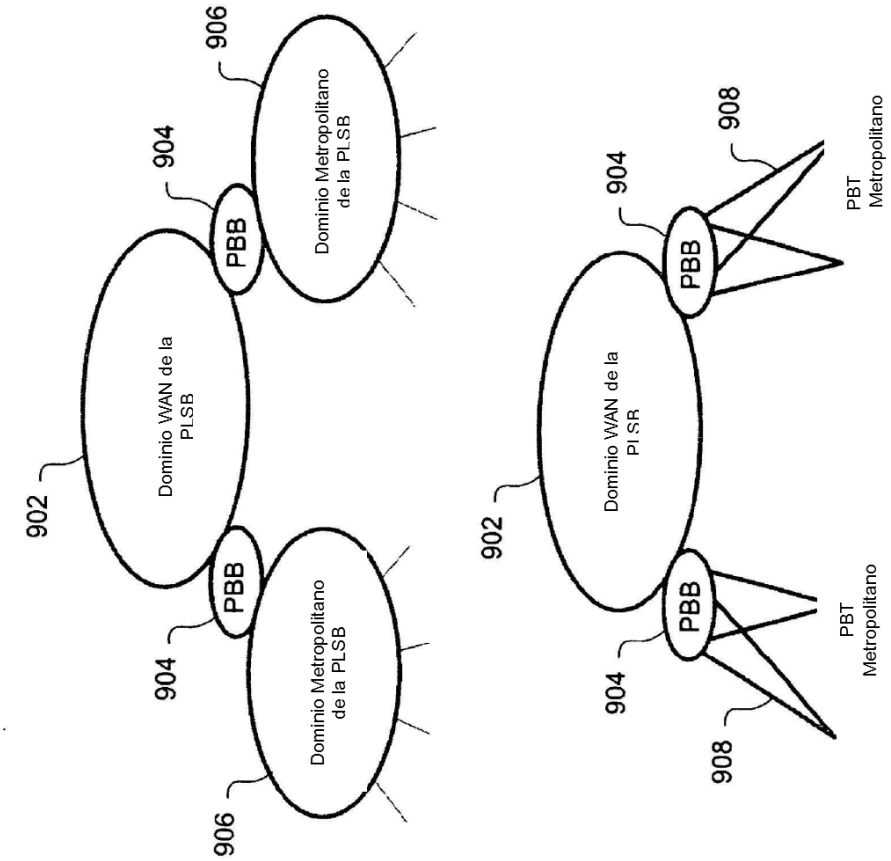
902
Dominio WAN de la PLSB
PBB
904
PBB
904
Dominio Metropolitano de la PLSB
906
Dominio Metropolitano de la PLSB
906
902
Dominio WAN de la PLSB
PBB
904
PBB
904
908
PBT Metropolitano
908
PBT Metropolitano

Fig. 9