

19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 374 314**

51 Int. Cl.:  
**H04B 1/74** (2006.01)  
**H04L 12/24** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 96 Número de solicitud europea: **07720502 .9**  
96 Fecha de presentación: **22.03.2007**  
97 Número de publicación de la solicitud: **2028768**  
97 Fecha de publicación de la solicitud: **25.02.2009**

54 Título: **MÉTODO, SISTEMA Y DISPOSITIVO DE PROTECCIÓN DE SERVICIO EN UNA RED SIN CONEXIÓN.**

30 Prioridad:  
**05.06.2006 CN 200610083530**

45 Fecha de publicación de la mención BOPI:  
**15.02.2012**

45 Fecha de la publicación del folleto de la patente:  
**15.02.2012**

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

72 Inventor/es:  
**YANG, Faming**

74 Agente: **Lehmann Novo, Isabel**

ES 2 374 314 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

## DESCRIPCIÓN

Método, sistema y dispositivo de protección de servicio en una red sin conexión

## 5 CAMPO DE LA INVENCION

La presente invención se refiere a la protección de red y más en particular, a un método, sistema y dispositivo para la protección del servicio en una red sin conexión.

## 10 ANTECEDENTES DE LA INVENCION

Una red sin conexión, con soporte de conmutación de protección, está constituida por un conmutador Ethernet situado en el núcleo, también referido como un dispositivo de núcleo, y un conmutador Ethernet o encaminador situado en el borde, también referido como un dispositivo de borde o un nodo de borde. El dispositivo de borde es responsable de realizar la operación de conmutación de servicio cuando se produce un fallo en la red con soporte de conmutación de protección. El dispositivo de borde es acoplado directamente a un dispositivo externo de la red con soporte de conmutación de protección. En la red con soporte de conmutación de protección, los datos se reenvían en un modo sin conexión. Por ejemplo, en Ethernet, los paquetes de datos se reenvían a través de una tabla de reenvío de rutas de datos establecida basándose en un entorno de árbol de expansión. La red que reenvía los paquetes de datos en un modo sin conexión está constituida por dispositivos de conmutadores Ethernet interconectados. La red se refiere también como un dominio de flujo.

En la técnica anterior, fue propuesta una solución de conmutación de protección para un servicio de red de área local virtual (VLAN) punto a punto (P2P). Además, un método de conmutación de protección para red VLAN punto a multipunto (P2MP) y una red VLAN multipunto a multipunto (MP2MP) está siendo objeto de estudio.

Se describen métodos de conmutación de protección de servicio para una red sin conexión según la técnica anterior. Puesto que no existe ninguna ruta de conexión orientada a la conexión en el dominio de flujo, se recomienda proteger el dominio de flujo completo. La protección del dominio de flujo así recomendada está dividida en un dominio de flujo de trabajo, un dominio de flujo de protección y varios puntos de conmutación de protección (PSP) acoplados a otros dominios de flujo. La Figura 1 ilustra un diagrama de protección de dominios de flujo para una red sin conexión. Cuando falla el dominio de flujo de trabajo o el dominio de flujo de protección, PSP es responsable del flujo del servicio de conmutación. Por ejemplo, si se supone que no se produce ningún fallo, en el dominio de flujo de protección, cuando se produce un fallo en el dominio de flujo de trabajo, el método de conmutación de protección sería el de que el PSP conmuta el servicio original, proporcionado a partir del dominio de flujo de trabajo, al dominio del flujo de protección.

Sin embargo, el método anterior, propuesto por la técnica anterior, presenta los inconvenientes indicados a continuación.

Por un lado, puesto que cada punto de conmutación ha de coordinarse con el resto de los puntos de conmutación con el fin de conmutar el flujo de servicio proporcionado desde el dominio de flujo de trabajo al dominio de flujo de protección. En consecuencia, la coordinación entre los PSPs es muy compleja. Por otro lado, puesto que no existe ninguna entrada directa correspondiente al flujo de datos conmutado desde el dominio de flujo de trabajo en el dominio de flujo de protección, los paquetes de datos de servicio serán objeto de inundación operativa después de la conmutación de protección. Por lo tanto, el mecanismo de conmutación de protección, para el dominio de flujo anterior, parece ser complicado y es deseable un estudio adicional.

Actualmente, existen dos soluciones de conmutación de protección para la protección del dominio del flujo.

La primera solución es una solución de conmutación de protección de servicio de red VLAN.

Esta solución de conmutación de protección es aplicable a una red Ethernet backbone central, con un árbol de B-VLAN de trabajo y un árbol de B-VLAN de protección establecidos para el identificador ID de red VLAN backbone de trabajo (B-VLAN ID) y el identificador ID de red B-VLAN de protección, respectivamente. En condiciones normales, el árbol de B-VLAN se puede utilizar y los correspondientes paquetes de datos de servicios desde fuera de la red backbone central se transmiten en función de la tabla de reenvío de rutas de datos conocida. Mientras tanto, el mensaje de control de continuidad (CC) para la gestión de fallos de continuidad (CFM) se transmite periódicamente para comprobar el estado de trabajo (NORMAL o FALLO) del árbol B-VLAN de trabajo y el B-VLAN de protección, respectivamente, de modo que la conmutación de protección para los datos de servicio se pueda realizar cuando se produce un fallo. Suponiendo que el árbol de B-VLAN de protección está en un estado operativo normal, cuando se produce un fallo en el árbol de B-VLAN de trabajo, todos los paquetes de datos de servicio proporcionados originalmente por el árbol de B-VLAN de trabajo se conmutan ahora al árbol de B-VLAN de protección para una entrega adicional.

La solución de conmutación de protección de servicio de red VLAN, propuesta por la solución anterior, no puede evitar la inundación operativa de flujos de datos de unidifusión en el dominio de flujo conmutado, en donde el flujo de datos de unidifusión fue reenviado en función de la tabla de reenvío de rutas de datos conocida antes de la conmutación. Además, cuando se produce un fallo en el árbol de B-VLAN de trabajo, los paquetes de datos en el árbol B-VLAN, que no están

5 sujetos al fallo, se conmutarían también al árbol B-VLAN de protección. La conmutación según esta solución se pone en práctica sobre una base de árbol por árbol, lo que significa que en tanto que se produzca cualquier fallo en el árbol B-VLAN de trabajo, la totalidad de los paquetes de datos en el árbol completo pasarían a través de la función de conmutación de protección. En consecuencia, esto podría causar que los paquetes de servicio quedaran fuera de la secuencia operativa.

La segunda solución es un método de conmutación de protección basado en un entorno de árbol de expansión (*spanning tree*).

10 Este método se puede poner en práctica como sigue. En una red con soporte de conmutación de protección constituida por conmutadores Ethernet y encaminadores, los dispositivos de borde tales como conmutadores Ethernet o encaminadores se utilizan para la conmutación de protección. Diferentes Identificadores VLAN IDs se utilizan en la red, con soporte de conmutación de protección, para representar árboles de expansión diferentes. Además, para cada nodo, se configura un árbol que excluye a ese nodo y para cada enlace, se configura un árbol que excluye ese enlace. En consecuencia, al menos un árbol integral está garantizado cuando se produce un fallo de nodo único o de enlace único. La topología del árbol configurado permanece invariable aun cuando se produce un fallo.

20 En la red con soporte de conmutación de protección, se utiliza un modo de reserva maestro o un modo de utilización compartida para proporcionar el servicio. En el modo de reserva maestro, se predefine un árbol maestro y un árbol de protección. En condiciones operativas normales, la totalidad de los servicios se proporcionan a lo largo del árbol maestro en función de la tabla de reenvíos de rutas de datos que se conoce. Cuando falla un nodo o un enlace en el árbol maestro, la totalidad de los servicios a través del árbol maestro se conmutan a uno de los árboles de protección en la red con soporte de conmutación de protección, que no está sujeto al fallo. En el modo de utilización compartida, y en condiciones operativas normales, los servicios se distribuyen uniformemente a todos los árboles de trabajo para su entrega. Cuando falla un nodo o un enlace en algún árbol, la totalidad de los servicios proporcionados a lo largo del árbol de trabajo, afectado por el fallo, serían conmutados a los árboles en reposo con fallos.

30 Con el fin de garantizar una conmutación de protección rápida cuando se produce un fallo en un enlace o en un nodo único, se utilizan tres tipos de mensajes para comprobar el funcionamiento de cada árbol en el método de conmutación de protección basado en el entorno de árbol de expansión, según la segunda solución propuesta.

- (1) Mensaje de Keep Alive (KA) o Siempre Activo. Un mensaje KA de cada identificador ID VLAN se difunde periódicamente por uno o más nodos de borde a los nodos de borde en reposo.
- 35 (2) Mensaje de Notificación de fallo. Si el mensaje KA de un determinado VLAN ID no se ha recibido por un nodo de borde determinado en un plazo de tiempo de detección, el nodo de borde informaría a todos los demás nodos de borde mediante un mensaje de notificación de fallo, de que el árbol al que corresponde el VLAN ID está en condición defectuosa.
- 40 (3) Mensaje de notificación de reparación de fallo. Cuando un nodo de borde determinado recibe un mensaje KA correspondiente desde el árbol original en el que se produjo el fallo, el nodo de borde informa a todos los demás nodos de borde, mediante un mensaje de notificación de reparación de fallo, de que el árbol al que corresponde el VLAN ID ha sido reparado a la condición normal.

45 La segunda solución está basada también en la conmutación árbol por árbol. Según esta segunda solución, cuando se conmutan los paquetes de datos de servicio, no se puede evitar la inundación operativa de flujos de datos de unidifusión, en el dominio de flujo conmutado, en donde el flujo de datos de unidifusión fue reenviado en función de la tabla de reenvíos de rutas de datos conocida antes de la conmutación. Cuando falla el árbol maestro o el árbol de trabajo, los paquetes de datos en el árbol maestro o en el árbol de trabajo, que no están sujetos al fallo, se conmutarían también al otro árbol de protección. En consecuencia, esto podría causar que los paquetes de datos de servicio quedaran fuera de la secuencia operativa.

55 El documento US 2003/016624 A1 da a conocer un método para gestionar rutas activas múltiples entre una pluralidad de conmutadores de red para identificar y seleccionar una ruta alternativa en respuesta al fallo de una ruta desde un conmutador a un dispositivo. Protocolos de equilibrio de carga permiten el uso simultáneo de múltiples rutas entre dispositivos de la red a través de una malla de conmutadores de red en cumplimiento operativo. Cuando falla un puerto de un conmutador de red, un conmutador selecciona un puerto alternativo que se puede utilizar para reenviar paquetes a dispositivos normalmente alcanzados a través del puerto en condición de fallo. Los conmutadores de redes intercambian mensajes para identificar las rutas alternativas potenciales. Una ruta alternativa potencial se utiliza para enviar un mensaje de sondeo a un conmutador de red próximo para determinar si está disponible una ruta a los dispositivos identificados a través del conmutador de red próximo. Dichos mensajes de sondeo se propagan a través de todos los conmutadores de redes intermedios entre el conmutador que detecta el puerto en condición de fallo hasta el dispositivo de red identificado. Mensajes de confirmación se reenvían para verificar la posible disponibilidad de una ruta alternativa. En aquellos casos en que un conmutador de red intermedio determina que la ruta completa no está disponible a través de ella al dispositivo identificado o en donde existe una ruta potencialmente mejor, se reenvía un mensaje de sondeo regenerado indicando así, a lo largo de la ruta, que se inició el mensaje de sondeo.

## SUMARIO DE LA INVENCION

- 5 Formas de realización de la presente invención dan a conocer un método, sistema y dispositivo para la conmutación de protección de servicio, sin conexión, en una red sin conexión, que puede poner en práctica la conmutación de protección para servicios punto a multipunto o multipunto a multipunto por intermedio de la conmutación de protección punto a punto. El método, sistema y dispositivo pueden evitar efectivamente el problema de la inundación operativa causado por la conmutación de protección.
- 10 Más concretamente, las soluciones técnicas según las formas de realización de la presente invención se presentan como sigue.
- 15 Un método para la conmutación de protección de servicio, en una red sin conexión, puede ser aplicable entre una pluralidad de puntos de conmutación de protección que pertenecen a una misma instancia de servicio. La pluralidad de puntos de conmutación de protección están situados en una red con soporte de conmutación de protección, que incluye un dominio de flujo de trabajo y un dominio de flujo de protección. Cada punto de conmutación de protección se acopla a al menos dos puntos de conmutación de protección distantes. Existe una ruta entre el punto de conmutación de protección y cada punto de conmutación de protección distante, en el dominio de flujo de trabajo y en el dominio de flujo de protección, respectivamente. El método comprende las etapas siguientes:
- 20 el establecimiento de una tabla de reenvío de rutas para la totalidad de los puntos de conmutación de protección en el dominio de flujo de trabajo y en el dominio de flujo de protección;
- 25 la difusión, por cada punto de conmutación de protección, de un mensaje de detección de fallo, periódicamente, a al menos dos puntos de conmutación de protección distantes a los que se acopla cada punto de conmutación de protección;
- 30 la determinación, por cada punto de conmutación de protección distante, de que se ha producido un fallo en una ruta en el dominio de flujo de trabajo si el punto de conmutación de protección no ha recibido el mensaje de detección de fallo, difundido por el punto de conmutación de protección distante, a partir de la ruta en el dominio de flujo de trabajo dentro de un tiempo de detección predeterminado;
- 35 la determinación, por cada punto de conmutación de protección distante, de que se ha producido un fallo en una ruta en el dominio de flujo de protección si el punto de conmutación de protección no ha recibido el mensaje de detección de fallo, difundido por el punto de conmutación de protección distante, a partir de la ruta en el dominio de flujo de protección dentro de un tiempo de detección predeterminado;
- 40 el envío de un mensaje de notificación de fallo, a través de la ruta en el otro dominio de flujo, al punto de conmutación de protección distante que está situado en la ruta en la que se produjo el fallo cuando cada punto de conmutación de protección detecta un fallo ocurrido en una ruta en uno de entre el dominio de flujo de trabajo y el dominio de flujo de protección y
- 45 la prestación de un servicio en la instancia de servicio, cuya dirección de destino es la dirección de origen del mensaje de notificación de fallo, a través de la ruta en el otro dominio de flujo en función de la tabla de reenvío de rutas después de recibir el mensaje de notificación de fallo desde el punto de conmutación de protección distante.
- 50 Un sistema para la conmutación de protección de servicio, en una red sin conexión, comprende un dominio de flujo de trabajo, un dominio de flujo de protección y una pluralidad de puntos de conmutación de protección pertenecientes a una misma instancia de servicio.
- 55 La pluralidad de puntos de conmutación de protección están situados en una red con soporte de conmutación de protección que comprende el dominio de flujo de trabajo y el dominio de flujo de protección. Cada punto de conmutación de protección se acopla a al menos dos puntos de conmutación de protección distantes. Además, existe una ruta entre el punto de conmutación de protección y cada punto de conmutación de protección distante, en el dominio de flujo de trabajo y en el dominio de flujo de protección, respectivamente, estando cada punto de conmutación de protección configurado para:
- 60 la difusión, por cada punto de conmutación de protección, de un mensaje de detección de fallo, periódicamente, a al menos dos puntos de conmutación de protección distantes a los que se acopla cada punto de conmutación de protección;
- 65 la determinación, por cada punto de conmutación de protección distante, de que un fallo se ha producido en una ruta en el dominio de flujo de trabajo si el punto de conmutación de protección no ha recibido el mensaje de detección de fallo, difundido por el punto de conmutación de protección distante, desde la ruta en el dominio de flujo de trabajo dentro de un tiempo de detección predeterminado;

la determinación, por cada punto de conmutación de protección distante, de que un fallo se ha producido en una ruta en el dominio de flujo de protección si el punto de conmutación de protección no ha recibido el mensaje de detección de fallo, difundido por el punto de conmutación de protección distante, desde la ruta en el dominio de flujo de protección dentro de un tiempo de detección predeterminado;

5 el envío de un mensaje de notificación de fallo, a través de la ruta en el otro dominio de flujo, al punto de conmutación de protección distante, que está situado en la ruta en la que se produjo el fallo, cuando cada punto de conmutación de protección detecta un fallo producido en una ruta en uno de entre el dominio de flujo de trabajo y el dominio de flujo de protección y

10 la prestación de un servicio en la instancia de servicio, cuya dirección de destino es la dirección de origen del mensaje de notificación de fallo, a través de la ruta en el otro dominio de flujo en función de la tabla de reenvíos de rutas después de recibir el mensaje de notificación de fallo desde el punto de conmutación de protección distante, en donde la tabla de reenvíos de rutas se establece para la totalidad de los puntos de conmutación de protección en el dominio de flujo de trabajo y en el dominio de flujo de protección.

15 Se puede deducir que el método, sistema y dispositivo de conmutación de protección de servicio, para una red sin conexión, según la presente invención, está basado en la conmutación de rutas punto a punto y no en la conmutación de árboles operativos. Cuando se produce un fallo en la red con soporte de conmutación de protección, solamente se conmuta el servicio prestado entre los puntos de conmutación de protección afectados por el fallo, mientras que los demás servicios entre los puntos de conmutación de protección, que no estén afectados por el fallo, no serán objeto de conmutación. Las formas de realización de la presente invención evitan, efectivamente, el problema de inundación operativa causado por la conmutación de protección, disminuyendo, de este modo, la influencia sobre el servicio MP2MP que se impone por el fallo producido en la red con soporte de conmutación de protección.

25 **BREVE DESCRIPCIÓN DE LOS DIBUJOS**

La Figura 1 es una ilustración de conmutación de protección de dominio de flujo en una red sin conexión;

30 La Figura 2 es una ilustración de configuración para una red sin conexión con soporte de conmutación de protección según una forma de realización de la presente invención;

La Figura 3 es una ilustración de supervisión del estado de la ruta para la red con soporte de conmutación de protección, según una forma de realización de la presente invención;

35 La Figura 4 es una ilustración de supervisión del estado de la ruta para la red con soporte de conmutación de protección, según una forma de realización de la presente invención;

40 La Figura 5a es una ilustración de suministro de paquetes de datos de unidifusión cuando la red con soporte de conmutación de protección está en una condición operativa normal, según una forma de realización de la presente invención;

45 La Figura 5b es una ilustración de suministro de paquetes de datos de unidifusión cuando la red con soporte de conmutación de protección está en condición defectuosa, según una forma de realización de la presente invención;

La Figura 6a es una ilustración de suministro de paquetes de datos de difusión cuando la red con soporte de conmutación de protección está en una condición normal, según una forma de realización de la presente invención y

50 La Figura 6b es una ilustración de suministro de paquetes de datos de difusión cuando la red con soporte de conmutación de protección está en condición defectuosa, según una forma de realización de la presente invención.

**DESCRIPCIÓN DETALLADA DE LA INVENCION**

55 Según las formas de realización de la presente invención, cuando se produce un fallo en una red con soporte de conmutación de protección, solamente el servicio prestado entre los puntos de conmutación de protección, afectados por el fallo, se conmutan mientras que el servicio entre los puntos de conmutación de protección, que no son afectados por el fallo, no serán conmutados.

60 Más concretamente, una red sin conexión, con soporte de conmutación de protección, comprende un dominio de flujo de trabajo, un dominio de flujo de protección y una pluralidad de puntos de conmutación de protección. El método, según las formas de realización de la presente invención, puede ser aplicable entre una pluralidad de puntos de conmutación de protección que pertenecen a una misma instancia de servicio. Cada punto de conmutación de protección está acoplado a al menos dos puntos de conmutación de protección distantes. Una ruta existe entre el punto de conmutación de protección y cada punto de conmutación de protección distante, en el dominio de flujo de trabajo y en el dominio de flujo de protección, respectivamente. En cada punto de conmutación de protección la información de la red sin conexión, con soporte de conmutación de protección, es objeto de configuración y se determina un puerto de trabajo y un puerto de

protección para cada punto de conmutación de protección. El puerto de trabajo está acoplado a al menos una ruta en el dominio de flujo de trabajo de la red con soporte de conmutación de protección. El puerto de protección está acoplado a al menos una ruta en el dominio de flujo de protección de la red con soporte de conmutación de protección. En una situación operativa normal, el punto de conmutación de protección envía/recibe paquetes de datos, o tráfico de servicio, a través de su puerto de trabajo en un dominio de flujo de trabajo. Mientras tanto, cada punto de conmutación de protección difunde periódicamente un mensaje de detección de fallo, tal como un mensaje Keep Alive (Siempre activo), a través de sus puertos de trabajo y puertos de protección, por intermedio del dominio de flujo de trabajo y del dominio de flujo de protección, respectivamente, al puerto de trabajo y al puerto de protección del punto de conmutación de protección en reposo que se acopla en la red con soporte de conmutación de protección y comprueba el estado operativo de la ruta de protección/trabajo local y el estado de la ruta de protección/trabajo distante. En un tiempo de detección predeterminado, si el puerto de trabajo de un punto de conmutación de protección determinado no recibe el mensaje de detección de fallo, el punto de conmutación de protección determina que se produjo un fallo en la ruta de trabajo punto a punto entre el punto de conmutación de protección distante que transmite el mensaje de detección de fallo y el propio punto de conmutación de protección. A continuación, el punto de conmutación de protección envía un mensaje de notificación de fallo a través de su propio puerto de protección al puerto de protección del punto de conmutación de protección distante que conecta la ruta de trabajo en donde se produjo el fallo. El punto de conmutación de protección distante, que recibe el mensaje de notificación de fallo, conmuta los paquetes de datos proporcionados a través de la ruta, en la que se produjo el fallo, al dominio de flujo de protección y transmite los paquetes de datos a través de su propio puerto de protección por intermedio del dominio de flujo de protección en función de la información de dirección contenida en el mensaje de notificación de fallo. En las formas de realización de la presente invención, el punto de conmutación de protección distante se refiere a otro punto de conmutación de protección que se acopla al punto de conmutación de protección a través de una ruta. Dicho de otro modo, el punto de conmutación de protección y su punto de conmutación de protección distante son dos dispositivos de conmutación de protección que son puntos de conmutación de protección distante entre sí y están acoplados a una ruta en el dominio de flujo de trabajo y también acoplados a una ruta en el dominio de flujo de protección. El punto de conmutación de protección puede referirse también como un punto de conmutación de protección distante.

Las formas de realización de la presente invención comprenden, además, lo que sigue. En un tiempo de detección predeterminado, si el puerto de trabajo anterior del punto de conmutación de protección, que determina la producción de un fallo en una ruta, recibe, una vez más, un mensaje de detección de fallo a través de la ruta en la que se produjo el fallo, el punto de conmutación de protección determina que la ruta retorna a la condición normal. Y el punto de conmutación de protección envía un mensaje de notificación de reparación del fallo a través de su puerto de trabajo al puerto de trabajo del punto de conmutación de protección distante al que se acopla la ruta. El punto de conmutación de protección que recibe el mensaje de notificación de reparación del fallo puede conmutar los paquetes de datos enviados a través del dominio del flujo de protección por intermedio de su puerto de protección, al dominio de flujo de trabajo y transmite los paquetes de datos a través de su puerto de trabajo.

Según las formas de realización de la presente invención, si el puerto de protección de un punto de conmutación de protección determinado no ha recibido el mensaje de detección de fallo en un tiempo de detección predeterminado, su procedimiento de procesamiento es similar al método anterior, que se omite aquí para mayor brevedad.

La finalidad, las soluciones técnicas y las ventajas con respecto a las formas de realización de la presente invención se harán más evidentes haciendo referencia a la siguiente descripción de las formas de realización, cuando se toman con referencia a los dibujos adjuntos.

La Figura 2 es una ilustración de la configuración para una red sin conexión con soporte de conmutación de protección, según una forma de realización de la presente invención. En la red con soporte de conmutación de protección, un grupo de acceso de VLAN está constituido por un grupo de puntos de acceso de VLAN con el mismo identificador VLAN ID. Cada punto de acceso de red VLAN o el punto de conmutación de protección, es un miembro en el grupo de acceso de red VLAN. Según se ilustra en la Figura 2, el dominio de flujo completo, objeto de protección, proporciona un servicio de suministro de red VLAN correspondiente para un grupo de acceso VLAN. Suponiendo que el identificador VLAN ID es VLAN1, PSP1- PSP4 son cuatro dispositivos de borde o cuatro puntos de acceso de VLAN en el grupo de acceso VLAN y cada punto de acceso VLAN tiene dos puertos: el puerto de trabajo W y el puerto de protección P. Los enlaces internos entre los puertos de trabajo W, según se indica por la línea de trazos, interactúan entre sí en el dominio de flujo de trabajo. Los enlaces internos entre cada puerto de protección P, según se indica por la línea de puntos y trazos, interactúan entre sí en el dominio de flujo de protección. El dominio de flujo de trabajo y el dominio de flujo de protección tienen sus nodos y enlaces separados. Cuando el dominio de flujo de trabajo o el dominio de flujo de protección reenvía los datos basados en el entorno del árbol de expansión, la topología de dicho árbol no varía con el fallo. La información de la red, con soporte de conmutación de protección, según se ilustra en el diagrama de configuración de la Figura 2, comprende lo que sigue:

(1) La configuración de la información local para cada punto de acceso VLAN en el grupo de acceso VLAN. La información local incluye un identificador ID de puerto de trabajo, un identificador ID de puerto de protección, la dirección de Control de Acceso a Medios de Soporte (MAC) del punto de acceso de red VLAN y la dirección de multidifusión del grupo de acceso VLAN.

(2) La configuración de la información distante para cada punto de acceso VLAN en el grupo de acceso VLAN. La información distante incluye las direcciones MAC de los otros puntos de acceso VLAN en el mismo grupo de acceso VLAN.

5 Las tablas 1 a 4 ilustran, respectivamente, la configuración de PSP1 – PSP4 en VLAN1, según se ilustra a continuación, para mayor brevedad, la dirección de multidifusión del grupo de acceso VLAN se omite en esta descripción.

Puerto de trabajo local	Puerto de protección local	Dirección MAC de acceso de VLAN local	Dirección MAC de acceso de VLAN distante
W1	P1	MAC1	MAC2, MAC3, MAC4

10 **Tabla 1**

Puerto de trabajo local	Puerto de protección local	Dirección MAC de acceso de VLAN local	Dirección MAC de acceso de VLAN distante
W2	P2	MAC2	MAC1, MAC3, MAC4

15 **Tabla 2**

Puerto de trabajo local	Puerto de protección local	Dirección MAC de acceso de VLAN local	Dirección MAC de acceso de VLAN distante
W3	P3	MAC3	MAC1, MAC2, MAC4

20 **Tabla 3**

Puerto de trabajo local	Puerto de protección local	Dirección MAC de acceso de VLAN local	Dirección MAC de acceso de VLAN distante
W4	P4	MAC4	MAC, MAC2, MAC3

25 **Tabla 4**

25 Si a cada punto de acceso de VLAN se le ha asignado un identificador respectivo, también referido como ID de Punto de Entidad de Mantenimiento (MEP ID). Según la norma de IEEE con respecto al estándar OAM, el identificador MEP ID está contenido en el mensaje de OAM para identificar el punto de entidad de mantenimiento. Entonces, la configuración de la información de la red con soporte de conmutación de protección, según una forma de realización de la presente invención, puede comprender, además, la configuración de un identificador MEP ID local o un identificador MEP ID del punto de acceso de VLAN, para cada punto de acceso de VLAN e información de MEP ID distante o identificadores MEP IDs para otros puntos de acceso de VLAN en el mismo grupo de acceso VLAN.

30 Una vez configurada la red con soporte de conmutación de protección, el grupo de acceso VLAN puede comenzar a funcionar. En condiciones normales, el punto de acceso de VLAN envía/recibe paquetes de datos a través del dominio de flujo de trabajo por intermedio de su puerto de trabajo. Mientras tanto, cada punto de acceso de VLAN, en el grupo de acceso VLAN, realiza periódicamente un procedimiento de detección de fallo. La puesta en práctica del procedimiento de detección de fallo se detalla a continuación.

35 El punto de acceso de VLAN difunde el mensaje KA a través de su puerto de trabajo y de su puerto de protección periódicamente, por ejemplo, a un intervalo periódico. El mensaje KA comprende la dirección de origen, la dirección de destino y el identificador VLAN ID del grupo de acceso VLAN. La dirección de destino es la dirección de multidifusión del grupo de acceso VLAN y la dirección de origen es la dirección MAC de acceso de VLAN para el punto de acceso de VLAN.

40 Los puntos de acceso de VLAN comprueban sus rutas de trabajo locales y rutas de protección locales, respectivamente, en el tiempo de detección predeterminado. Estas rutas son todas ellas rutas punto a punto. Para un punto de acceso VLAN determinado, una ruta de trabajo local es una ruta a través de la cual un punto de acceso de VLAN distante envía datos, a través del dominio de flujo de trabajo, por intermedio de un puerto de trabajo al puerto de trabajo de este punto de acceso de VLAN. Una ruta de protección local es una ruta a través de la cual un punto de acceso de VLAN distante envía datos a través del dominio de flujo de protección por intermedio de un puerto de protección al puerto de protección de este punto de acceso de red VLAN.

Los puntos de acceso de VLAN comprueban sus rutas de trabajo distantes y sus rutas de protección distantes, respectivamente. Estas rutas son todas ellas rutas del tipo punto a punto. Para un punto de acceso de VLAN determinado, una ruta de trabajo distante es una ruta a través de la cual el punto de acceso de VLAN envía datos a través del dominio de flujo de trabajo por intermedio del puerto de trabajo, a un punto de acceso de VLAN distante y llega a un puerto de trabajo del punto de acceso de VLAN distante. Una ruta de protección distante, es una ruta a través de la cual el punto de acceso de VLAN envía datos a través del dominio de flujo de protección, por intermedio del puerto de protección, a un puerto de protección de un punto de acceso de VLAN distante y llega a un puerto de protección del punto de acceso de VLAN distante. El punto de acceso de VLAN obtiene su estado de ruta de trabajo distante y el estado de ruta de protección distante en función del estado de la ruta de trabajo local o del estado de la ruta de protección local del punto de acceso de VLAN distante.

La Figura 3 es una ilustración de la supervisión del estado de rutas para la red con soporte de conmutación de protección, según una forma de realización de la presente invención. Según se ilustra en la Figura 3, cada punto de acceso de VLAN transmite un mensaje KA por intermedio del puerto de trabajo y del puerto de protección, periódicamente. Mientras tanto, cada punto de acceso de VLAN recibe el mensaje KA y determina si existe algún fallo producido en la ruta asociada en función del hecho de si el mensaje KA ha sido recibido en un periodo de tiempo de detección predeterminado. El mensaje KA comprende una dirección de origen, una dirección de destino y un identificador VLAN ID. La dirección de origen es la dirección MAC de acceso de red VLAN del punto de acceso de VLAN que transmite el mensaje KA. La dirección de destino es la dirección de multidifusión del grupo de acceso VLAN y el identificador VLAN ID es el VLAN ID del grupo de acceso de VLAN. La puesta en práctica detallada se describe a continuación.

El proceso de detectar el estado de la ruta de trabajo es como sigue:

- 1) Cuando un punto de acceso de VLAN no ha recibido un mensaje KA desde un punto de acceso de VLAN distante, en su puerto de trabajo/protección, dentro de un tiempo de detección predeterminado, se determina que se ha producido un fallo local en una ruta local correspondiente. El estado de trabajo de la ruta es, de este modo, registrado como "FALLO". El punto de acceso de VLAN envía un mensaje de notificación de fallo de ruta de trabajo al punto de acceso de VLAN distante. El mensaje de notificación de fallo de ruta de trabajo comprende una dirección de origen, una dirección de destino y un identificador VLAN ID. La dirección de destino es la dirección MAC de acceso de VLAN del punto de acceso de VLAN distante. La dirección de origen es la dirección MAC de acceso VLAN del punto de acceso de red VLAN.
- 2) Cuando un punto de acceso de red VLAN recibe un mensaje KA desde un punto de acceso de VLAN distante determinado, en su puerto de trabajo/protección, en un tiempo de detección predeterminado, pero el estado de trabajo de la ruta local correspondiente es "FALLO", es decir, se produjo un fallo una vez y luego, el punto de acceso de VLAN envía una notificación de reparación de fallo de la ruta de trabajo por intermedio del puerto de trabajo al punto de acceso de VLAN distante y el estado de trabajo de la ruta se registra como "NORMAL". La notificación de reparación de fallo de la ruta de trabajo incluye una dirección de origen, una dirección de destino y un identificador VLAN ID. La dirección de destino es la dirección MAC de acceso del punto de acceso de VLAN distante. La dirección de origen es la dirección MAC de acceso de red VLAN del punto de acceso de red VLAN.
- 3) Cuando un punto de acceso de VLAN recibe un mensaje de notificación de fallo de ruta de trabajo o un mensaje de notificación de reparación de fallo de la ruta de trabajo, el punto de acceso de VLAN determina la ruta en donde se produjo el fallo o la reparación del fallo distante, en función del mensaje de notificación de fallo o del mensaje de notificación de reparación de fallo y determina el estado de la ruta como "FALLO" o "NORMAL".

El proceso para detectar el estado de la ruta de protección es idéntico al proceso anterior para detectar el estado de la ruta de trabajo, con la ruta de trabajo anterior simplemente sustituida por la ruta de protección.

La Figura 4 es una ilustración de la detección del estado de fallo de la ruta para la red, con soporte de conmutación de protección, según una forma de realización de la presente invención. A modo de ejemplo, se ilustra el proceso de detección de fallo con referencia a la Figura 4. En la Figura 4, se utiliza una línea de trazo continuo unidireccional para indicar la dirección de transmisión del mensaje KA que se transmite periódicamente. Una línea de trazos unidireccional se utiliza para indicar la dirección de transmisión del mensaje de notificación de fallo. Una cruz "X" se utiliza para indicar que el enlace está en condición defectuosa.

Según se ilustra en la Figura 4, el punto de acceso PSP1 de VLAN 1 envía un mensaje KA, periódicamente, a través de su puerto de trabajo y de su puerto de protección. En el punto de acceso PSP2 de red VLAN 1, puesto que el enlace está en condición defectuosa, el PSP2 no puede recibir el mensaje KA procedente del punto PSP1 distante en su puerto de trabajo. En consecuencia, se determina que se ha producido un fallo en la ruta de trabajo entre el PSP1 y el extremo local. A continuación, el PSP2 envía un mensaje de notificación de fallo a través de su puerto de protección al puerto de protección del PSP1. Después de recibir el mensaje de notificación de fallo, el PSP1 puede determinar que se ha

producido un fallo distante en la ruta de trabajo correspondiente en función de la información de dirección contenida en el mensaje de notificación de fallo.

5 Puesto que la dirección de origen del mensaje KA anterior comprende una dirección MAC de acceso de VLAN, una tabla de reenvío de rutas de datos asociada con la dirección MAC de acceso de VLAN se puede establecer en el dominio de flujo de trabajo y en el dominio de flujo de protección mediante autoaprendizaje. La puesta en práctica del método de autoaprendizaje es bien conocida por los expertos en esta materia. Por consiguiente, la puesta en práctica del método de autoaprendizaje se omite en esta descripción para mayor brevedad. En lugar del aprendizaje de la dirección, la tabla de reenvío de rutas de datos puede establecerse también utilizando un protocolo de control. Por ejemplo, un Protocolo de Registros Múltiples (MRP) se puede utilizar para registro de la dirección MAC de acceso de VLAN y una tabla de reenvío de rutas de datos se predefine en el dominio de flujo de trabajo y en el dominio de flujo de protección. Es decir, la tabla de reenvío de rutas de datos de la dirección MAC del acceso de VLAN se establece propagando el mensaje de registro, que transmite la dirección MAC del acceso de VLAN, a lo largo del árbol operativo.

15 Conviene señalar que los puntos de acceso de VLAN, según las formas de realización de la presente invención, están todavía en soporte del método de detección de fallo existente, tal como agregación de fallos, desadaptación, etc.

20 En una forma de realización de la presente invención, diferentes grupos de acceso VLAN pueden permitirse, además, que tengan acceso a diferentes dominios del flujo de trabajo y dominios del flujo de protección. Por ejemplo, el dominio de flujo de trabajo y el dominio de flujo de protección, accedidos por un grupo de acceso VLAN, son el dominio de flujo de protección y el dominio de flujo de trabajo accedidos por otro grupo de acceso VLAN. Además, en una forma de realización de la presente invención, se permite a un punto de conmutación de protección funcionar como puntos de acceso VLAN múltiples, que pertenecen a diferentes grupos de acceso VLAN. Dicho de otro modo, la información de localización y la información distante de una pluralidad de diferentes grupos de acceso VLAN se pueden configurar en un solo punto de conmutación de protección. Según el método, una dirección MAC de acceso de VLAN respectiva se puede configurar para el puerto de trabajo y el puerto de protección en cada punto de acceso de red VLAN.

25 Lo que antecede describe la puesta en práctica de la configuración de la red con soporte de conmutación de protección y el método de detección de fallo con respecto al método de conmutación de protección, según las formas de realización de la presente invención. La finalidad de la detección del fallo es conmutar los paquetes de datos transmitidos, a través del enlace en el que se produjo el fallo, a un enlace normal para continuidad de la transmisión.

30 Por ejemplo, en donde el punto de conmutación de protección es el punto de acceso de VLAN, el procesamiento de los paquetes de datos a transmitirse, comprende los tres aspectos siguientes:

35 1) Encapsulado de MAC.

40 Para los paquetes de datos procedentes de fuera de la red con soporte de conmutación de protección, para encapsular la cabecera de MAC exterior, la dirección de origen de la cabecera de MAC exterior es la dirección MAC de acceso de VLAN del punto de acceso de VLAN que transmite los paquetes de datos y la dirección de destino es la dirección MAC de acceso de VLAN del punto de acceso de VLAN distante que recibe los paquetes de datos.

45 La cabecera MAC externa se puede determinar en función de una regla de mapeado predeterminada de la dirección MAC. Por ejemplo, aprendiendo la dirección de origen de la cabecera MAN interior y la dirección de origen de la cabecera MAC exterior del paquete de datos desde el extremo distante, se puede obtener una tabla de mapeado que almacena la dirección MAC externa y la dirección MAC interna. Por ejemplo, en donde una dirección MAC de acceso distante A efectúa el mapeado de una dirección MAC interna B, si un paquete de datos llega a un nodo de borde a través del dominio de flujo de borde y si la dirección de destino del paquete de datos es la dirección MAC denominada B, en tal caso, el nodo de borde puede determinar el nodo distante asociado con la dirección MAC, denominada A, a la que necesita transmitirse el paquete de datos mediante búsqueda en la tabla de mapeado. La dirección de la cabecera externa, encapsulada para el paquete de datos, es la dirección MAC, denominada A. La puesta en práctica del encapsulado de la cabecera de MAC, el autoaprendizaje del mapeado de direcciones MAC son operaciones bien conocidas para los expertos en esta materia, por lo que se omitirá en esta descripción con fines de brevedad.

50 Cuando no se puede determinar la dirección MAC de acceso de VLAN del punto de acceso de VLAN distante, la dirección MAC de destino de la cabecera MAC externa es una dirección de difusión o una dirección de multidifusión asignada al grupo de acceso VLAN.

55 2) Encapsulado de VLAN TAG.

60 Se pueden utilizar dos métodos para determinar si se requiere el encapsulado de VLAN TAG para el paquete de datos. El primer método consiste en encapsular un VLAN TAG externo para el paquete de datos, según la información de configuración predeterminada, que incluye el identificador VLAN ID de acceso. La VLAN TAG incluye la información de VLAN ID. El segundo método consiste en que si la VLAN TAG externa original en el paquete de datos ha incluido ya la información de VLAN ID de acceso correspondiente, no se realizará el encapsulado en el paquete de datos.

65

3) Transmisión del paquete de datos.

(1) Para el paquete de datos que ha sido encapsulado con la información del identificador VLAN ID, si la dirección de destino de la cabecera de MAC es una dirección de difusión o una dirección de multidifusión, el procesamiento del paquete de datos de difusión o de multidifusión se realiza como sigue.

Si ninguna de las rutas de trabajo distantes asociadas con el grupo de acceso de VLAN, que se identifica por el VLAN ID, ha encontrado un fallo distante, el paquete de datos se transmite por intermedio del puerto de trabajo. Si al menos una ruta de trabajo distante, asociada con el grupo de acceso VLAN identificado por el identificador VLAN ID, ha encontrado un fallo distante y ninguna de las rutas de protección distantes, asociadas con el grupo de acceso VLAN ha encontrado un fallo distante, el paquete de datos se transmite por intermedio del puerto de protección. Si al menos una ruta distante, en el dominio de flujo de trabajo, ha encontrado un fallo distante y al menos una ruta de protección, en el dominio de flujo de protección, ha encontrado un fallo, el paquete de datos se puede eliminar o el paquete de datos se puede transmitir a través del puerto de trabajo o del puerto de protección.

(2) Para el paquete de datos que ha sido encapsulado con el identificador VLAN ID que también ha sido encapsulado, si la dirección de destino de la cabecera de MAC es una dirección de unidifusión, la dirección de unidifusión es la dirección MAC de acceso de VLAN de un punto de acceso de VLAN distante en el grupo de acceso de VLAN. El procesamiento de un paquete de datos de unidifusión se realiza como sigue.

Una ruta de trabajo distante y una ruta de protección distante, que comienzan desde el extremo local, se determinan en función de la dirección MAC de acceso VLAN del punto de acceso de VLAN distante. Si la ruta de trabajo distante no tiene ningún fallo, el paquete de datos se transmite a través del puerto de trabajo. Si la ruta de trabajo distante presenta un fallo, pero la ruta de protección distante no tiene ningún fallo, el paquete de datos se transmite a través del puerto de protección. Si la ruta de trabajo distante y la ruta de protección distante presentan fallos, se elimina el paquete de datos.

Conviene señalar que para cada punto de conmutación de protección, se puede preconfigurar una relación de mapeado entre la dirección MAC de destino del paquete de datos y la dirección MAC de acceso de VLAN de destino (es decir, la dirección MAC del acceso de VLAN del punto de acceso de VLAN distante) antes de que se reciba el paquete de datos desde fuera de la red con soporte de conmutación de protección. En este caso, el procesamiento del paquete de datos solamente comprende los procesos anteriores 2) y (1) del proceso anterior 3). El proceso (2) del proceso anterior 3) se presenta como sigue.

La dirección MAC del punto de conmutación de protección distante se puede obtener mediante la búsqueda de la relación de mapeado preconfigurada. A continuación, la ruta de trabajo distante y la ruta de protección distante correspondiente se pueden determinar basándose en la dirección MAC del punto de conmutación de protección distante. Si la ruta de trabajo distante no presenta ningún fallo, el paquete de datos se transmite a través del puerto de trabajo. Si la ruta de trabajo distante presenta un fallo, pero la ruta de protección no tiene ningún fallo, el paquete de datos se transmite a través del puerto de protección. Si la ruta de trabajo y la ruta de protección distantes presentan fallos, se elimina el paquete de datos. Además, conviene señalar que, con el fin de evitar el problema de inundación operativa causado por la conmutación de protección, un protocolo de control, tal como MRP, se puede utilizar para el registro de la dirección MAC de destino de los datos de servicio con el fin de predefinir una tabla de reenvío de rutas en el dominio de flujo de trabajo y en el dominio de flujo de protección.

Tomando como ejemplo un grupo de acceso de VLAN, el proceso de transmitir los paquetes de datos en situación normal y cuando se produce un fallo, en la red sin conexión, con soporte de conmutación de protección, se describe a continuación haciendo referencia a la descripción de las formas de realización.

La Figura 5a es una ilustración de la transmisión de paquetes de datos de unidifusión cuando la red, con soporte de conmutación de protección, está en una condición operativa normal, según una forma de realización de la presente invención. Según se ilustra en la Figura 5a, la ruta de transmisión del paquete de datos de unidifusión transmitido desde el punto de acceso PSP1 de VLAN 1 para el punto de acceso PSP2 de VLAN1 se indica por una flecha única en negrillas. La ruta de transmisión del paquete de datos de unidifusión, transmitido desde el punto de acceso PSP1 de VLAN1 al punto de acceso PSP3 de VLAN1, se indica por la flecha única de trazo continuo. Los datos se transmiten a lo largo de las rutas anteriores por intermedio del puerto de trabajo y a través del dominio de flujo de trabajo.

La Figura 5b es una ilustración de la transmisión de paquetes de datos de unidifusión en el caso de que la red, con soporte de conmutación de protección, esté en condición defectuosa, según una forma de realización de la presente invención. Según se ilustra en la Figura 5b, se supone que el enlace, en donde aparece X, se detecta como estando en condición defectuosa. Una vez informado PSP1 de la notificación de fallo, el PSP1 conmutará los paquetes de datos de unidifusión, transmitidos desde el propio PSP1 al punto de acceso PSP2 de la red VLAN1, a una ruta en el dominio de flujo de protección, en donde los paquetes de datos se transmiten desde el puerto de protección de PSP1 al puerto de protección de PSP2, según se ilustra por una flecha en negrillas en la Figura 5b. Los paquetes de datos transmitidos desde el punto PSP1 al punto PSP3 siguen todavía la ruta original y se transmiten a través del dominio de flujo de trabajo, según se ilustra por la flecha única de trazo continuo en la Figura 5b.

La Figura 6a es una ilustración de la transmisión de paquetes de datos de difusión cuando la red, con soporte de conmutación de protección, está en una condición normal, según una forma de realización de la presente invención. La ruta de trabajo es idéntica a la ilustrada en la Figura 5a, por lo que se omite en esta descripción con fines de brevedad.

5 La Figura 6b es una ilustración de la transmisión de paquetes de datos de difusión en el caso en que la red con soporte de conmutación de protección esté en una condición defectuosa según una forma de realización de la presente invención. Según se ilustra en la Figura 6b, se supone que el enlace en donde aparece X se detecta como defectuoso. Una vez informado el punto PSP1 de la notificación del fallo, el PSP1 conmutará los paquetes de datos de difusión, transmitidos desde el PSP1 al punto de acceso PSP2 de la red VLAN1, a una ruta en el dominio de flujo de protección en  
10 donde los paquetes de datos se transmiten desde el puerto de protección de PSP1 al puerto de protección de PSP2, según se ilustra por la flecha única en negrillas en la Figura 6b. Mientras tanto, el PSP1 conmuta los paquetes de datos de difusión, transmitidos desde el punto PSP1 al punto de acceso PSP3 de VLAN a una ruta en el dominio de flujo de protección, en donde los paquetes de datos se transmiten desde el puerto de protección de PSP1 al puerto de protección de PSP3, según se ilustra por la flecha única de trazo continuo.

15 Como puede deducirse de las formas de realización anteriores, para paquetes de datos transmitidos en el mismo grupo de acceso de VLAN, cuando se produce un fallo, en la mayoría de los casos, solamente una pequeña fracción del flujo de datos resulta afectada por el fallo. El método de conmutación de protección, según la presente invención, solamente conmuta los servicios que se refieren a los puntos de acceso de VLAN afectados por el fallo. Los servicios respecto a los  
20 puntos de acceso de VLAN que no han sido afectados por el fallo no serán conmutados. Por lo tanto, el servicio MP2MP es menos perjudicado por el fallo.

Las formas de realización de la presente invención dan a conocer, además, un sistema para la conmutación de protección en una red sin conexión. El sistema comprende un dominio de flujo de trabajo, un dominio de flujo de  
25 protección y una pluralidad de puntos de conmutación de protección pertenecientes a una misma instancia de servicio.

La pluralidad de puntos de conmutación de protección están situados en una red con soporte de conmutación de protección, que incluye el dominio de flujo de trabajo y el dominio de flujo de protección. Cada punto de conmutación de protección se acopla a al menos dos puntos de conmutación de protección distantes. Además, existe una ruta entre el  
30 punto de conmutación de protección y cada punto de conmutación de protección distante en el dominio de flujo de trabajo y en el dominio de flujo de protección, respectivamente.

Según las formas de realización de la presente invención, cada punto de conmutación de protección difunde un mensaje de detección de fallo a al menos dos puntos de conmutación de protección distantes, a los que se acopla. Cada punto de conmutación de protección detecta la ruta conectada entre el punto de conmutación de protección y cada punto de conmutación de protección distante en el dominio de flujo de trabajo y en el dominio de flujo de protección, respectivamente, para comprobar si existe cualquier fallo producido. Si el punto de conmutación de protección no ha recibido un mensaje de detección de fallo difundido desde el punto de conmutación de protección distante, a través de una ruta en el dominio de flujo de trabajo en un tiempo de detección predeterminado, el punto de conmutación de  
40 protección determina que se produjo un fallo en la ruta en el dominio de flujo de trabajo y envía un mensaje de notificación de fallo al punto de conmutación de protección distante en la ruta en la que se produjo el fallo, a través de una ruta en el dominio de flujo de protección. Si el punto de conmutación de protección no ha recibido un mensaje de detección de fallo difundido desde el punto de conmutación de protección distante, a través de una ruta en el dominio de flujo de protección en un tiempo de detección predeterminado, el punto de conmutación de protección determina que se produjo un fallo a lo largo de la ruta en el dominio de flujo de protección y envía un mensaje de notificación de fallo al punto de conmutación de protección distante, en la ruta en la que se produjo el fallo, a través de una ruta en el dominio de flujo de trabajo. Después de que el punto de conmutación de protección distante reciba el mensaje de notificación de fallo, a través de la ruta en el dominio de flujo de trabajo, conmuta el servicio en la instancia de servicio, que se está transmitiendo a lo largo de la ruta en la que se produjo el fallo y cuya dirección de destino es la dirección de origen del  
50 mensaje de notificación de fallo, a una ruta en el dominio de flujo de trabajo para una nueva entrega. Después de que el punto de conmutación de protección reciba el mensaje de notificación de fallo transmitido a través de la ruta en el dominio de flujo de protección, el servicio que fue anteriormente proporcionado a través de la ruta en la que se produjo el fallo se proporciona ahora a través de la ruta en el dominio de flujo de protección.

55 Según la presente forma de realización de la invención, una tabla de reenvío de rutas se almacena por anticipado en el punto de conmutación de protección. El servicio conmutado será reenviado en función de la tabla de reenvíos de rutas.

Si el punto de conmutación de protección recibe un mensaje de detección de fallo, desde el punto de conmutación de protección distante a partir de la ruta en donde fue detectado anteriormente un fallo, la ruta en donde fue detectado  
60 anteriormente el fallo se considera como estando reparada. Y un mensaje de notificación de reparación de fallo se transmite al punto de conmutación de protección distante a través de la ruta en donde se detectó anteriormente el fallo. El punto de conmutación de protección distante determina la ruta en la que se realizó la reparación del fallo en función de la información de dirección de origen en el mensaje de notificación de reparación del fallo y proporciona el servicio conmutado a través de la ruta objeto de reparación de fallo.

65

Las formas de realización de la presente invención dan a conocer, además, un dispositivo de conmutación de protección que pertenece a una misma instancia de servicio junto con al menos dos dispositivos de conmutación de protección. Cada dispositivo de conmutación de protección está situado en una red con soporte de conmutación de protección, que incluye el dominio de flujo de trabajo y el dominio de flujo de protección. Cada punto de conmutación de protección se acopla a al menos dos dispositivos de conmutación de protección distantes. Una ruta existe entre el dispositivo de conmutación de protección y cada dispositivo de conmutación de protección distante, en el dominio de flujo de trabajo y en el dominio de flujo de protección, respectivamente. El dispositivo comprende un primer módulo configurado para difundir periódicamente un mensaje de detección de fallo, a través de rutas en el dominio de flujo de trabajo y un dominio de flujo de protección a al menos dos dispositivos de conmutación de protección distantes que se acoplan a las rutas. Si un mensaje de detección de fallo no ha sido recibido desde una ruta en el dominio de flujo de trabajo en un tiempo de detección predeterminado, se determina que se produjo un fallo en la ruta en el dominio de flujo de trabajo. Si un mensaje de detección de fallo no ha sido recibido desde una ruta en el dominio de flujo de protección en un tiempo de detección predeterminado, se determina que se produjo un fallo en la ruta en el dominio de flujo de protección. El dispositivo comprende, además, un segundo módulo. Si el primer módulo determina que se produce un fallo en la ruta en el dominio de flujo de trabajo, el segundo módulo envía un mensaje de notificación de fallo a través de una ruta en el dominio de flujo de protección y entrega el servicio a través de una ruta en el dominio de flujo de protección, en donde la ruta en el dominio de flujo de protección está acoplada al dispositivo de conmutación de protección distante, que está situado en la ruta en la que se produjo el fallo. Si el primer módulo determina que se produce un fallo en la ruta en el dominio de flujo de protección, el segundo módulo envía un mensaje de notificación de fallo a través de una ruta en el dominio de flujo de trabajo y entrega el servicio a lo largo de una ruta en el dominio de flujo de trabajo, en donde la ruta en el dominio de flujo de trabajo está acoplada al dispositivo de conmutación de protección distante, que se localiza a lo largo de la ruta en la que se produjo el fallo.

Según la presente forma de realización de la invención, el dispositivo de conmutación de protección comprende, además, un tercer módulo. Después de recibir el mensaje de notificación de fallo del dispositivo de conmutación de protección distante, a través de la ruta en el dominio de flujo de trabajo, el tercer módulo entrega el servicio, que fue anteriormente entregado a través de la ruta en la que se produjo el fallo, por intermedio de la ruta en el dominio de flujo de trabajo. Después de recibir el mensaje de notificación de fallo del dispositivo de conmutación de protección distante a través de la ruta en el dominio de flujo de protección, el tercer módulo entrega el servicio, que fue anteriormente entregado a través de la ruta en la que se produjo el fallo, por intermedio de la ruta en el dominio de flujo de protección.

Además, si el dispositivo de conmutación de protección recibe un mensaje de detección de fallo desde la ruta en donde se detectó anteriormente un fallo, dicha ruta en que se produjo el fallo se considera como reparada. El mensaje de notificación de reparación de fallo se transmite a través de la ruta en donde se detectó anteriormente el fallo. Después de que el tercer módulo del dispositivo de conmutación de protección distante reciba el mensaje de notificación de reparación de fallo, el tercer módulo determina la ruta en la que se produjo la reparación del fallo en función de la dirección de origen en el mensaje de notificación de reparación del fallo y entrega el servicio conmutado a través de la ruta en la que se produjo la reparación del fallo.

## REIVINDICACIONES

1. Un método para conmutación de protección de servicio en una red sin conexión, aplicable entre una pluralidad de puntos de conmutación de protección que pertenecen a una misma instancia de servicio, en donde la pluralidad de puntos de conmutación de protección están situados en una red con un soporte de conmutación de protección que comprende un dominio de flujo de trabajo y un dominio de flujo de protección y cada punto de conmutación de protección está acoplado a al menos dos puntos de conmutación de protección distantes y una ruta existe entre el punto de conmutación de protección y cada uno de sus puntos de conmutación de protección distantes en el dominio de flujo de trabajo y en el dominio de flujo de protección, respectivamente, y en donde el método se caracteriza porque comprende las etapas que consisten en:
- establecer una tabla de reenvío de rutas para todos los puntos de conmutación de protección en el dominio de flujo de trabajo y en el dominio de flujo de protección;
- difundir, por cada uno de los puntos de conmutación de protección, un mensaje de detección de fallo, periódicamente, hacia al menos dos puntos de conmutación de protección distantes a los que se acopla cada punto de conmutación de protección;
- determinar, por cada punto de conmutación de protección distante, que un fallo se ha producido en una ruta en el dominio de flujo de trabajo si el punto de conmutación de protección no ha recibido el mensaje de detección de fallo, difundido por el punto de conmutación de protección distante, desde la ruta situada en el dominio de flujo de trabajo dentro de un tiempo de detección predeterminado;
- determinar, por cada punto de conmutación de protección distante, que un fallo se ha producido en una ruta en el dominio de flujo de protección si el punto de conmutación de protección no ha recibido el mensaje de detección de fallo, difundido por el punto de conmutación de protección distante, desde la ruta situada en el dominio de flujo de protección dentro de un tiempo de detección predeterminado;
- enviar un mensaje de notificación de fallo, a través de la ruta en el otro dominio de flujo, al punto de conmutación de protección distante que está situado en la ruta en donde se produjo el fallo cuando cada punto de conmutación de protección detecta un fallo ocurrido en una ruta en uno de entre el dominio de flujo de trabajo y el dominio de flujo de protección y
- proporcionar un servicio en la instancia de servicio, cuya dirección de destino es la dirección de origen del mensaje de notificación de fallo, a través de la ruta en el otro dominio de flujo, en función de la tabla de reenvío de rutas, después de haber recibido el mensaje de notificación de fallo desde el punto de conmutación de protección distante.
2. El método según la reivindicación 1, caracterizado porque el punto de conmutación de protección es un punto de acceso de red de área local virtual (VLAN) y porque el establecimiento de la tabla de reenvío de rutas comprende las etapas que consisten en:
- establecer la tabla de reenvío de rutas mediante autoaprendizaje según la dirección del controlador de acceso al medio de soporte (MAC) de destino contenida en el mensaje de detección de fallo o
- utilizar un protocolo de registros múltiples (MRP) para establecer la tabla de reenvío de rutas de VLAN mediante el registro de una dirección de unidifusión.
3. El método según la reivindicación 2, caracterizado porque el punto de conmutación de protección es un punto de acceso de red de área local virtual (VLAN) y porque el método comprende, además, las etapas que consisten en:
- configurar información de la red con soporte de conmutación de protección en el punto de acceso VLAN, en donde la información de la red con soporte de conmutación de protección comprende:
- información local del punto de acceso VLAN, comprendiendo la información local una dirección MAC del punto de acceso VLAN local, una dirección de multidifusión de un grupo de acceso VLAN que comprende el punto de acceso VLAN local y al menos un punto de acceso VLAN que tiene el mismo identificador VLAN ID que el punto de acceso VLAN local y el identificador VLAN ID del grupo de acceso VLAN;
- información distante del punto de acceso VLAN, que comprende una dirección MAC de al menos un punto de acceso VLAN en el grupo de acceso VLAN con la exclusión del punto de acceso VLAN local;
- en donde el mensaje de detección de fallo comprende el identificador VLAN ID, la dirección de destino y la dirección de origen del grupo de acceso VLAN, en donde la dirección de destino es la dirección de multidifusión del grupo de acceso VLAN y la dirección de origen es la dirección MAC del punto de acceso VLAN local;

en donde la difusión del mensaje de detección comprende la difusión del mensaje de detección de fallo en función del identificador VLAN ID, la dirección de destino y la dirección de origen del grupo de acceso de VLAN incluido en el mensaje de detección de fallo.

5 **4.** El método según la reivindicación 1, caracterizado porque el punto de conmutación de protección es un punto de acceso de red de área local virtual (VLAN) y porque dicho método comprende, además, las etapas que consisten en:

configurar información de la red con un soporte de conmutación de protección en el punto de acceso VLAN, en donde la información de la red con soporte de conmutación de protección comprende:

10 información local del punto de acceso VLAN, comprendiendo la información local una dirección MAC del punto de acceso VLAN local, una dirección de multidifusión de un grupo de acceso VLAN que comprende el punto de acceso VLAN local y al menos un punto de acceso VLAN que tiene el mismo identificador VLAN ID que el punto de acceso VLAN local y el identificador VLAN ID del grupo de acceso VLAN y

15 la información distante del punto de acceso VLAN que comprende una dirección MAC de al menos un punto de acceso VLAN en el grupo de acceso VLAN con la exclusión del punto de acceso VLAN local;

20 el mensaje de notificación de fallo que comprende el identificador VLAN ID, la dirección de destino y la dirección de origen del grupo de acceso VLAN, en donde la dirección de destino es una dirección MAC del punto de acceso VLAN distante en la ruta en donde se produjo el fallo y la dirección de origen es la dirección MAC del punto de acceso VLAN local;

25 determinar la ruta en donde se produjo el fallo en función de la información de dirección de origen en el mensaje de notificación de fallo cuando el punto de acceso VLAN recibe el mensaje de notificación de fallo desde el punto de acceso VLAN distante.

30 **5.** El método según la reivindicación 1, caracterizado porque el punto de conmutación de protección es un punto de acceso de red de área local virtual (VLAN) y porque el método comprende, además, las etapas que consisten en:

configurar información de la red con un soporte de conmutación de protección en el punto de acceso VLAN, en donde la información de la red con soporte de conmutación de protección comprende:

35 información local del punto de acceso VLAN que comprende una dirección MAC del punto de acceso VLAN local, una dirección de multidifusión de un grupo de acceso VLAN que comprende el punto de acceso VLAN local y al menos un punto de acceso VLAN que tiene el mismo identificador VLAN ID que el punto de acceso VLAN local y el identificador VLAN ID del grupo de acceso VLAN, información distante del punto de acceso VLAN, que comprende: una dirección MAC de al menos un punto de acceso VLAN en el grupo de acceso VLAN, estando excluido el punto de acceso VLAN local;

40 enviar, por cada punto de acceso VLAN, un mensaje de notificación de reparación de fallo al punto de acceso VLAN distante a través de la ruta en donde se detectó anteriormente un fallo si un punto de acceso VLAN recibe el mensaje de detección de fallo desde el punto de acceso VLAN distante a través de la ruta en donde se detectó anteriormente un fallo, en donde el mensaje de notificación de reparación de fallo comprende el identificador VLAN ID, la dirección de destino y la dirección de origen del grupo de acceso VLAN, siendo la dirección de destino una dirección MAC del punto de acceso VLAN distante en la ruta en donde se detectó anteriormente un fallo y siendo la dirección de origen la dirección MAC del punto de acceso VLAN local;

50 determinar, por cada punto de acceso VLAN, la ruta en donde fue reparado el fallo según la dirección de origen contenida en el mensaje de notificación de reparación de fallo después de que un punto de acceso VLAN haya recibido el mensaje de notificación de reparación de fallo, desde la ruta en donde se detectó anteriormente un fallo y proporcionar el servicio que fue prestado a través de la ruta en el otro dominio, entre el dominio de flujo de trabajo y el dominio de flujo de protección, a través de la ruta en donde fue reparado el fallo.

55 **6.** Un sistema para conmutación de protección de servicio en una red sin conexión que comprende un dominio de flujo de trabajo, un dominio de flujo de protección y una pluralidad de puntos de conmutación de protección que pertenecen a una misma instancia de servicio, en donde la pluralidad de puntos de conmutación de protección están situados en una red con un soporte de conmutación de protección que comprende el dominio de flujo de trabajo y el dominio de flujo de protección y cada punto de conmutación de protección está acoplado a al menos dos puntos de conmutación de protección distantes y en donde existe una ruta entre el punto de conmutación de protección y cada uno de sus puntos de conmutación de protección distantes en el dominio de flujo de trabajo y en el dominio de flujo de protección, respectivamente, y en donde el sistema está caracterizado porque:

60 cada punto de conmutación de protección está configurado para:

65

## ES 2 374 314 T3

difundir periódicamente un mensaje de detección de fallo hacia al menos dos puntos de conmutación de protección distantes a los cuales está acoplado cada punto de conmutación de protección;

5 determinar que se produjo un fallo en una ruta en el dominio de flujo de trabajo si el punto de conmutación de protección no ha recibido el mensaje de detección de fallo, difundido por el punto de conmutación de protección distante, desde la ruta en el dominio de flujo de trabajo dentro de un tiempo de detección predeterminado;

10 determinar que se produjo un fallo en una ruta en el dominio de flujo de protección si el punto de conmutación de protección no ha recibido el mensaje de detección de fallo, difundido por el punto de conmutación de protección distante, desde la ruta en el dominio de flujo de protección dentro de un tiempo de detección predeterminado;

15 enviar un mensaje de notificación de fallo, a través de la ruta en el otro dominio de flujo, al punto de conmutación de protección distante, que está situado en la ruta en donde se produjo el fallo, cuando cada punto de conmutación de protección detecta un fallo que se ha producido en una ruta en un dominio entre el dominio de flujo de trabajo y el dominio de flujo de protección y

20 proporcionar un servicio en la instancia de servicio, cuya dirección de destino es la dirección de origen del mensaje de notificación de fallo, a través de la ruta en el otro dominio de flujo, en función de la tabla de reenvío de rutas después de haber recibido el mensaje de notificación de fallo desde el punto de conmutación de protección distante, en donde la tabla de reenvío de rutas se establece para todos los puntos de conmutación de protección en el dominio de flujo de trabajo y en el dominio de flujo de protección.

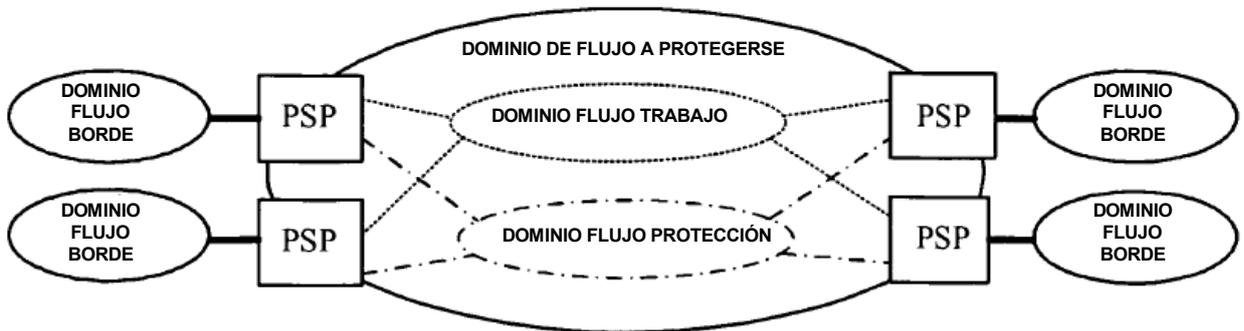


Figura 1

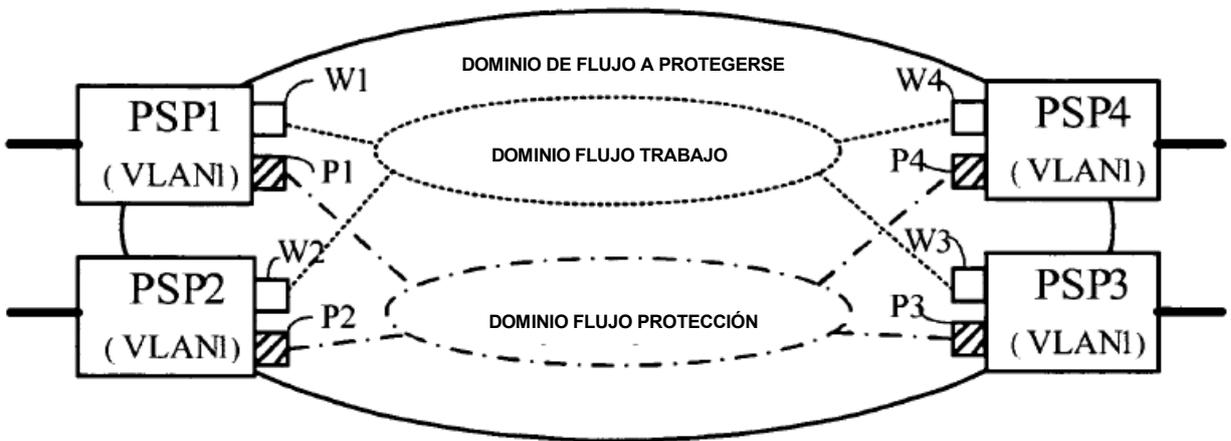


Figura 2

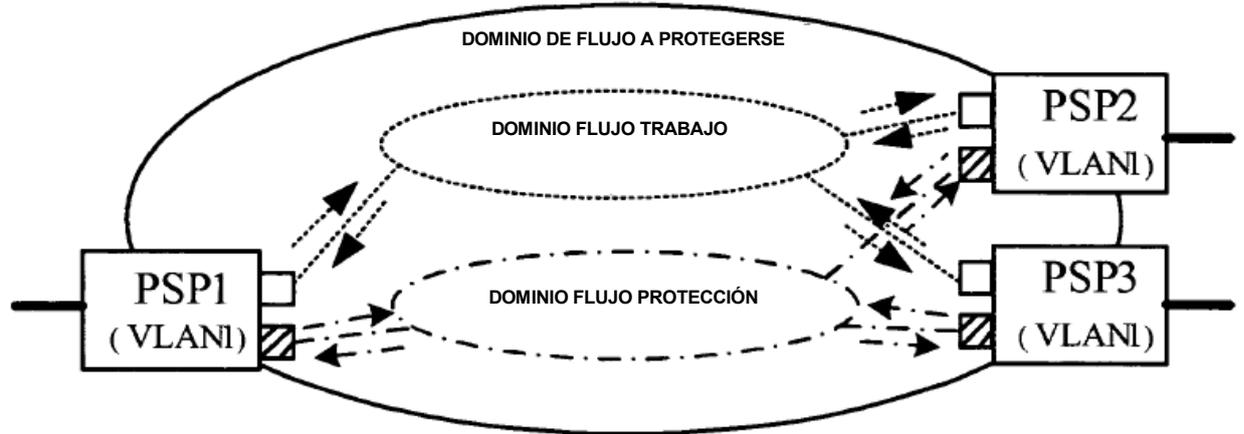


Figura 3



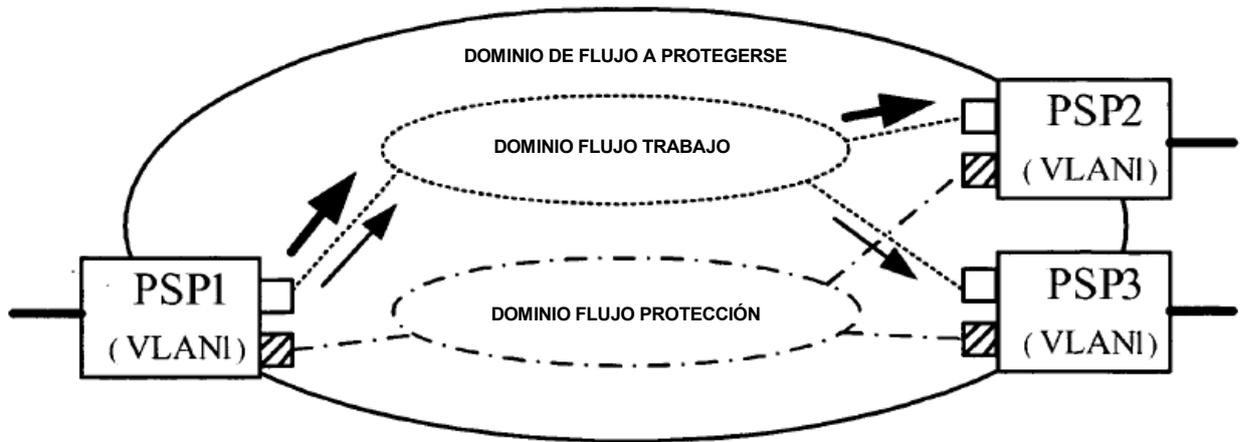


Figura 6a

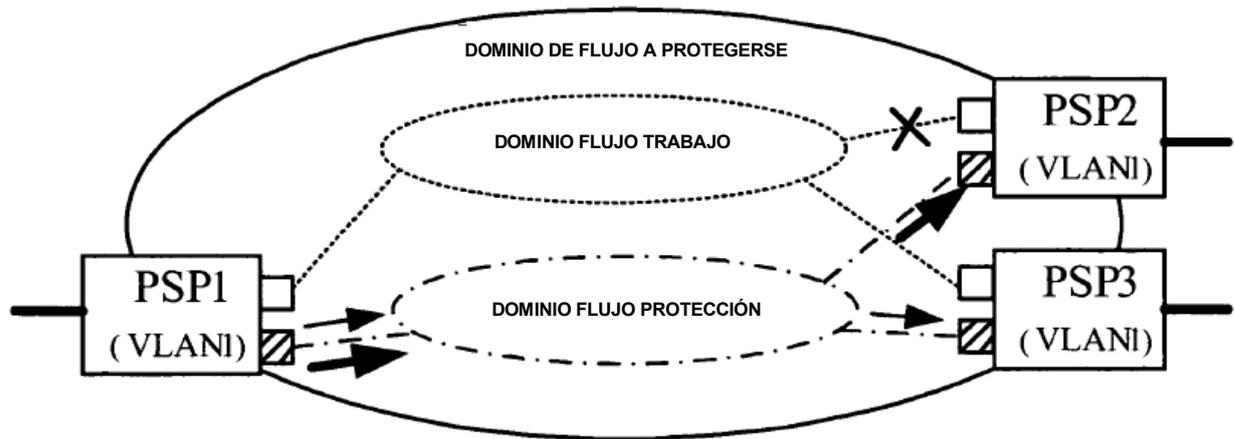


Figura 6b