(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 375 326**

(51) Int. CI.:
H04L 12/43 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08870940 .7**
(96) Fecha de presentación: **27.12.2008**
(97) Número de publicación de la solicitud: **2224644**
(97) Fecha de publicación de la solicitud: **01.09.2010**

(54) Título: **MÉTODO, SISTEMA Y DISPOSITIVO DE PROTECCIÓN EN UNA RED DE TRANSPORTE DE PAQUETES.**

(30) Prioridad:
29.12.2007 CN 200710033044

(45) Fecha de publicación de la mención BOPI:
28.02.2012

(45) Fecha de la publicación del folleto de la patente:
28.02.2012

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

(72) Inventor/es:
HE, Jia;
YANG, Yang;
ZHANG, Yongjun;
XIE, Wenjun;
HUANG, Shanguo y
GU, Wanyi

(74) Agente: **Lehmann Novo, Isabel**

DESCRIPCIÓN

Método, sistema y dispositivo de protección en una red de transporte de paquetes

Campo de la tecnología

La presente invención está relacionada con el campo de las tecnologías de las comunicaciones, y más en particular, con un método de protección que utiliza un anillo de protección compartida en una red de transporte de paquetes, un dispositivo nodal de una red de transporte de paquetes, y un sistema en una red de transporte de paquetes.

Antecedentes de la invención

Con objeto de mejorar la eficiencia y fiabilidad del transporte, una red de transporte utiliza usualmente una red en anillo. Tomando como ejemplo un anillo de protección compartida T-MPLS (TM-SPRing), se establece una relación lógica de adyacencia entre cada dos nodos de la red en anillo, y el establecimiento de la relación de conexión entre nodos correspondientes no está limitado por los dispositivos físicos y una topología de control de acceso al medio (MAC). La conexión entre los nodos vecinos recibe el nombre de tramo, y el tramo es una conexión bidireccional (pudiendo ser un tramo físico o una conexión lógica). Basándose en la tecnología T-MPLS (Transporte-Conmutación Multiprotocolo Basada en Etiquetas) se implementa una entidad de canal de transporte configurada para transportar flujos de datos de servicio entre los nodos del anillo mediante un grupo de LSP (Caminos Conmutados de Etiquetas). El TM-SPRing utiliza una estructura de doble anillo, y las direcciones de circulación de los flujos de datos de los servicios de los dos anillos son opuestas, los dos anillos constan de un anillo de trabajo (dirección de trabajo) y un anillo de protección (dirección opuesta a la dirección de trabajo), cada anillo puede establecer una pluralidad de LSP en función del volumen de la demanda de servicios, con el fin de asignar diferentes LSP a los diferentes flujos de datos de los servicios. La protección del TM-SPRing se aplica al tramo entre los nodos vecinos y se lleva a cabo mediante una función OAM (Operación, Administración y Mantenimiento) del tramo.

Cuando se produce un fallo en el tramo, para impedir que falle el tramo entre los nodos adyacentes es preciso confirmar un mecanismo de protección completo, con el fin de proteger rápidamente contra el fallo del tramo y transportar de forma correcta y efectiva el flujo de datos de servicio. En la actualidad, el mecanismo de protección habitual que utiliza el anillo de protección compartida dispone de dos mecanismos de conmutación, a saber, un mecanismo steering (dirección) y un mecanismo wrapping (cambio de dirección), y la principal diferencia entre el mecanismo steering y el mecanismo wrapping consiste en que, después de producirse el fallo del tramo, los nodos que inician la conmutación del flujo de datos de servicio son diferentes, donde, en el mecanismo steering, el nodo que inicia la conmutación del flujo de datos de servicio es un nodo de origen del flujo de datos de servicio, mientras en el mecanismo wrapping, el nodo que inicia la conmutación del flujo de datos de servicio es un nodo adyacente al tramo afectado por el fallo. El mecanismo wrapping se caracteriza por un tiempo corto de inicio de la conmutación y por una correspondiente tasa de pérdida de paquetes baja, pero un camino de protección wrapping conmutado no es un enrutamiento óptimo. Un camino de protección steering con mecanismo steering es el enrutamiento óptimo, pero el mecanismo steering se caracteriza por un tiempo largo de inicio de la conmutación y por una correspondiente tasa de pérdida de paquetes alta.

Una red de paquetes en anillo resistente a fallos (RPR) actual utiliza una solución de protección basada en una combinación del mecanismo wrapping y del mecanismo steering, y la implementación de la solución se lleva a cabo de acuerdo con los siguientes pasos.

En primer lugar, después de que haya ocurrido el fallo, un nodo adyacente al tramo afectado por el fallo lo detecta, y ejecuta inmediatamente la operación de conmutación de acuerdo con el mecanismo wrapping, de modo que un primer flujo de datos de servicio evita el tramo afectado por el fallo, esto es, el primer flujo de datos de servicio afectado (el flujo de datos de servicio que está a punto de pasar por el tramo afectado por el fallo en la dirección de trabajo) es redirigido al otro anillo para ser transportado, y, al mismo tiempo, el nodo adyacente al tramo afectado por el fallo envía en ambas direcciones un mensaje de solicitud de protección que contiene información del tramo afectado por el fallo.

A continuación, cuando reciben el mensaje de solicitud de protección, los nodos de origen y destino del flujo de datos de servicio llevan a cabo la operación de conmutación de acuerdo con el mecanismo steering, de tal modo que un segundo flujo de datos de servicio subsiguiente al primer flujo de datos de servicio es transferido al otro anillo para ser transportado, con el fin de evitar el tramo afectado por el fallo.

Un tiempo de inicio de la acción de conmutación en esta solución es igual al tiempo de inicio de la acción de conmutación de acuerdo con el mecanismo wrapping, y la razón es que la solución con protección wrapping se utiliza en primer lugar, por lo que la tasa de pérdida de paquetes del primer flujo de datos de servicio es baja. Además, después de llevarse a cabo la acción de conmutación de acuerdo con el mecanismo steering, el camino final recorrido por el segundo flujo de datos de servicio es el mismo que el camino de protección steering en el mecanismo steering, y es el enrutamiento óptimo en el otro anillo, mejorando de este modo la utilización de los recursos de la red, evitando la introducción de un tiempo de retardo innecesario, e integrando ventajas de las dos

soluciones constituidas por el mecanismo wrapping y el mecanismo steering.

En la técnica anterior han resultado evidentes los siguientes problemas.

De acuerdo con la descripción de los dos pasos anteriores, en la solución se cambia dos veces el camino del flujo de datos de servicio. La primera vez, el primer flujo de datos de servicio es conmutado del camino de trabajo al camino de protección wrapping para su transporte, y la segunda vez, el segundo flujo de datos de servicio es conmutado del camino de protección wrapping al camino de protección steering para su transporte. Comparado con el camino de protección steering, el camino de protección wrapping realiza la redirección del camino sobre el anillo de trabajo, por lo que es posible que el segundo flujo de datos de servicio enviado después del instante de la segunda conmutación alcance el nodo de destino antes que el primer flujo de datos de servicio enviado después del instante de la primera conmutación, lo que daría como resultado un problema de alteración de secuencia de los flujos de datos de servicio.

La técnica de transporte de paquetes tiene como finalidad implementar una plataforma portadora uniforme multiservicio, y necesita transportar un servicio TDM (Multiplexación por División de Tiempo), y el servicio TDM tiene unos requisitos estrictos en relación con la secuencia temporal.

El artículo "Analysis and improved performance of RPR protection" (presentado por Amund Kvalbein y otros en la 12ª Conferencia Internacional del IEEE del 16 al 19 de Noviembre de 2004) divulga un Resilient Packet Ring (Anillo de Paquetes Resistente a Fallos) (RPR, IEEE 802.17). En el artículo se simulan diferentes escenarios de error, con protecciones tanto steering como wrapping. Desafortunadamente, no siempre se puede garantizar la recuperación en 50 ms si se requiere que los paquetes se entreguen en orden, debido a que, para evitar la reordenación de los paquetes, el RPR utiliza un período de estabilización de la topología (por defecto 40 ms) muy largo. Se sugiere un mecanismo de protección que no exige esperar a que la nueva topología se estabilice, y proporciona una recuperación en 50 ms para todo el tráfico. Para la entrega en orden de los paquetes, el mecanismo de protección descarta un número muy pequeño de paquetes en comparación con el mecanismo del estándar RPR.

Resumen de la invención

La presente invención está dirigida a un método de protección en una red de transporte de paquetes, un dispositivo nodal de una red de transporte de paquetes, y un sistema en una red de transporte de paquetes capaces de resolver un problema de alteración de secuencia que se produce cuando en la red de transporte de paquetes se aplica una solución de protección basada en una combinación de un mecanismo wrapping y un mecanismo steering.

El problema técnico objetivo se resuelve mediante las reivindicaciones del método de las reivindicaciones 1 y 3 y sus reivindicaciones dependientes, mediante la reivindicación del dispositivo de la reivindicación 5 y sus reivindicaciones dependientes, y mediante la reivindicación del sistema de la reivindicación 8 y sus reivindicaciones dependientes.

En la presente invención, el primer flujo de datos de servicio se envía a través del camino de protección wrapping, y el nodo del flujo de datos de servicio suspende el envío al camino de protección wrapping del segundo flujo de datos de servicio subsiguiente al primer flujo de datos de servicio, y almacena temporalmente el segundo flujo de datos de servicio. Cuando el primer flujo de datos de servicio ha pasado completamente por segunda vez por el nodo del flujo de datos de servicio, se conmuta el segundo flujo de datos de servicio del camino de protección wrapping al camino de protección steering, resolviéndose de este modo el problema de alteración de secuencia que se produce cuando en la red de transporte de paquetes se aplica la solución de protección basada en la combinación del mecanismo wrapping y del mecanismo steering, con el fin de perfeccionar el mecanismo de protección del sistema en la red de transporte de paquetes, y mejorar la capacidad del sistema para protegerse frente a fallos.

Breve descripción de los dibujos

Con objeto de ilustrar más claramente las soluciones técnicas conformes con los modos de realización de la presente invención o de la técnica anterior, a continuación se citan brevemente las figuras adjuntas para describir los modos de realización o la técnica anterior. En apariencia, en la siguiente descripción los dibujos adjuntos son sólo algunos de los modos de realización de la presente invención.

La FIG. 1 es un diagrama de flujo esquemático de un método de protección en una red de transporte de paquetes de acuerdo con un modo de realización de la presente invención;

La FIG. 2 es una vista esquemática de un formato de trama de información de conmutación de protección automática (APS);

La FIG. 3 es una vista esquemática de una descripción del contenido de una solicitud de protección en la información de APS;

La FIG. 4 es una vista esquemática de una operación de conmutación wrapping en el paso 404 de acuerdo con un modo de realización de la presente invención;

La FIG. 5 es una vista esquemática de una operación en la que un nodo de origen es conmutado a un camino de protección steering en el paso 409 de acuerdo con un modo de realización de la presente invención;

La FIG. 6 es una vista esquemática de una operación en la que un nodo de origen y un nodo de destino son conmutados a un camino de protección steering de acuerdo con un modo de realización de la presente invención;

La FIG. 7 es una vista esquemática de otro método de protección en una red de transporte de paquetes de acuerdo con un modo de realización de la presente invención;

La FIG. 8 es una vista esquemática de la estructura de un dispositivo nodal de origen/dispositivo nodal de destino de acuerdo con un modo de realización de la presente invención; y

La FIG. 9 es una vista esquemática de la estructura de un sistema en una red de transporte de paquetes de acuerdo con un modo de realización de la presente invención.

Descripción detallada de los modos de realización

La presente invención proporciona un método de protección en una red de transporte de paquetes, un dispositivo nodal en una red de transporte de paquetes, y un sistema en una red de transporte de paquetes capaces de resolver un problema de alteración de secuencia que ocurre cuando en la red de transporte de paquetes se aplica una solución de protección basada en una combinación de un mecanismo wrapping y un mecanismo steering.

En lo que sigue, se describen de forma detallada el método, el dispositivo y el sistema de acuerdo con los modos de realización de la presente invención, haciendo referencia a los dibujos que la acompañan.

La FIG. 1 es un diagrama de flujo esquemático de un método de protección en una red de transporte de paquetes de acuerdo con un modo de realización de la presente invención. En el método, tomando como ejemplo un TM-SPRing, se completa una conmutación de un mecanismo wrapping a un mecanismo steering. Además, la presente invención se puede aplicar, aunque no se limita, a una red en anillo según el estándar Provider Backbone Bridging – Traffic Engineering (Puente de Red Troncal de Proveedor - Ingeniería de Tráfico) (PBB-TE), y otros sistemas en la red de transporte de paquetes. En referencia a la FIG. 1, el método consta fundamentalmente de los siguientes pasos.

En el paso 401, se produce un fallo en un tramo determinado del anillo TM-SPRing, y se aplica la protección del TM-SPRing al fallo del tramo entre nodos adyacentes.

En el paso 402, un nodo adyacente al tramo afectado por el fallo detecta el fallo del tramo, y cada uno de los nodos del TM-SPRing monitoriza información sobre la red en anillo e identifica a tiempo el tramo afectado por el fallo en la red en anillo. El fallo del tramo puede ser de dos tipos: uno es fallo en la señal del tramo (SF), en cuyo SF el flujo de datos de servicio no puede ser transportado en el tramo afectado por el fallo, el nodo adyacente al tramo afectado por el fallo en el sentido de avance de una dirección de trabajo no puede recibir el flujo de datos de servicio y el SF se puede detectar mediante una función de comprobación de interconexión de un paquete OAM; el otro es degradación de la señal del tramo (SD), en cuyo SD el flujo de datos de servicio puede ser transportado en el tramo afectado por el fallo, pero la calidad del flujo de datos de servicio recibido por el nodo adyacente al tramo afectado por el fallo en el sentido de avance de la dirección de trabajo es mala, la SD se puede detectar mediante pérdida de paquetes, retardo y otras funciones del paquete OAM, cada uno de los nodos de la red en anillo identifica si el tramo adyacente al nodo funciona normalmente o sufre el fallo monitorizando los paquetes OAM que pasan a través del nodo, y cuando se detecta el fallo del tramo se ejecuta el paso 403.

En las aplicaciones prácticas es necesario ilustrar los dos puntos siguientes.

En primer lugar, el fallo del tramo se divide en fallo de un solo anillo y fallo de los dos anillos. En un modo de realización de la presente invención los dos tipos de fallo son procesados por el nodo relacionado de acuerdo con el mismo mecanismo en términos de operación de conmutación. En la descripción del modo de realización de la presente invención se toma como ejemplo el fallo en los dos anillos, aunque sigue siendo aplicable el contenido de la presente invención en el fallo en un solo anillo.

En segundo lugar los flujos de datos de servicio transportados sobre el anillo de protección compartida en la red de transporte de paquetes son servicios bidireccionales, y en el fallo de los dos anillos se ven afectados los flujos de datos de servicio en las dos direcciones. El flujo de datos de servicio afectado por el fallo en una dirección es conmutado y el flujo de datos de servicio en la otra dirección también es conmutado. En el modo de realización de la presente invención, los procedimientos para el proceso en ambas direcciones son sustancialmente consistentes. Por simplicidad de la descripción, en la ilustración del modo de realización de la presente invención se describe cómo proteger el flujo de datos de servicio en una dirección, aunque la presente invención también es aplicable al procedimiento para el proceso en la otra dirección.

En el paso 403, el nodo adyacente al tramo afectado por el fallo envía un mensaje de solicitud de protección (posiblemente de forma bidireccional). El mensaje de solicitud de protección tiene la forma de información APS, con

el fin de notificar a cada uno de los nodos del TM-SPRing la información sobre el tramo afectado por el fallo, y comunicarse con otro nodo adyacente al tramo afectado por el fallo, completando de este modo la conmutación de acuerdo con el mecanismo wrapping. Un formato de trama de la información APS es como el que se muestra en la FIG. 2, y la información APS comprende un campo de encabezamiento de etiqueta, un campo de tipo de función y una PDU (Unidad de Datos de Protocolo) APS. Una descripción del contenido de la solicitud de protección comprende la ID de un nodo de origen configurada para identificar e indicar un nodo de origen, la ID de un nodo de destino configurada para identificar e indicar un nodo de destino, información de solicitud/estado del puente, y algunos bytes reservados. En el modo de realización de la presente invención, la función de identificación de la presente invención se puede completar utilizando una función de ampliación de un 8º bit de los bytes reservados de la información APS; como se muestra en la FIG. 3, al bit se le asigna el valor 1 (el valor del bit de la información APS antes de la función de ampliación es 0), de modo que la información APS desempeñe la función de indicar que se suspenda el envío del flujo de datos de servicio.

En el paso 404, el nodo adyacente al tramo afectado por el fallo completa la conmutación de la protección wrapping, concretamente mediante la conmutación del flujo de datos de servicio que está siendo transmitido de un LSP de trabajo a un LSP de protección. El TM-SPRing hereda un método de transporte de datos de un MPLS, cada camino de servicio corresponde a un LSP, y a cada tramo se le asigna una etiqueta en el LSP para transportar correctamente el flujo de datos de servicio. El TM-SPRing completa la conmutación operando con las etiquetas del flujo de datos de servicio, cada nodo del TM-SPRing almacena en una base de datos las etiquetas del LSP de trabajo y el LSP de protección de cada flujo de datos de servicio del nodo, y la etiqueta del LSP de trabajo y la etiqueta del LSP de protección de cada flujo de datos de servicio de cada nodo se corresponden entre sí, conmutándose correctamente de este modo el flujo de datos de servicio.

Cada nodo del TM-SPRing es adyacente a dos tramos, y tomando como referencia una dirección de avance de un camino del flujo de datos de servicio, una etiqueta del tramo entre dicho nodo y el nodo adyacente anterior según el sentido de avance del flujo de datos de servicio se denomina etiqueta ascendente del nodo, y una etiqueta del tramo entre dicho nodo y el nodo adyacente posterior según el sentido de avance del flujo de datos de servicio se denomina etiqueta descendente del nodo.

Entre los nodos adyacentes al fallo se puede realizar una operación para establecer un puente, y mientras el puente esté establecido es necesario operar con la etiquetas del flujo de datos de servicio, y la operación consta, específicamente, de los siguientes pasos.

Para el nodo adyacente al tramo afectado por el fallo en el sentido ascendente a la dirección de trabajo, la etiqueta del tramo adyacente en el sentido ascendente del LSP de trabajo del nodo se reemplaza por la etiqueta del tramo adyacente en el sentido descendente del LSP de protección del nodo, y el flujo de datos de servicio se reenvía utilizando la etiqueta del tramo adyacente en el sentido descendente del LSP de protección del nodo, de modo que, para ser transportado, el flujo de datos de servicio transmitido se conmuta del LSP de trabajo al LSP de protección.

Para el nodo adyacente al tramo afectado por el fallo en el sentido descendente de la dirección de trabajo, la etiqueta del tramo adyacente en el sentido ascendente del LSP de protección del nodo se reemplaza por la etiqueta del tramo adyacente en el sentido descendente del LSP de trabajo del nodo, y el flujo de datos de servicio se reenvía utilizando la etiqueta del tramo adyacente en el sentido descendente del LSP de trabajo del nodo.

La etiqueta se asigna y se sustituye utilizando un mecanismo Mirror (Espejo), de modo que las etiquetas de la parte de superposición del LSP de trabajo y del LSP de protección pueden utilizar el mismo valor, y cuando se reemplaza la etiqueta del nodo adyacente al fallo, el valor de la etiqueta no cambia. A continuación se describen los pasos de la operación de asignación de la etiqueta según el mecanismo Mirror en las implementaciones específicas.

En el paso A1, la operación se basa en una cierta dirección de un camino del flujo de datos de servicio bidireccional, por ejemplo, una dirección de trabajo en el sentido de las agujas del reloj, y de acuerdo con un algoritmo del camino más corto, se determina un camino de trabajo más corto para el flujo de datos de servicio entre el nodo de origen y el nodo de destino sobre el anillo del TM-SPRing en el sentido de las agujas del reloj, y el camino de trabajo más corto sirve como LSP de trabajo (asumiendo la dirección de trabajo).

En el paso A2 se determina el camino de protección más corto sobre el anillo del TM-SPRing en el sentido contrario al de las agujas del reloj, y el camino de protección más corto sirve como LSP de protección (asumiendo una dirección contraria a la dirección de trabajo, esto es, la dirección de protección) del LSP de trabajo.

En el paso A3, se asigna la etiqueta a cada uno de los tramos del LSP de trabajo y del LSP de protección. Para simplificar la operación, la etiqueta de trabajo y la etiqueta de protección del flujo de datos de servicio en el tramo de superposición del LSP de trabajo y el LSP de protección pueden adoptar el mismo valor. En el modo de realización de la presente invención, las etiquetas de cada uno de los tramos que corresponden al camino de protección wrapping y al camino de protección steering utilizadas respectivamente por el mecanismo wrapping y el mecanismo steering son habitualmente las mismas. Ciertamente, en las implementaciones específicas se pueden asignar etiquetas diferentes. Además, las etiquetas se pueden asignar manualmente o pueden ser asignadas

dinámicamente por el sistema.

Adicionalmente, en el modo de realización de la presente invención, el mecanismo para asignar y reemplazar las etiquetas en la red de transporte de paquetes puede ser un mecanismo Mirror, un mecanismo de asignación único, un mecanismo Tunnel (Túnel), un mecanismo estándar de asignación de etiquetas y otros mecanismos de asignación de etiquetas de la técnica anterior.

En relación con la FIG. 4, en el paso 404, por ejemplo, el flujo de datos de servicio desde un Nodo1 (nodo de origen) a un Nodo4 (nodo de destino) encuentra un fallo entre un Nodo2 y un Nodo3, el Nodo2 reemplaza una etiqueta 20 de la dirección de trabajo por una etiqueta 20 del LSP de protección, y reenvía el flujo de datos de servicio utilizando la etiqueta 20 del LSP de protección con el fin de conmutar el flujo de datos de servicio al LSP de protección para ser transportado; y el Nodo3 reemplaza una etiqueta 40 de la dirección de protección por una etiqueta 40 del LSP de trabajo y conmuta el flujo de datos de servicio al LSP de trabajo para ser transportado.

En el paso 405, después de recibir la información de la solicitud de protección, cada uno de los otros nodos del anillo, excepto los nodos adyacentes al fallo, extrae de la información de la solicitud de protección la información de ID del nodo de origen y la información de ID del nodo de destino, obtiene información de la posición del tramo afectado por el fallo, e identifica una relación entre el nodo del anillo y el flujo de datos de servicio afectado por el tramo en el que se ha producido el fallo; si el nodo es un nodo intermedio (no es el nodo de origen ni el de destino) del flujo de datos de servicio afectado por el tramo en el que se ha producido el fallo, el procedimiento continúa en el paso 406.

Si el nodo es el nodo de origen/nodo de destino del flujo de datos de servicio afectado por el tramo en el que se ha producido el fallo, el procedimiento continúa en el paso 407.

Por un tramo puede pasar una pluralidad de flujos de datos de servicio, y en general el tramo en el que se ha producido el fallo puede afectar a una pluralidad de flujos de datos de servicio. Por ejemplo, el nodo del TM-SPRing puede tener diferentes relaciones con diferentes flujos de datos de servicio afectados por el tramo en el que se ha producido el fallo: el nodo del TM-SPRing puede ser el nodo intermedio del flujo 1 de datos de servicio afectado por el tramo en el que se ha producido el fallo, y también puede ser el nodo de origen del flujo 2 de datos de servicio afectado por el tramo en el que se ha producido el fallo. En las implementaciones específicas, la operación de protección se realiza basándose en un camino del flujo de datos de servicio, y durante el proceso de protección del flujo de datos de servicio se confirma la relación entre cada uno de los nodos del anillo y el flujo de datos de servicio.

En el paso 406, si el nodo actual no es un nodo adyacente al tramo afectado por el fallo ni el nodo de origen o el nodo de destino del flujo de datos de servicio afectado por el tramo en el que se ha producido el fallo, al nodo siguiente en el sentido de avance se le envía únicamente la información de la solicitud de protección.

Si, de acuerdo con la información de la solicitud de protección, se determina que el nodo no es el nodo adyacente al tramo afectado por el fallo, y se detecta que la calidad del flujo de datos de servicio recibido por el nodo es mala o no es posible recibir el flujo de datos de servicio, el nodo no genera la información de la solicitud de protección, evitando de este modo que la información de la solicitud de protección se genere una y otra vez.

En el paso 407, si el nodo es el nodo de origen/nodo de destino del flujo de datos de servicio afectado por el tramo en el que se ha producido el fallo, el nodo de origen/nodo de destino realiza las siguientes operaciones.

El nodo de origen/nodo de destino envía un primer flujo de datos de servicio a través de un camino de protección wrapping; aquí, el TM-SPRing tiene un camino de protección establecido para proteger el flujo de datos de servicio, y el camino de protección comprende un camino de protección wrapping y un camino de protección steering.

Tras recibir el mensaje de solicitud de protección, el nodo de origen/nodo de destino envía el mensaje de solicitud de protección a un nodo posterior en el sentido de avance.

Después de recibir el mensaje de solicitud de protección, el nodo de origen/nodo de destino suspende el envío de un segundo flujo de datos de servicio (que puede ser un flujo de datos de entrada al anillo) subsiguiente al primer flujo de datos de servicio a través del camino de protección wrapping, y almacena temporalmente el segundo flujo de datos de servicio en un buffer (memoria de almacenamiento temporal). Concretamente, el segundo flujo de datos de servicio puede ser almacenado temporalmente en un buffer de retorno del nodo de origen/nodo de destino, donde el segundo flujo de datos de servicio sirve como flujo de datos de servicio subsiguiente al primer flujo de datos de servicio enviado al camino de protección wrapping antes del instante en el que el nodo de origen suspendió el envío. El TM-SPRing dispone para todos los nodos del anillo de dos Buffers unidireccionales dinámicos: un Buffer de envío y un Buffer de retorno, donde la dirección de trabajo recibe el nombre de dirección de avance y la dirección de protección (dirección opuesta a la del LSP de trabajo) recibe el nombre de dirección de retorno, y el Buffer dinámico quiere decir que se dispone un contador en la entrada del Buffer, de modo que durante el proceso de conmutación se devuelve una longitud efectiva del flujo de datos de servicio, lo que permite ajustar el pointer (puntero), implementándose de este modo la asignación dinámica del Buffer.

En el dispositivo del nodo de origen/nodo de destino, la función de recibir el mensaje de solicitud de protección se puede implementar mediante una unidad de recepción.

En el dispositivo del nodo de origen/nodo de destino, la función de suspender el envío del segundo flujo de datos de servicio a través del camino de protección wrapping se puede implementar mediante una unidad de retención. Después de que la unidad de recepción reciba el mensaje de solicitud de protección, la unidad de retención suspende el envío del segundo flujo de datos de servicio a través del camino de protección wrapping.

En el dispositivo del nodo de origen/nodo de destino, el segundo flujo de datos de servicio es almacenado temporalmente en el buffer, y el buffer es una unidad de almacenamiento temporal que desempeña la función de almacenamiento temporal en el dispositivo del nodo de origen/nodo de destino.

El nodo de origen/nodo de destino añade un identificador a continuación de la última trama del primer flujo de datos de servicio: concretamente, amplía la función del mensaje de solicitud de protección recibido (información APS), cambia a 1 el valor del 8º bit de los bytes reservados de la información APS (el valor original es 0), y añade la información APS ampliada como identificador a continuación de la última trama del primer flujo de datos de servicio enviado a través del camino de protección wrapping.

En el dispositivo del nodo de origen/nodo de destino, la función de adjuntar el identificador a continuación de la última trama del primer flujo de datos de servicio se completa mediante una unidad de anexión de identificador en una unidad de detección del dispositivo del nodo de origen/nodo de destino.

Se debe observar que la información APS que tiene la función de indicar que se suspenda el envío del segundo flujo de datos de servicio y la información APS (mensaje de solicitud de protección) que contiene la información del fallo que ha sido recibida inicialmente por el nodo de origen/nodo de destino se diferencian únicamente en el valor de sus respectivos 8º bits de los bytes reservados, y los datos en las demás posiciones son idénticos. Después de recibir la información APS no ampliada que contiene la información del fallo, el nodo de origen amplía la función de la información APS adjuntándole el identificador a través de la operación de ampliación de función, y el nodo de origen/nodo de destino continúa enviando la información APS no ampliada al nodo siguiente en el sentido de avance.

Adicionalmente, en el modo de realización de la presente invención, la función de la información APS se amplía, la función de indicar que se suspenda el envío del flujo de datos de servicio se añade a la información APS, pero las funciones inherentes no cambian, y otras operaciones relacionadas con la información APS tampoco cambian. Se debe observar que la función de indicación es una ampliación de la función OAM, la cual no se limita a utilizar la información APS, se pueden utilizar otras funciones OAM, o se puede ampliar otro paquete de mensaje.

En el paso 408, el nodo de origen/nodo de destino monitoriza la información del TM-SPRing y determina si se ha recibido el identificador. El primer flujo de datos de servicio transportado a través del camino de protección wrapping puede pasar por segunda vez por el nodo de origen/nodo de destino, de modo que el nodo de origen/nodo de destino recibe necesariamente el identificador enviado previamente por el nodo de origen. Cuando se recibe el identificador, el procedimiento continúa en el paso 409, y en caso contrario se repite el paso 408.

En el dispositivo del nodo de origen/nodo de destino, la función de determinar si se ha recibido el identificador se puede completar mediante una unidad de determinación en la unidad de detección del dispositivo del nodo de origen/nodo de destino.

En el paso 409, el nodo de origen/nodo de destino elimina el identificador, conmuta el camino de protección wrapping al camino de protección steering, y envía el segundo flujo de datos de servicio almacenado temporalmente. Concretamente, el nodo de origen/nodo de destino conmuta el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering, y envía el segundo flujo de datos de servicio almacenado temporalmente en dirección opuesta a través del Buffer de retorno. Aquí, el nodo de origen/nodo de destino transporta el segundo flujo de datos de servicio almacenado temporalmente a través del camino de protección steering. Durante la operación de conmutación, la etiqueta del tramo adyacente siguiente del LSP de trabajo del nodo de origen/nodo de destino se debe reemplazar por la etiqueta del tramo adyacente siguiente del LSP de protección del nodo de origen/nodo de destino, y se reenvía el segundo flujo de datos de servicio utilizando la etiqueta del tramo del LSP de protección.

En el dispositivo del nodo de origen/nodo de destino, la función de conmutación del camino de protección wrapping al camino de protección steering y envío del segundo flujo de datos de servicio almacenado temporalmente se implementa mediante una unidad de proceso de detección del dispositivo del nodo de origen/nodo de destino.

La implementación conjunta del paso 407, el paso 408 y el paso 409, asegura que cuando el nodo de origen/nodo de destino procesa la conmutación, el flujo de datos de servicio enviado en primer lugar llega antes, y de este modo no se produce el problema de alteración de secuencia de los flujos de datos de servicio.

Como se muestra en la FIG. 5, por ejemplo, el fallo se produce en el tramo entre el Nodo2 y el Nodo3, y el proceso de conmutación del nodo de origen y el camino para el transporte del flujo de datos de servicio en el modo de realización de la presente invención se describen del siguiente modo.

En B1, para el camino de transporte del primer flujo de datos de servicio sobre el camino de protección wrapping:

El primer flujo de datos de servicio se envía desde el nodo de origen Nodo1 y llega al nodo de destino Nodo4 a través del camino

Nodo1→Nodo2→Nodo1→Nodo6→Nodo5→Nodo4→Nodo3→Nodo4

En B2, para un proceso de tratamiento específico:

En primer lugar, el Nodo1 recibe el identificador enviado por el Nodo3, cambia a 1 el valor del 8º bit de los bytes reservados de la información APS, y construye el identificador que tiene la función de indicar que se suspenda el envío del flujo de datos de servicio.

A continuación, el Nodo1 suspende el envío (que corresponde al instante de suspensión del nodo de origen) del segundo flujo de datos de servicio subsiguiente al primer flujo de datos de servicio al camino de protección wrapping, añade el identificador a continuación de la última trama del primer flujo de datos de servicio enviado a través del camino de protección wrapping, envía el primer flujo de datos de servicio a través del camino de protección wrapping, y al mismo tiempo almacena temporalmente en el Buffer de retorno el segundo flujo de datos de servicio retenido.

A continuación, cuando el Nodo1 no detecta que se haya recibido el identificador, ello quiere decir que el primer flujo de datos de servicio que ha pasado por el Nodo1 en la dirección de protección del camino de protección wrapping no ha pasado por el camino Nodo1→Nodo2→Nodo1, y el Nodo1 no actúa. Cuando el Nodo1 detecta que se ha recibido el identificador, ello quiere decir que la última trama del primer flujo de datos de servicio transportado a través del camino de protección wrapping y enviado antes del instante de la retención ha pasado por el camino Nodo1→Nodo2→Nodo1, y llega a la posición siguiente del LSP de protección del Nodo1. Aquí, el Nodo1 realiza el proceso de la conmutación (que corresponde al instante de la conmutación del nodo de origen) de acuerdo con el mecanismo de protección steering, la etiqueta de una salida del Nodo1 se fija en 71 en lugar de 20, el Nodo1 en primer lugar envía en la dirección de protección el primer flujo de datos de servicio almacenado temporalmente en el Buffer de retorno, y transporta directamente el segundo flujo de datos de servicio subsiguiente por el camino de protección steering. El nodo de destino no realiza la conmutación, desde el instante de la suspensión del envío del nodo de origen hasta el instante de la conmutación del nodo de origen, y el flujo de datos de servicio transportado por el camino de protección wrapping llega al nodo de destino a través del camino Nodo1→Nodo6→Nodo5→Nodo4→Nodo3→Nodo4 después del instante de la conmutación del nodo de origen. De esta forma, el primer flujo de datos de servicio enviado en primer lugar llega antes al nodo de destino, de manera que se asegura la correcta relación de secuencia temporal entre el primer flujo de datos de servicio y el segundo flujo de datos de servicio.

Asimismo, el proceso de conmutación del nodo de destino y el camino de transporte del flujo de datos de servicio se pueden describir mediante referencia al proceso de conmutación del nodo de origen y al camino de transporte del flujo de datos de servicio, específicamente, como se muestra en la vista esquemática de la operación en la que el nodo de origen y el nodo de destino se conmutan al camino de protección steering de acuerdo con el modo de realización de la presente invención de la FIG. 6, con el fin de asegurar que cuando se conmuta el nodo de destino no se produce el problema de la alteración de secuencia del flujo de datos de servicio.

En el paso 410, tanto el nodo de origen como el nodo de destino completan la conmutación de acuerdo con el mecanismo de protección steering, conmutan el flujo de datos de servicio del camino de protección wrapping al camino de protección steering para su transporte, y completan el procedimiento de conmutación del mecanismo wrapping al mecanismo steering. Como se muestra en la FIG. 6, a modo de descripción, por ejemplo, se ha producido un fallo en el tramo entre el Nodo2 y el Nodo3, y tras haberse completado la conmutación de la protección en el nodo de destino, el camino de transporte del flujo de datos de servicio subsiguiente desde el nodo de origen hasta el nodo de destino es Nodo1→Nodo6→Nodo5→Nodo4.

Como una forma de implementación, el proceso del mensaje de solicitud de protección en el nodo de destino y la operación de conmutación correspondiente, se desarrollan de la siguiente forma, esto es, en el proceso, después del proceso de tratamiento del nodo de origen, el proceso realizado en el nodo de destino se puede reemplazar por los siguientes pasos, y el proceso completo es como se muestra en la FIG. 7.

En el paso 1001, tras recibir la información de solicitud de protección, el nodo de destino monitoriza la información del TM-SPRing, y determina si se ha recibido el identificador procedente del nodo de origen. El nodo de destino recibe necesariamente el identificador enviado por el nodo de origen, y cuando el nodo de destino recibe el identificador por primera vez, el proceso continúa en el paso 1002; de otro modo, se repite el paso 1001.

El nodo de destino recibe el identificador por primera vez, lo que indica que el primer flujo de datos de servicio transportado a través del camino de protección wrapping ha pasado completamente por el nodo de destino, y es transportado al nodo de destino a lo largo del camino de protección wrapping de acuerdo con el mecanismo wrapping.

En el paso 1002, el nodo de destino suspende el envío del segundo flujo de datos de servicio al camino de protección wrapping, y almacena temporalmente el segundo flujo de datos de servicio. Concretamente, el nodo de destino almacena temporalmente el segundo flujo de datos de servicio en el Buffer de retorno, y al mismo tiempo el nodo de destino recibe el primer flujo de datos de servicio a través del camino de protección wrapping.

En el paso 1003, el nodo de destino determina si se ha recibido por segunda vez el identificador procedente del nodo de origen, y si el identificador procedente del nodo de origen se ha recibido por segunda vez, el procedimiento continúa en el paso 1004; de otro modo, se repite el paso 1003.

En el paso 1004, el nodo de destino conmuta el camino de protección wrapping al camino de protección steering, conmuta el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering y, a continuación, empieza a recibir el flujo de datos de servicio subsiguiente almacenado temporalmente en el Buffer de retorno a través del camino de protección steering, con el fin de completar la conmutación de acuerdo con el mecanismo de protección steering.

La implementación conjunta del paso 1001, el paso 1002, el paso 1003 y el paso 1004 asegura que cuando el nodo de destino realiza la conmutación de la protección no se produce el problema de alteración de secuencia de los flujos de datos de servicio. Como se muestra en la FIG. 6, por ejemplo, se ha producido un fallo en el tramo entre el Nodo2 y el Nodo3, y tras haberse completado la conmutación de la protección, el camino de transporte del flujo de datos de servicio subsiguiente desde el nodo de origen hasta el nodo de destino es Nodo1→Nodo6→Nodo5→Nodo4.

Integrando las unidades que tienen ciertas funciones del método, en el modo de realización de la presente invención se pueden obtener un dispositivo relacionado y un sistema relacionado.

Un dispositivo del nodo de origen/dispositivo del nodo de destino dispone de unidades funcionales como se muestra en la FIG. 8, y las unidades funcionales comprenden una unidad 1101 de recepción, una unidad 1102 de retención, una unidad 1103 de almacenamiento temporal, una unidad 1104 de detección, y una unidad 1105 de respuesta a la detección que tienen las funciones correspondientes descritas más arriba, donde la unidad 1104 de detección comprende una unidad 11041 de anexión del identificador y una unidad 11042 de determinación que tienen las funciones correspondientes descritas más arriba. Se debe observar que cuando el dispositivo del nodo de destino determina, mediante un identificador proporcionado por la unidad de anexión de identificador, que un flujo de datos de servicio ha pasado por dicho nodo de destino, el nodo de destino no necesita la unidad de anexión de identificador.

Un sistema en una red de transporte de paquetes dispone de dispositivos como los que se muestran en la FIG. 9, y los dispositivos comprenden un dispositivo 1201 del nodo adyacente al tramo afectado por el fallo y un dispositivo 1202 del nodo de origen/nodo de destino, donde el dispositivo 1202 del nodo de origen/nodo de destino comprende una unidad 12021 de retención, una unidad 12022 de almacenamiento temporal, una unidad 12023 de detección, y una unidad 12024 de respuesta a la detección que tienen las funciones correspondientes descritas más arriba.

Como una de las formas de implementación, el dispositivo del nodo de origen/dispositivo del nodo de destino puede comprender, además, la unidad de recepción mencionada en el método.

En el método, el dispositivo y el sistema, de acuerdo con el modo de realización de la presente invención, en primer lugar, se envía el primer flujo de datos de servicio a través del camino de protección wrapping. Después, el nodo del flujo de datos de servicio suspende el envío del segundo flujo de datos de servicio subsiguiente al primer flujo de datos de servicio al camino de protección wrapping, y almacena temporalmente el segundo flujo de datos de servicio. Cuando el primer flujo de datos de servicio vuelve a pasar completamente por el nodo del flujo de datos de servicio, el segundo flujo de datos de servicio almacenado temporalmente es conmutado del camino de protección wrapping al camino de protección steering, resolviéndose de este modo el problema de alteración de secuencia que se produce cuando en la red de transporte de paquetes se aplica la solución de protección que combina el mecanismo wrapping y el mecanismo steering, con el fin de reforzar el mecanismo de protección del sistema en la red de transporte de paquetes y mejorar la capacidad del sistema de defensa frente a fallos. Se debe observar que el nodo de origen del flujo de servicio y el nodo de destino del flujo de servicio son los nodos del flujo de datos de servicio que tienen la función de enviar el flujo de datos de servicio, y los demás nodos que tienen las funciones descritas en la presente invención también se encuentran dentro del alcance de la protección de la presente invención.

Las personas con una experiencia ordinaria de la técnica deben entender que la totalidad o una parte de los procesos del método de acuerdo con los modos de realización se pueden implementar mediante un programa de

ordenador que controle al hardware pertinente. El programa se puede mantener en un medio de almacenamiento legible por el ordenador. Cuando se ejecuta el programa, se llevan a cabo los procesos del método de acuerdo con los modos de realización de la presente invención. El medio de almacenamiento puede ser un disco magnético, un disco óptico, una memoria de sólo lectura (ROM) o una memoria de acceso aleatorio (RAM).

Las descripciones anteriores constituyen meramente algunos ejemplos de los modos de realización de la presente invención.

REIVINDICACIONES

1. Un método de protección en una red de transporte de paquetes, en donde se establece un camino de protección para un flujo de datos de servicio transportado sobre un anillo de protección compartida en la red de transporte de paquetes, el flujo de datos de servicio comprende al menos un primer flujo de datos de servicio y un segundo flujo de datos de servicio, y el camino de protección comprende un camino de protección wrapping y un camino de protección steering, comprendiendo el método:

enviar el primer flujo de datos de servicio a través del camino de protección wrapping;

suspender, por parte de un nodo del flujo de datos de servicio, el envío al camino de protección wrapping del segundo flujo de datos de servicio subsiguiente al primer flujo de datos de servicio, y almacenar temporalmente el segundo flujo de datos de servicio; y

pasar completamente por segunda vez el primer flujo de datos de servicio por el nodo del flujo de datos de servicio y conmutar el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering;

en donde, después de enviar el primer flujo de datos de servicio a través del camino de protección wrapping, el método comprende, además:

añadir un identificador a continuación del primer flujo de datos de servicio,

el paso completo por segunda vez del primer flujo de datos de servicio por el nodo del flujo de datos de servicio comprende:

recibir el identificador del nodo del flujo de datos de servicio;

en donde

el método comprende, además: recibir del nodo del flujo de datos de servicio un mensaje de solicitud de protección que indica que se proteja el flujo de datos de servicio; y

la suspensión, por parte del nodo del flujo de datos de servicio, del envío al camino de protección wrapping del segundo flujo de datos de servicio subsiguiente comprende: suspender, por parte del nodo del flujo de datos de servicio, el envío al camino de protección wrapping del segundo flujo de datos de servicio de acuerdo con el mensaje de solicitud de protección.

2. El método de protección en una red de transporte de paquetes de acuerdo con la reivindicación 1, en donde el mensaje de solicitud de protección tiene la forma de una información de conmutación de protección automática, APS, y en donde la función del mensaje de solicitud de protección recibido se amplía, el valor del 8º bit de los bytes reservados de la información APS se cambia a 1, y la información APS ampliada se añade como identificador a continuación de la última trama del primer flujo de datos de servicio enviado a través del camino de protección wrapping.

3. Un método de protección en una red de transporte de paquetes, en donde se establece un camino de protección para un flujo de datos de servicio transportado sobre un anillo de protección compartida en una red de transporte de paquetes, el flujo de datos de servicio comprende al menos un primer flujo de datos de servicio y un segundo flujo de datos de servicio, y el camino de protección comprende un camino de protección wrapping y un camino de protección steering, comprendiendo el método:

enviar, por parte de un nodo de origen del flujo de servicio, el primer flujo de datos de servicio a través del camino de protección wrapping;

suspender, por parte del nodo de origen del flujo de servicio, el envío al camino de protección wrapping del segundo flujo de datos de servicio subsiguiente al primer flujo de datos de servicio, y almacenar temporalmente el segundo flujo de datos de servicio;

pasar completamente por segunda vez, por parte del primer flujo de datos de servicio, por el nodo de origen del flujo de servicio, y conmutar el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering;

pasar completamente por primera vez, por parte del primer flujo de datos de servicio, por el nodo de destino del flujo de servicio, suspender el envío del segundo flujo de datos de servicio al camino de protección wrapping, y almacenar temporalmente el segundo flujo de datos de servicio; y

pasar completamente por segunda vez, por parte del primer flujo de datos de servicio, por el nodo de destino del

flujo de servicio, y conmutar el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering;

en donde

después de enviar, por parte del nodo de origen del flujo de servicio, el primer flujo de datos de servicio a través del camino de protección wrapping, el método comprende, además: añadir, por parte del nodo de origen del flujo de servicio, un identificador a continuación del primer flujo de datos de servicio;

el paso completo por segunda vez, por parte del primer flujo de datos de servicio, por el nodo de origen del flujo de servicio comprende: recibir el identificador por parte del nodo de origen del flujo de servicio;

el paso completo por primera vez, por parte del primer flujo de datos de servicio, por el nodo de destino del flujo de servicio comprende: recibir por primera vez el identificador por parte del nodo de destino del flujo de servicio; y

el paso completo por segunda vez, por parte del primer flujo de datos de servicio, por el nodo de destino del flujo de servicio comprende: recibir por segunda vez el identificador por parte del nodo de destino del flujo de servicio;

en donde

el método comprende, además: recibir, por parte del nodo de origen del flujo de servicio, un mensaje de solicitud de protección que indica que se proteja el flujo de datos de servicio; y

la suspensión, por parte del nodo de origen del flujo de servicio, del envío al camino de protección wrapping del segundo flujo de datos de servicio subsiguiente al primer flujo de datos del servicio, comprende: suspender, por parte del nodo de origen del flujo de servicio, el envío al camino de protección wrapping del segundo flujo de datos de servicio de acuerdo con el mensaje de solicitud de protección.

4. El método de protección en una red de transporte de paquetes de acuerdo con la reivindicación 3, en donde el mensaje de solicitud de protección tiene la forma de una información de conmutación de protección automática, APS, y en donde la función del mensaje de solicitud de protección recibido se amplía, el valor del 8º bit de los bytes reservados de la información APS se cambia a 1, y la información APS ampliada se añade como identificador a continuación de la última trama del primer flujo de datos de servicio enviado a través del camino de protección wrapping.

5. Un dispositivo nodal de una red de transporte de paquetes, en donde el dispositivo nodal de la red de transporte de paquetes está situado en un anillo de protección compartida de la red de transporte de paquetes, el anillo de protección compartida dispone de un camino de protección para transportar un flujo de datos de servicio, el flujo de datos de servicio comprende al menos un primer flujo de datos de servicio y un segundo flujo de datos de servicio, y el camino de protección comprende un camino de protección wrapping y un camino de protección steering, en donde el dispositivo nodal comprende:

una unidad (1102) de retención, configurada para suspender el envío del segundo flujo de datos de servicio subsiguiente al primer flujo de datos de servicio al camino de protección wrapping, después de haber enviado el primer flujo de datos de servicio al camino de protección wrapping;

una unidad (1103) de almacenamiento temporal, configurada para almacenar temporalmente el segundo flujo de datos de servicio;

una unidad (1104) de detección, configurada para detectar si el flujo de datos de servicio ha pasado completamente por el nodo; y

una unidad (1105) de respuesta a la detección, configurada para conmutar el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering cuando la unidad (1104) de detección detecta que el primer flujo de datos de servicio ha pasado completamente por segunda vez por el nodo;

en donde la unidad (1104) de detección comprende:

una unidad (11041) de anexión de identificador, configurada para añadir un identificador a continuación del primer flujo de datos de servicio; y

una unidad (11042) de determinación, configurada para determinar si se ha recibido el identificador, y, en caso afirmativo, confirmar que el flujo de datos de servicio ha pasado completamente por el nodo;

el dispositivo nodal comprende, además:

una unidad (1101) de recepción, configurada para hacer que la unidad de retención suspenda el envío del segundo flujo de datos de servicio a través del camino de protección wrapping, después de haber recibido un mensaje de solicitud de protección que indica que hay que proteger el flujo de datos de servicio.

6. El dispositivo nodal de una red de transporte de paquetes de acuerdo con la reivindicación 5, en donde el mensaje de solicitud de protección tiene la forma de una información de conmutación de protección automática, APS, y en donde la función del mensaje de solicitud de protección recibido se amplía, el valor del 8º bit de los bytes reservados de la información APS se cambia a 1, y la información APS ampliada se añade como identificador a continuación de la última trama del primer flujo de datos de servicio enviado a través del camino de protección wrapping.

7. El dispositivo nodal de una red de transporte de paquetes de acuerdo con la reivindicación 5 ó 6, en donde el dispositivo nodal de la red de transporte de paquetes es un dispositivo nodal de origen de un flujo de servicio o un dispositivo nodal de destino de un flujo de servicio.

8. Un sistema en una red de transporte de paquetes, en donde, en el sistema se aplica un anillo de protección compartida de la red de transporte de paquetes, el anillo de protección compartida dispone de un camino de protección para transportar un flujo de datos de servicio, el flujo de datos de servicio comprende al menos un primer flujo de datos de servicio y un segundo flujo de datos de servicio, el camino de protección comprende un camino de protección wrapping y un camino de protección steering, el sistema comprende un dispositivo nodal (1202) de origen de un flujo de servicio y un dispositivo nodal (1202) de destino de un flujo de servicio en el anillo de protección compartida, en donde

el dispositivo nodal (1202) de origen del flujo de servicio está configurado para suspender el envío del segundo flujo de datos de servicio subsiguiente al primer flujo de datos de servicio al camino de protección wrapping, después de haber enviado el primer flujo de datos de servicio al camino de protección wrapping, y almacenar temporalmente el segundo flujo de datos de servicio; y conmutar el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering cuando el primer flujo de datos de servicio ha pasado completamente por segunda vez por el nodo del flujo de datos de servicio; y

el dispositivo nodal (1202) de destino del flujo de servicio está configurado para detectar si el flujo de datos de servicio ha pasado completamente por el nodo de destino del flujo de servicio; suspender el envío del segundo flujo de datos de servicio al camino de protección wrapping, cuando una segunda unidad de detección detecta que el primer flujo de datos de servicio ha pasado completamente por primera vez por el nodo de destino del flujo de servicio, y almacenar temporalmente el segundo flujo de datos de servicio; y conmutar el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering, cuando la segunda unidad de detección detecta que el primer flujo de datos de servicio ha pasado completamente por segunda vez por el nodo de destino del flujo de servicio;

en donde el dispositivo nodal de origen del flujo de servicio comprende:

una primera unidad (1102) de retención, configurada para suspender el envío del segundo flujo de datos de servicio subsiguiente al primer flujo de datos de servicio al camino de protección wrapping, después de haber enviado el primer flujo de datos de servicio al camino de protección wrapping;

una primera unidad (1103) de almacenamiento temporal, configurada para almacenar temporalmente el segundo flujo de datos de servicio;

una primera unidad (1104) de detección, configurada para detectar si el flujo de datos de servicio ha pasado completamente por el nodo de origen del flujo de servicio; y

una primera unidad (1105) de respuesta a la detección, configurada para conmutar el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering, cuando la primera unidad de detección detecta que el primer flujo de datos de servicio ha pasado completamente por segunda vez por el nodo de origen del flujo de servicio;

y

el dispositivo nodal de destino del flujo de servicio comprende:

una segunda unidad (1104) de detección, configurada para detectar si el flujo de datos de servicio ha pasado completamente por el nodo de destino del flujo de servicio;

una segunda unidad (1102) de retención, configurada para suspender el envío del segundo flujo de datos de servicio al camino de protección wrapping, cuando la segunda unidad (1104) de detección detecta que el primer flujo de datos de servicio ha pasado completamente por primera vez por el nodo (1202) de destino del flujo de servicio;

una segunda unidad (1103) de almacenamiento temporal, configurada para almacenar temporalmente el segundo

flujo de datos de servicio; y

una segunda unidad (1105) de respuesta a la detección, configurada para conmutar el segundo flujo de datos de servicio almacenado temporalmente del camino de protección wrapping al camino de protección steering, cuando la segunda unidad (1104) de detección detecta que el primer flujo de datos de servicio ha pasado completamente por segunda vez por el nodo (1202) de destino del flujo de servicio;

en donde la primera unidad (1104) de detección comprende:

una unidad (11041) de anexión de identificador, configurada para añadir un identificador a continuación del primer flujo de datos de servicio; y

una unidad (11042) de determinación, configurada para determinar si se ha recibido el identificador, y, si el identificador se ha recibido, confirmar que el primer flujo de datos de servicio ha pasado completamente por el nodo (1202) de origen del flujo de servicio;

y

la segunda unidad (1104) de detección está configurada para determinar si se ha recibido el identificador, y, si el identificador se ha recibido, confirmar que el primer flujo de datos de servicio ha pasado completamente por el nodo (1202) de destino del flujo de servicio;

en donde el dispositivo nodal (1202) de origen del flujo de servicio comprende, además:

una unidad (1101) de recepción, configurada para hacer que la unidad (1102) de retención suspenda el envío del segundo flujo de datos de servicio a través del camino de protección wrapping, después de haber recibido un mensaje de solicitud de protección que indica que hay que proteger el flujo de datos de servicio.

9. El sistema en una red de transporte de paquetes de acuerdo con la reivindicación 8, en donde el mensaje de solicitud de protección tiene la forma de una información de conmutación de protección automática, APS, y en donde la función del mensaje de solicitud de protección recibido se amplía, el valor del 8º bit de los bytes reservados de la información APS se cambia a 1, y la información APS ampliada se añade como identificador a continuación de la última trama del primer flujo de datos de servicio enviado a través del camino de protección wrapping.

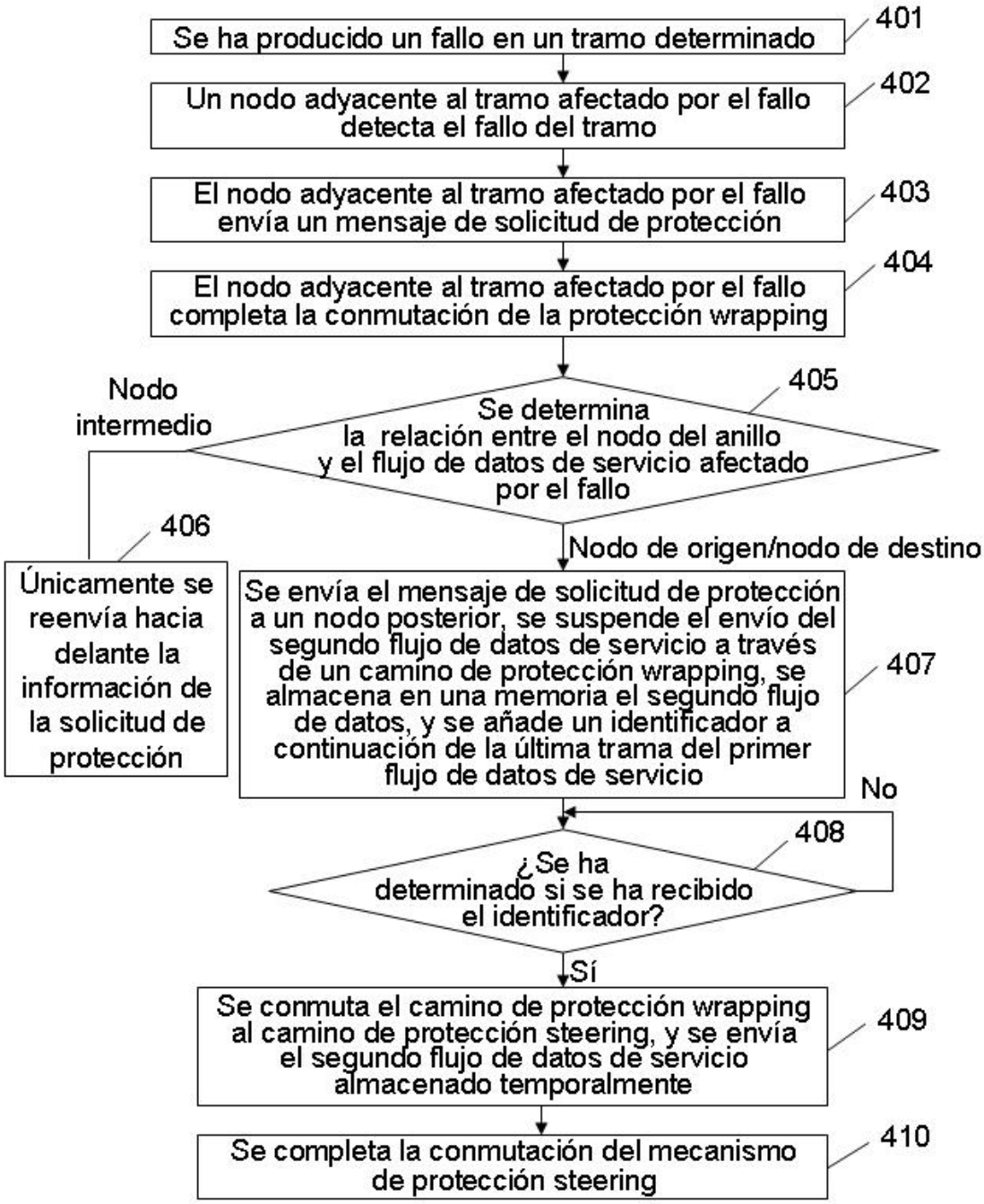
Se ha producido un fallo en un tramo determinado
401
Un nodo adyacente al tramo afectado por el fallo detecta el fallo del tramo
402
El nodo adyacente al tramo afectado por el fallo envía un mensaje de solicitud de protección
403
El nodo adyacente al tramo afectado por el fallo completa la conmutación de la protección wrapping
404
Nodo intermedio
Se determina la relación entre el nodo del anillo y el flujo de datos de servicio afectado por el fallo
405
Nodo de origen/nodo de destino
406
Únicamente se reenvía hacia delante la información de la solicitud de protección
Se envía el mensaje de solicitud de protección a un nodo posterior, se suspende el envío del segundo flujo de datos de servicio a través de un camino de protección wrapping, se almacena en una memoria el segundo flujo de datos, y se añade un identificador a continuación de la última trama del primer flujo de datos de servicio
407
No
¿Se ha determinado si se ha recibido el identificador?
408
Sí
Se conmuta el camino de protección wrapping al camino de protección steering, y se envía el segundo flujo de datos de servicio almacenado temporalmente
409
Se completa la conmutación del mecanismo de protección steering
410

FIG. 1

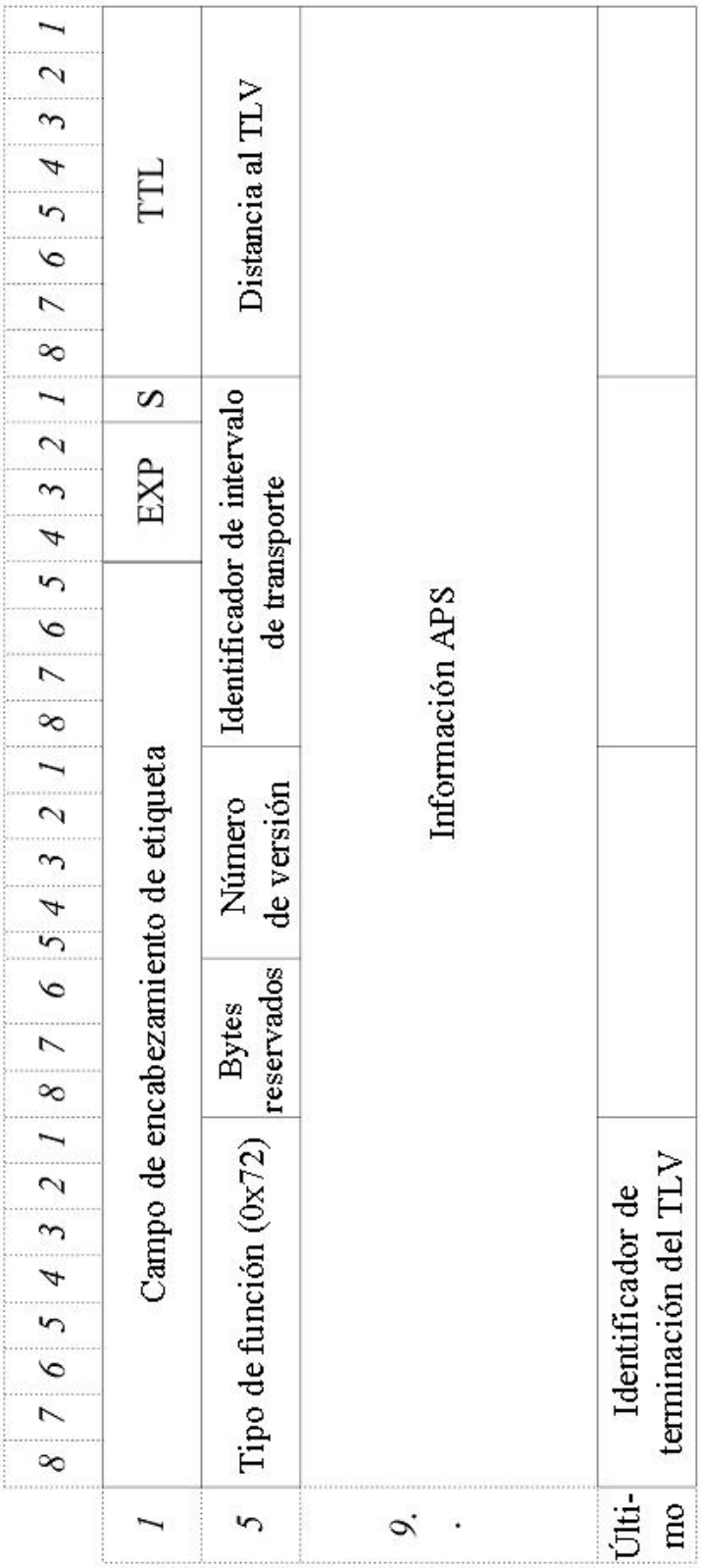
8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1 8 7 6 5 4 3 2 1
1
Campo de encabezamiento de etiqueta
EXP
S
TTL
5
Tipo de función (0x72)
Bytes reservados
Número de versión
Identificador de intervalo de transporte
Distancia al TLV
9.
.
.
Información APS
Últi-mo
Identificador de terminación del TLV

FIG. 2

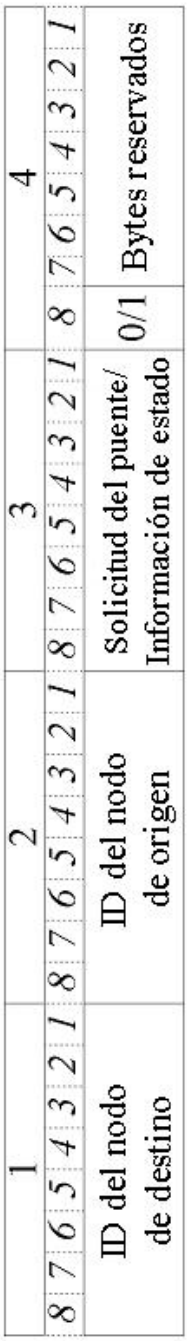
1
2
3
4
8 7 6 5 4 3 2 1
ID del nodo de destino
ID del nodo de origen
Solicitud del puente/ Información de estado
0/1
Bytes reservados

FIG. 3

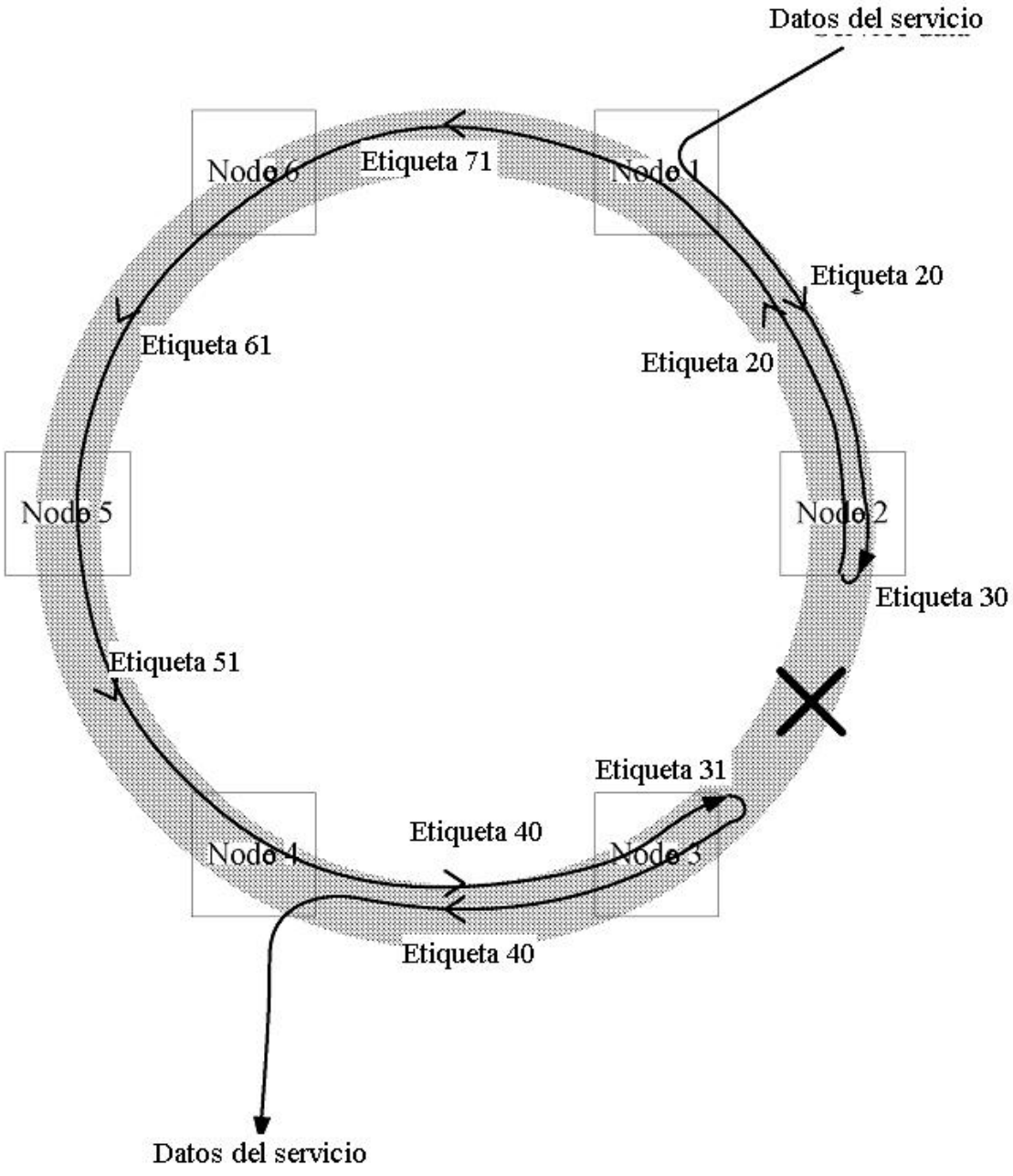
Datos del servicio
Nodo 6
Etiqueta 71
Nodo 1
Etiqueta 20
Etiqueta 61
Etiqueta 20
Nodo 5
Nodo 2
Etiqueta 30
Etiqueta 51
Etiqueta 31
Nodo 4
Etiqueta 40
Nodo 3
Etiqueta 40
Datos del servicio

FIG. 4

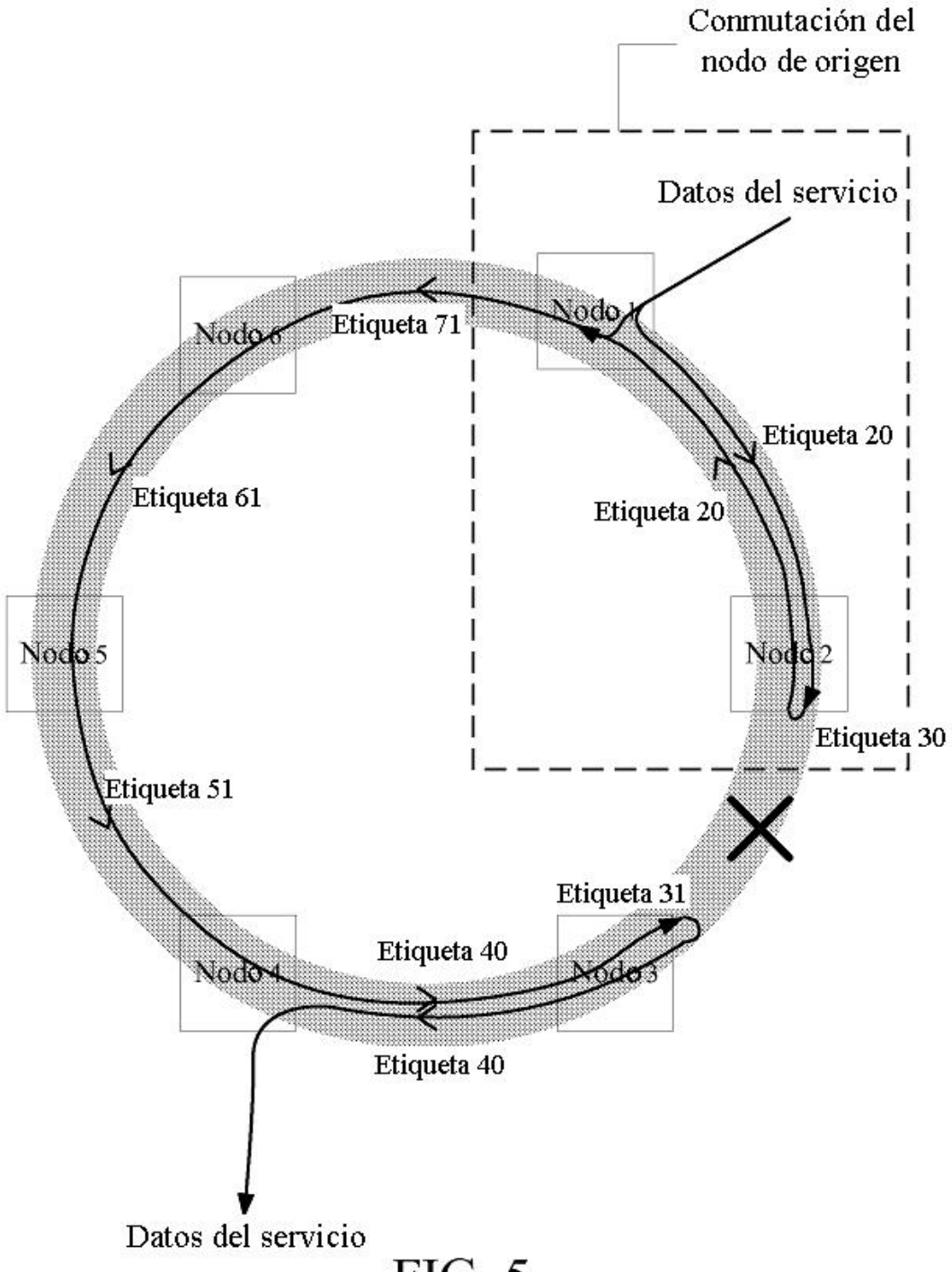
Conmutación del nodo de origen
Datos del servicio
Nodo 1
Nodo 2
Nodo 3
Nodo 4
Nodo 5
Nodo 6
Etiqueta 71
Etiqueta 20
Etiqueta 20
Etiqueta 61
Etiqueta 30
Etiqueta 51
Etiqueta 31
Etiqueta 40
Etiqueta 40
Datos del servicio

FIG. 5

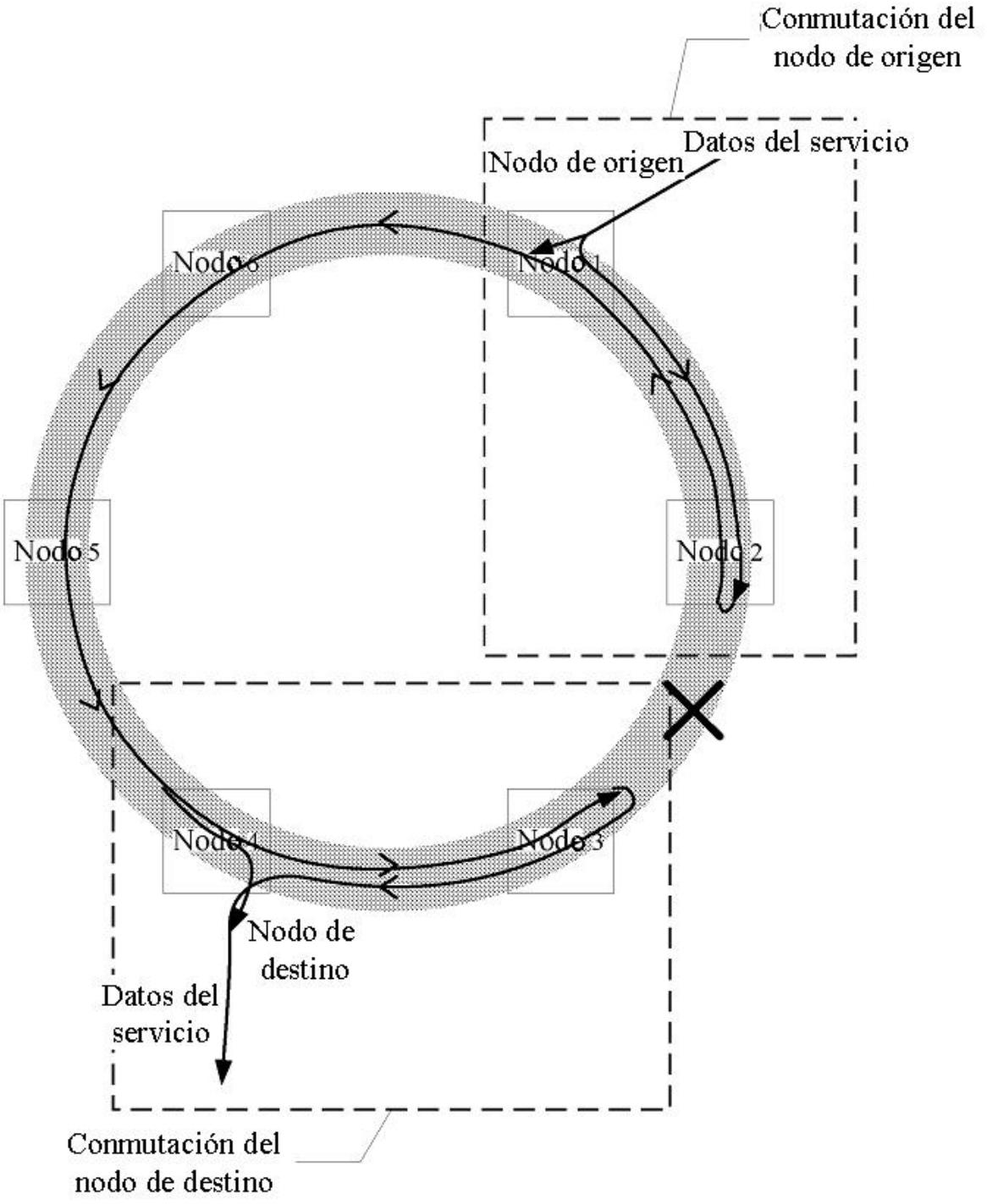
Conmutación del nodo de origen
Nodo de origen
Datos del servicio
Nodo 6
Nodo 1
Nodo 5
Nodo 2
Nodo 4
Nodo 3
Nodo de destino
Datos del servicio
Conmutación del nodo de destino

FIG. 6

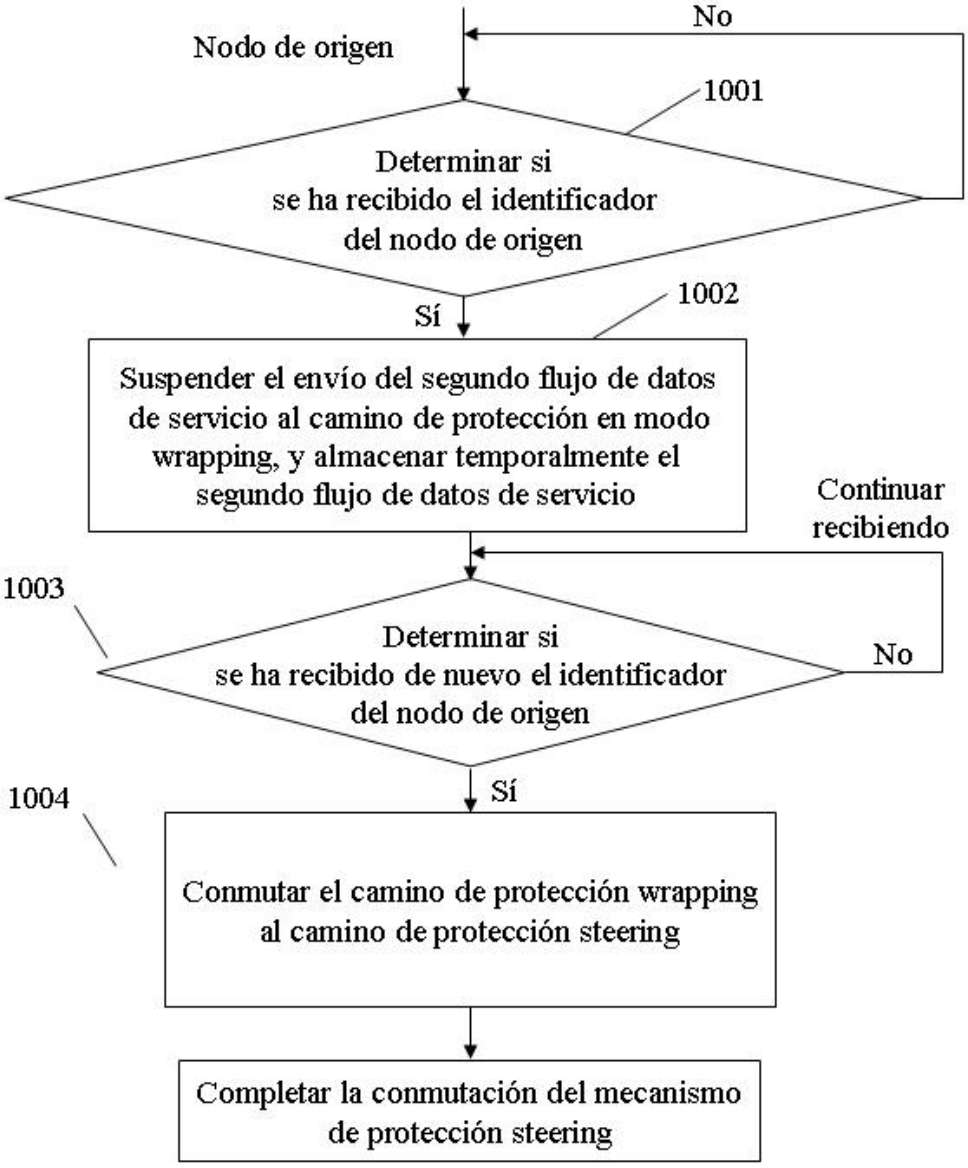
Nodo de origen
No
1001
Determinar si
se ha recibido el identificador
del nodo de origen
Sí
1002
Suspender el envío del segundo flujo de datos
de servicio al camino de protección en modo
wrapping, y almacenar temporalmente el
segundo flujo de datos de servicio
Continuar
recibiendo
1003
Determinar si
se ha recibido de nuevo el identificador
del nodo de origen
No
Sí
1004
Conmutar el camino de protección wrapping
al camino de protección steering
Completar la conmutación del mecanismo
de protección steering

FIG. 7

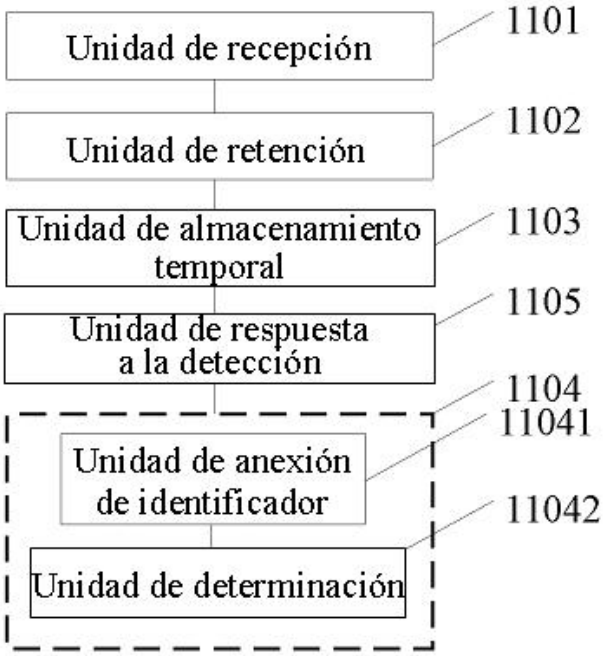
Unidad de recepción
1101
Unidad de retención
1102
Unidad de almacenamiento temporal
1103
Unidad de respuesta a la detección
1105
1104
11041
Unidad de anexión de identificador
11042
Unidad de determinación

FIG. 8

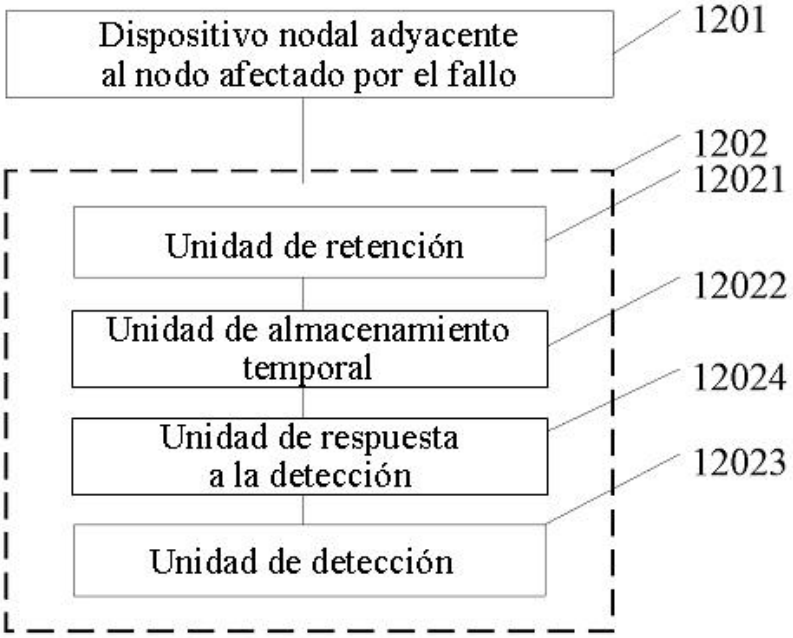
Dispositivo nodal adyacente al nodo afectado por el fallo
1201
1202
12021
Unidad de retención
12022
Unidad de almacenamiento temporal
12024
Unidad de respuesta a la detección
12023
Unidad de detección

FIG. 9