(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 762 075**

(51) Int. CI.:

H04L 12/70 (2013.01)
H04L 12/64 (2006.01)
H04L 12/26 (2006.01)
H04L 12/24 (2006.01)
H04L 5/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **29.06.2013 E 17171394 (4)**

(97) Fecha y número de publicación de la concesión europea: **02.10.2019 EP 3264693**

(54) Título: **Método y sistema de protección para una red multidominio y nodo**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
22.05.2020

(73) Titular/es:

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

(72) Inventor/es:

YE, MIN y
LONG, HAO

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

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 y sistema de protección para una red multidominio y nodo.

Campo técnico

La presente invención se refiere al campo de las tecnologías de comunicaciones de redes, y en particular, a un método y sistema de protección para una red multidominio y un nodo.

Antecedentes

Para un servicio a través de múltiples dominios de red, se puede desplegar un mecanismo de protección en cada uno de los múltiples dominios de red para implementar, en forma de protección por sectores, una protección de extremo a extremo para el servicio. Para evitar un fallo en la protección del servicio cuando falla un único nodo, generalmente se utiliza una forma de interconexión de nodos duales entre dominios de red. En este caso, a diferencia de un mecanismo de protección lineal tradicional con un origen único y un destino único, existen múltiples nodos de origen y/o múltiples nodos de destino en un único dominio de protección.

En el mecanismo de protección de red multidominio actual, se deben configurar múltiples trayectos de protección en un nodo de conmutación de protección para implementar la protección en forma de multiorigen y/o multidestino en un dominio de red único. Cada trayecto de protección conecta un origen diferente y un destino diferente, de manera que la conmutación de protección se puede implementar de manera eficaz para un servicio protegido cuando falla una red multidominio. Este mecanismo requiere variaciones en funciones del nodo de conmutación de protección. Sin embargo, en un lado de acceso al servicio, un servicio accede a un red a través de un nodo de acceso al servicio único, y el nodo de acceso al servicio generalmente solo admite el mecanismo de protección lineal de origen único/destino único tradicional. Debido a que existe una gran cantidad de nodos de acceso al servicio en el lado de acceso, en el mecanismo de protección actual, una gran cantidad de nodos de acceso al servicio deben ser reconstruidos y actualizados para admitir protección en múltiples nodos de origen y/o nodos de destino, lo que conlleva una implementación de dispositivo compleja y costes de dispositivo altos.

El documento US 2005/249119 se refiere a un mecanismo de indicación y supresión de alarma (AIS) en una red OAM Ethernet.

Compendio

Las realizaciones de la presente invención ofrecen un método y sistema para una red multidominio, y un nodo, con el fin de resolver un problema en la técnica anterior en que una gran cantidad de nodos de acceso al servicio deben reconstruirse y actualizarse, lo que conlleva una implementación de dispositivo compleja y costes de dispositivo altos.

Las realizaciones de la presente invención utilizan las siguientes soluciones técnicas:

Un primer aspecto de la presente invención ofrece un método de protección para una red multidominio, donde la red multidominio incluye un primer dominio y un segundo dominio, donde el primer dominio y el segundo dominio se intersecan en un primer nodo y un segundo nodo; y el método incluye:

después de que el segundo nodo detecta que un primer enlace falla, desconectar un primer trayecto de protección en el nodo, y conectar un primer subtrayecto y un trayecto que está dentro del segundo dominio, utiliza el segundo nodo como un punto extremo, y se utiliza para portar un servicio; y enviar, en el primer subtrayecto, un primer mensaje de supervisión de fallos que lleva la primera información de mantenimiento a un tercer nodo, donde:

la primera información de mantenimiento es la misma que la segunda información de mantenimiento llevada en un segundo mensaje de supervisión de fallos; el segundo mensaje de supervisión de fallos es enviado en el primer trayecto de protección por parte del primer nodo al tercer nodo y se utiliza para supervisar un fallo del primer trayecto de protección; el primer enlace es un enlace entre el primer nodo y el segundo nodo; el servicio es un servicio que pasa a través del primer dominio y el segundo dominio; el primer trayecto de protección está formado por el empalme del primer subtrayecto y un segundo subtrayecto y es un trayecto de protección de un primer trayecto en funcionamiento; el primer trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo y el tercer nodo dentro del primer dominio; el primer subtrayecto es un trayecto entre el segundo nodo y el tercer nodo; y el segundo subtrayecto es un trayecto que pasa a través del primer enlace y que está entre del primer nodo y el segundo nodo.

En una primera posible forma de implementación, la desconexión de un primer trayecto de protección en el nodo, y la conexión de un primer subtrayecto y un trayecto que está dentro del segundo dominio, utiliza el segundo nodo como un punto extremo, y se utiliza para portar un servicio que específicamente incluye:

desconectar el primer trayecto de protección y un segundo trayecto de protección en el nodo; y conectar el primer subtrayecto y un tercer subtrayecto, en donde el segundo trayecto de protección está formado por el empalme del tercer subtrayecto y un cuarto subtrayecto y es un trayecto de protección de un segundo trayecto en funcionamiento; el segundo trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo y un cuarto

nodo dentro del segundo dominio; el tercer subtrayecto es un trayecto entre el segundo nodo y el cuarto nodo; y el cuarto subtrayecto es un trayecto entre el primer nodo y el segundo nodo.

En referencia al primer aspecto o la primera forma de implementación posible del primer aspecto, en una segunda forma de implementación posible, la segunda información de mantenimiento incluye un identificador de un grupo de entidades de mantenimiento al que pertenece un punto extremo de mantenimiento del primer trayecto de protección, un identificador de punto extremo de grupo de entidades de mantenimiento de un punto extremo de mantenimiento del primer trayecto de protección en el primer nodo, y un identificador de punto extremo de grupo de entidades de mantenimiento de un punto extremo de mantenimiento del primer trayecto de protección en el tercer nodo.

En referencia al primer aspecto o la primera forma de implementación posible del primer aspecto, en una tercera forma de implementación posible, la segunda información de mantenimiento incluye un identificador de una asociación de mantenimiento al que pertenece un punto extremo de mantenimiento del primer trayecto de protección, un identificador de punto extremo de asociaciones de mantenimiento de un punto extremo de mantenimiento del primer trayecto de protección en el primer nodo, y un identificador de punto extremo de asociaciones de mantenimiento de un punto extremo de mantenimiento del primer trayecto de protección en el tercer nodo.

En referencia al primer aspecto o primera forma de implementación posible del primer aspecto, en una cuarta forma de implementación posible, la segunda información de mantenimiento incluye un identificador de traza de camino de supervisión de conexión en cascada en el primer trayecto de protección.

En referencia al primer aspecto, o a la primera forma de implementación posible, la segunda forma de implementación posible, la tercera forma de implementación posible, o la cuarta forma de implementación posible del primer aspecto, en una quinta forma de implementación posible, el método además incluye: antes de que el segundo nodo detecte que el primer enlace falla, reenviar, por parte del segundo nodo, el segundo mensaje de supervisión de fallos recibido al tercer nodo, y registrar la segunda información de mantenimiento llevada en el segundo mensaje de supervisión de fallos recibido.

En referencia al primer aspecto o a cualquier aspecto de la primera forma de implementación posible a la quinta forma de implementación posible del primer aspecto, en una sexta forma de implementación posible, el método además incluye: antes de que el segundo nodo detecte que el primer enlace falla, reenviar, por parte del segundo nodo, la segunda información de conmutación de protección automática recibida al tercer nodo, donde la segunda información de conmutación de protección automática es información enviada en el primer trayecto de protección por el primer nodo al tercer nodo; y después de que el segundo nodo detecta que el primer enlace falla, enviar, en el primer trayecto de protección, la primera información de conmutación de protección automática al tercer nodo.

En referencia a la sexta forma de implementación posible del primer aspecto, en una séptima forma de implementación posible, el método además incluye: antes de que el segundo nodo detecte que el primer enlace falla, reenviar, por el segundo nodo, un tercer mensaje de conmutación de protección automática recibido al primer nodo, y mantener una máquina de estado de conmutación de protección según el tercer mensaje de conmutación de protección automática, donde el tercer mensaje de conmutación de protección automática es información enviada en el primer trayecto de protección por el tercer nodo al primer nodo; y después de que el segundo nodo detecta que el primer enlace falla, detener, por parte del segundo nodo, el reenvío del tercer mensaje de conmutación de protección automática.

En referencia a la sexta forma de implementación posible o la séptima forma de implementación posible del primer aspecto, en una octava forma de implementación posible, el método además incluye: después de que el segundo nodo detecta que el primer enlace falla, cuando la tercera información de conmutación de protección automática que es enviado por parte del tercer nodo y que se reciben las solicitudes de conmutación al primer trayecto de protección, enviar, por parte del segundo nodo, un mensaje de notificación al segundo dominio, donde el mensaje de notificación se utiliza para dar la instrucción de que el segundo nodo se utilice para conectar el primer dominio y el segundo dominio.

En referencia al primer aspecto o cualquiera de la primera forma de implementación posible a la octava forma de implementación posible del primer aspecto, en una novena forma de implementación posible, el método además incluye: antes de que el segundo nodo detecte que el primer enlace falla, reenviar, por parte del segundo nodo, un tercer mensaje de supervisión de fallos recibido al primer nodo, y supervisar un fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos, donde el tercer mensaje de supervisión de fallos es un mensaje que es enviado en el primer trayecto de protección por el tercer nodo al primer nodo y que se utiliza para supervisar el primer trayecto de protección; y después de que el segundo nodo detecta que el primer enlace falla, detener, por parte del segundo nodo, el reenvío del tercer mensaje de supervisión de fallos.

Un segundo aspecto de la presente invención ofrece un nodo, que incluye una unidad de detección, una unidad de conmutación, y una unidad de procesamiento, en donde:

la unidad de detección está configurada para detectar un fallo de un primer enlace, en donde el primer enlace es un enlace entre un primer nodo y el nodo;

la unidad de conmutación está configurada para: después de que se detecta que el primer enlace falla, desconectar un primer trayecto de protección en el nodo, y conectar un primer subtrayecto y un trayecto que está dentro de un segundo dominio, utiliza el nodo como un punto extremo, y se utiliza para portar un servicio, donde el servicio es un servicio que pasa a través de un primer dominio y de un segundo dominio;

el primer dominio y el segundo dominio se intersecan en el primer nodo y el nodo; el primer trayecto de protección está formado por el empalme del primer subtrayecto y un segundo subtrayecto y es un trayecto de protección de un primer trayecto en funcionamiento; el primer trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo y un tercer nodo dentro del primer dominio; el primer subtrayecto es un trayecto entre el nodo y el tercer nodo; y el segundo subtrayecto es un trayecto que pasa a través del primer enlace y que está dentro del primer nodo y el nodo; y

la unidad de procesamiento está configurada para: después de que se detecta que el primer enlace falla, enviar, en el primer subtrayecto, un primer mensaje de supervisión de fallos que lleva una primera información de mantenimiento al tercer nodo, en donde la primera información de mantenimiento es la misma que la segunda información de mantenimiento llevada en un segundo mensaje de supervisión de fallos; y el segundo mensaje de supervisión de fallos es un mensaje que es enviado en el primer trayecto de protección por el primer nodo al tercer nodo y que se utiliza para supervisar un fallo del primer trayecto de protección.

En una primera forma de implementación posible, la unidad de conmutación está específicamente configurada para: después de que se detecta que el primer enlace falla, desconectar el primer trayecto de protección y un segundo trayecto de protección en el nodo, y conectar el primer subtrayecto y un tercer subtrayecto, donde el segundo trayecto de protección está formado por el empalme del tercer subtrayecto y un cuarto subtrayecto y es un trayecto de protección de un segundo trayecto en funcionamiento; el segundo trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo y un cuarto nodo dentro del segundo dominio; el tercer subtrayecto es un trayecto entre el nodo y el cuarto nodo; y el cuarto subtrayecto es un trayecto entre el primer nodo y el nodo.

En referencia a la primera forma de implementación posible del segundo aspecto, en una segunda forma de implementación posible, la unidad de conmutación incluye específicamente un primer puente, un primer selector, y una unidad de control, donde:

un extremo de salida del primer selector está conectado al primer subtrayecto; un primer extremo de entrada del primer selector está conectado al segundo subtrayecto; un segundo extremo de entrada del primer selector está conectado a un segundo extremo de salida del primer puente; un primer extremo de salida del primer puente está conectado al cuarto subtrayecto; un extremo de entrada del primer puente está conectado al tercer subtrayecto; y

la unidad de control está configurada para: después de que se detecta que el primer enlace falla, controlar el extremo de entrada del primer puente para desconectarlo del primer extremo de salida del primer puente y para conectarlo al segundo extremo de salida del primer puente, y controlar el extremo de salida del primer selector para desconectarlo del primer extremo de entrada del primer selector y para conectarlo al segundo extremo de entrada del primer selector.

En referencia a la segunda forma de implementación posible del segundo aspecto, en una tercera forma de implementación posible, la unidad de conmutación además incluye un segundo puente y un segundo selector, donde:

un extremo de entrada del segundo puente está conectado al primer subtrayecto; un primer extremo de salida del segundo puente está conectado al segundo subtrayecto; un segundo extremo de salida del segundo puente está conectado a un segundo extremo de entrada del segundo selector; un primer extremo de entrada del segundo selector está conectado al cuarto subtrayecto; un extremo de salida del segundo selector está conectado al tercer subtrayecto; y

la unidad de control está configurada además para: después de que se detecta que el primer enlace falla, controlar el extremo de entrada del segundo puente para desconectarlo del primer extremo de salida del segundo puente y para conectarlo al segundo extremo de salida del segundo puente, y controlar el extremo de salida del segundo selector para desconectarlo del primer extremo de entrada del segundo selector y para conectarlo al segundo extremo de entrada del segundo selector.

En referencia al segundo aspecto, o la primera forma de implementación posible, la segunda forma de implementación posible, o la tercera forma de implementación posible del segundo aspecto, en una cuarta forma de implementación posible, la unidad de procesamiento está además configurada para: antes de que se detecte que el primer enlace falla, reenviar el segundo mensaje de supervisión de fallos y una segunda información de conmutación de protección automática al tercer nodo, donde la segunda información de conmutación de protección automática es información enviada en el primer trayecto de protección por el primer nodo al tercer nodo; y después de que se detecta que el primer enlace falla, enviar, en el primer trayecto de protección, la primera información de conmutación de protección automática al tercer nodo.

En referencia a la cuarta forma de implementación posible del segundo aspecto, en una quinta forma de implementación posible, el nodo además incluye una unidad de registro, configurada para: antes de que se detecte

que el primer enlace falla, registrar la segunda información de mantenimiento llevada en el segundo mensaje de supervisión de fallos recibido.

En referencia al segundo aspecto o cualquier aspecto de la primera forma de implementación posible a la quinta forma de implementación posible del segundo aspecto, en una sexta forma de implementación posible, la unidad de procesamiento está además configurada para: antes de que se detecte que el primer enlace falla, reenviar un tercer mensaje de conmutación de protección automática recibido al primer nodo, y mantener una máquina de estado de conmutación de protección según el tercer mensaje de conmutación de protección automática, donde el tercer mensaje de conmutación de protección automática es información enviada en el primer trayecto de protección por el tercer nodo al primer nodo; y después de que se detecta que el primer enlace falla, detener el reenvío del tercer mensaje de conmutación de protección automática.

En referencia a la sexta forma de implementación posible del segundo aspecto, en una séptima forma de implementación posible, el nodo además incluye una unidad de notificación configurada para: después de que se detecta que el primer enlace falla, cuando la tercera información de conmutación de protección automática que es enviada por parte del tercer nodo y que se reciben las solicitudes de conmutación al primer trayecto de protección, enviar un mensaje de notificación al cuarto nodo, donde el mensaje de notificación se utiliza para dar la instrucción de que el nodo se utilice para conectar el primer dominio y el segundo dominio para el servicio.

En referencia al segundo aspecto o cualquiera de la primera forma de implementación posible a la séptima forma de implementación posible del segundo aspecto, en una octava forma de implementación posible, la unidad de procesamiento está además configurada para: antes de que se detecte que el primer enlace falla, reenviar un tercer mensaje de supervisión de fallos recibido al primer nodo, y supervisar un fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos, donde el tercer mensaje de supervisión de fallos es un mensaje que es enviado en el primer trayecto de protección por el tercer nodo al primer nodo y que se utiliza para supervisar el primer trayecto de protección; y después de que el primer enlace falla, detener el reenvío del tercer mensaje de supervisión de fallos.

En referencia a la octava forma de implementación posible del segundo aspecto, en una novena forma de implementación posible, la unidad de procesamiento específicamente incluye:

un tercer puente, configurado para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática; y enviar el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática a una primera unidad de mantenimiento y un segundo conmutador;

la primera unidad de mantenimiento, configurada para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática que se emiten por parte del tercer puente, mantener la máquina de estado de conmutación de protección según el tercer mensaje de conmutación de protección automática, y supervisar el fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos; regenerar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática; y enviar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática regenerados a un primer conmutador;

el primer conmutador, configurado para: reenviar, al tercer nodo, el segundo mensaje de supervisión de fallos y una segunda información de conmutación de protección automática recibidos que son enviados por el primer nodo; antes de que se detecte que el primer enlace falla, prohibir el reenvío del primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y después de que se detecta que el primer enlace falla, enviar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y

el segundo conmutador, configurado para: antes de que se detecte que el primer enlace falla, enviar el tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática recibidos al primer nodo; y después de que se detecta que el primer enlace falla, detener el envío del tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática.

En referencia a la octava forma de implementación posible del segundo aspecto, en una décima forma de implementación posible, la unidad de procesamiento específicamente incluye:

un tercer puente, configurado para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática; y enviar el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática a una primera unidad de mantenimiento y una segunda unidad de mantenimiento;

la primera unidad de mantenimiento, configurada para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática que se emiten por parte del tercer puente, mantener la máquina de estado de conmutación de protección según el tercer mensaje de conmutación de protección automática, y supervisar el fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos; regenerar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática; y enviar el primer mensaje

de supervisión de fallos y la primera información de conmutación de protección automática regenerados a un primer conmutador;

la segunda unidad de mantenimiento, configurada para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática que se emiten por parte del tercer puente, y enviar el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática a un segundo conmutador; y reenviar, al tercer nodo, el segundo mensaje de supervisión de fallos y la segunda información de conmutación de protección automática recibidos que son enviados por el primer nodo;

el primer conmutador, configurado para: antes de que se detecte que el primer enlace falla, prohibir el reenvío del primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y después de que se detecta que el primer enlace falla, enviar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y

el segundo conmutador, configurado para: antes de que se detecte que el primer enlace falla, enviar el tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática recibidos al primer nodo; y después de que se detecta que el primer enlace falla, detener el envío del tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática.

Un tercer aspecto de la presente invención ofrece un sistema de protección para una red multidominio, donde la red multidominio incluye un primer dominio y un segundo dominio, donde el primer dominio y el segundo dominio se intersecan en un primer nodo y un segundo nodo; y el sistema incluye:

el primer nodo, configurado para enviar, en un primer trayecto de protección, un segundo mensaje de supervisión de fallos que se utiliza para supervisar un fallo del primer trayecto de protección a un tercer nodo, donde el segundo mensaje de supervisión de fallos lleva una segunda información de mantenimiento;

el segundo nodo, que es el nodo según el segundo aspecto o cualquiera de las formas de implementación posibles del segundo aspecto; y

el tercer nodo, configurado para: recibir el primer mensaje de supervisión de fallos o el segundo mensaje de supervisión de fallos; y supervisar el fallo del primer trayecto de protección según el primer mensaje de supervisión de fallos o el segundo mensaje de supervisión de fallos.

Según el método y sistema de protección para una red multidominio y el nodo que se proveen en las realizaciones de la presente invención, se implementa la optimización de un trayecto de protección mediante el procesamiento solo en un nodo intersecante, de manera que los nodos no intersecantes puedan tener compatibilidad hacia atrás con un mecanismo de protección actual, reduciendo así la complejidad y costes del dispositivo.

Breve descripción de los dibujos

Para describir las soluciones técnicas en las realizaciones de la presente invención de manera más clara, a continuación se describen brevemente los dibujos que acompañan esta memoria necesarios para describir las realizaciones. Según parece, los dibujos adjuntos de la siguiente descripción simplemente muestran algunas realizaciones de la presente invención, y una persona con experiencia ordinaria en la técnica puede incluso obtener otros dibujos a partir de los dibujos adjuntos sin esfuerzos creativos.

La Figura 1 es un diagrama de flujo de un método de protección para una red multidominio según una realización de la presente invención;

la Figura 2 es un diagrama de una topología de red multidominio según una realización de la presente invención;

la Figura 3 es un diagrama de otra topología de red multidominio según una realización de la presente invención;

la Figura 4 es un diagrama de incluso otra topología de red multidominio según una realización de la presente invención;

la Figura 5 es un diagrama de bloque estructural de un nodo según una realización de la presente invención;

la Figura 6a es un diagrama de bloque estructural de una unidad de conmutación según una realización de la presente invención;

la Figura 6b es un diagrama de bloque estructural de otra unidad de conmutación según una realización de la presente invención;

la Figura 7a es un diagrama de bloque estructural de una primera subunidad de procesamiento según una realización de la presente invención;

la Figura 7b es un diagrama de bloque estructural de otra primera subunidad de procesamiento según una realización de la presente invención;

la Figura 7c es un diagrama de bloque estructural de incluso otra primera subunidad de procesamiento según una realización de la presente invención;

la Figura 8 es un diagrama de bloque estructural de otro nodo según una realización de la presente invención; y

la Figura 9 es un diagrama de bloque estructural de un sistema de protección para una red multidominio según una realización de la presente invención.

Descripción de las realizaciones

Las realizaciones de la presente invención ofrecen un método y sistema de protección para una red multidominio y un nodo. Para hacer que las soluciones técnicas en la presente invención sean más comprensibles, a continuación se describen en detalle las realizaciones de la presente invención en referencia a los dibujos que la acompañan.

Ha de quedar claro que las realizaciones descritas son simplemente algunas, pero no todas, las realizaciones de la presente invención. Todas las demás realizaciones obtenidas por una persona con experiencia ordinaria en la técnica a partir de las realizaciones de la presente invención sin esfuerzos creativos estarán comprendidas dentro del alcance de protección de la presente invención, tal y como se define en las reivindicaciones adjuntas.

En una realización de la presente invención, se muestra en la Figura 1 un diagrama de flujo de un método de protección para una red multidominio. La red multidominio incluye un primer dominio y un segundo dominio, donde el primer dominio y el segundo dominio que se intersecan en un primer nodo y un segundo nodo. El método incluye las siguientes etapas:

Etapa E101. Después de que el segundo nodo detecta que un primer enlace falla, desconectar un primer trayecto de protección en el nodo, y conectar un primer subtrayecto y un trayecto que está dentro del segundo dominio, utiliza el segundo nodo como un punto extremo, y se utiliza para portar un servicio.

Etapa E102. Enviar, en el primer subtrayecto, un primer mensaje de supervisión de fallos que lleva la primera información de mantenimiento a un tercer nodo.

La primera información de mantenimiento es la misma que la segunda información de mantenimiento llevada en un segundo mensaje de supervisión de fallos; el segundo mensaje de supervisión de fallos es enviado en el primer trayecto de protección por el primer nodo al tercer nodo y se utiliza para supervisar un fallo del primer trayecto de protección; el primer enlace es un enlace entre el primer nodo y el segundo nodo; y el servicio es un servicio que pasa a través del primer dominio y el segundo dominio.

El primer trayecto de protección está formado por el empalme del primer subtrayecto y un segundo subtrayecto y es un trayecto de protección de un primer trayecto en funcionamiento; el primer trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo y el tercer nodo dentro del primer dominio; el primer subtrayecto es un trayecto entre el segundo nodo y el tercer nodo; el segundo subtrayecto es un trayecto que pasa a través del primer enlace y está entre el primer nodo y el segundo nodo.

Específicamente, la etapa E101 puede incluir: desconectar el primer trayecto de protección y un segundo trayecto de protección en el nodo; y conectar el primer subtrayecto y un tercer subtrayecto.

El segundo trayecto de protección está formado por el empalme del tercer subtrayecto y un cuarto subtrayecto y es un trayecto de protección de un segundo trayecto en funcionamiento; el segundo trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo y un cuarto nodo dentro del segundo dominio; el tercer subtrayecto es un trayecto entre el segundo nodo y el cuarto nodo; y el cuarto subtrayecto es un trayecto entre el primer nodo y el segundo nodo.

Específicamente, la segunda información de mantenimiento puede incluir un identificador de un grupo de entidades de mantenimiento al que pertenece un punto extremo de mantenimiento del primer trayecto de protección, un identificador de punto extremo de grupo de entidades de mantenimiento de un punto extremo de mantenimiento del primer trayecto de protección en el primer nodo, y un identificador de punto extremo de grupo de entidades de mantenimiento de un punto extremo de mantenimiento del primer trayecto de protección en el tercer nodo.

De manera alternativa, la segunda información de mantenimiento puede incluir un identificador de una asociación de mantenimiento al que pertenece un punto extremo de mantenimiento del primer trayecto de protección, un identificador de punto extremo de asociaciones de mantenimiento de un punto extremo de mantenimiento del primer trayecto de protección en el primer nodo, y un identificador de punto extremo de asociaciones de mantenimiento de un punto extremo de mantenimiento del primer trayecto de protección en el tercer nodo.

De manera alternativa, la segunda información de mantenimiento puede incluir un identificador de traza de camino de supervisión de conexión en cascada en el primer trayecto de protección.

Además, el método puede incluir: antes de que el segundo nodo detecte que el primer enlace falla, reenviar, por parte del segundo nodo, el segundo mensaje de supervisión de fallos recibido al tercer nodo, y registrar la segunda información de mantenimiento llevada en el segundo mensaje de supervisión de fallos recibido.

Asimismo, el método puede además incluir: antes de que el segundo nodo detecte que el primer enlace falla, reenviar, por parte del segundo nodo, la segunda información de conmutación de protección automática recibida al tercer nodo, donde la segunda información de conmutación de protección automática es información enviada en el primer trayecto de protección por el primer nodo al tercer nodo; y después de que el segundo nodo detecta que el primer enlace falla, enviar, en el primer trayecto de protección, la primera información de conmutación de protección automática al tercer nodo.

Asimismo, el método puede además incluir: antes de que el segundo nodo detecte que el primer enlace falla, reenviar, por parte del segundo nodo, un tercer mensaje de conmutación de protección automática recibido al primer nodo, y mantener una máquina de estado de conmutación de protección según el tercer mensaje de conmutación de protección automática, donde el tercer mensaje de conmutación de protección automática es información enviada en el primer trayecto de protección por el tercer nodo al primer nodo; y

después de que el segundo nodo detecta que el primer enlace falla, detener, por parte del segundo nodo, el reenvío del tercer mensaje de conmutación de protección automática.

Asimismo, el método puede además incluir: después de que el segundo nodo detecta que el primer enlace falla, cuando la información de conmutación de protección automática que se envía por parte del tercer nodo y que se reciben las solicitudes de conmutación al primer trayecto de protección, enviar, por parte del segundo nodo, un mensaje de notificación al segundo dominio, donde el mensaje de notificación se utiliza para dar la instrucción de que el segundo nodo se utilice para conectar el primer dominio y el segundo dominio.

Asimismo, el método puede además incluir: antes de que el segundo nodo detecte que el primer enlace falla, reenviar, por parte del segundo nodo, un tercer mensaje de supervisión de fallos recibido al primer nodo, y supervisar un fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos, donde el tercer mensaje de supervisión de fallos es un mensaje que se envía en el primer trayecto de protección por el tercer nodo al primer nodo y que se utiliza para supervisar el primer trayecto de protección; y después de que el segundo nodo detecta que el primer enlace falla, detener, por parte del segundo nodo, el reenvío del tercer mensaje de supervisión de fallos.

A continuación se describe en detalle un método y sistema de protección para una red multidominio y un nodo que se proveen en las realizaciones de la presente invención.

En la Realización 1, esta realización de la presente invención ofrece un método de protección para una red multidominio. En la Figura 2 se muestra una topología de la red multidominio. La red multidominio incluye el dominio 1 y el dominio 2. El dominio 1 y el dominio 2 se intersecan en el nodo B y el nodo C. El nodo B y el nodo C se llaman "nodos intersecantes" o se pueden llamar "nodos portales" (nodo portal). El nodo A, el nodo E y el nodo F están en el dominio 1, y el nodo D, el nodo G y el nodo H están en el dominio 2.

El enlace B-C es un enlace entre el nodo B y el nodo C. El enlace B-C puede ser un enlace directo ente el nodo B y el nodo C o puede ser un enlace no directo que incluye segmentos de enlace múltiple entre el nodo B y el nodo C.

Puede haber múltiples servicios protegidos en todo el dominio 1 y el dominio 2. En esta realización, el servicio protegido 200 que pasa a través del dominio 1 y el dominio 2 se utiliza como un ejemplo para esta descripción. En condiciones normales, el servicio protegido 200 se transmite en un trayecto en funcionamiento entre el nodo A y el nodo D.

La red multidominio además incluye cuatro trayectos:

un trayecto en funcionamiento 210, que es un trayecto en funcionamiento para servicio protegido 200 entre el nodo A y el nodo B dentro del dominio 1 y que se utiliza para portar el servicio protegido 200 dentro del dominio 1, donde una ruta es A-E-B;

un trayecto en funcionamiento 220, que es un trayecto en funcionamiento para servicio protegido 200 entre el nodo B y el nodo D dentro del dominio 2 y que se utiliza para portar el servicio protegido 200 dentro del dominio 2, donde una ruta es B-G-D;

un trayecto de protección 230, que es un trayecto de protección de un trayecto en funcionamiento 210 en el dominio 1 y que está formado por el empalme del trayecto 250 y trayecto 260 en el nodo C, donde una ruta es A-F-C-B; el trayecto 250 y el trayecto 260 se pueden llamar subtrayectos de trayecto de protección 230, donde el trayecto 250 es un trayecto entre el nodo A y el nodo C, el trayecto 260 es un trayecto que pasa a través del enlace B-C y que está entre el nodo C y el nodo B, es decir, un enlace intraportal (enlace intraportal), y el empalme se puede implementar al configurar una conexión cruzada o una entrada de reenvío en el nodo C, con el fin de que el servicio se pueda reenviar de manera transparente entre el trayecto 250 y el trayecto 260; y

un trayecto de protección 240, que es un trayecto de protección de un trayecto en funcionamiento 220 en el dominio 2 y que está formado por el empalme del trayecto 270 y trayecto 280 en el nodo C, donde una ruta es B-C-H-D; el trayecto 270 y el trayecto 280 se pueden llamar subtrayectos de trayecto de protección 240, donde el trayecto 270 es un trayecto entre el nodo D y el nodo C, el trayecto 280 es un trayecto entre el nodo C y el nodo B, es decir, un enlace intraportal (enlace intraportal), y el empalme se puede implementar al configurar una conexión cruzada o una entrada de reenvío en el nodo C, con el fin de que el servicio se pueda reenviar de manera transparente entre el trayecto 270 y el trayecto 280.

En condiciones normales, el servicio protegido 200 se porta en un trayecto en funcionamiento 210 y un trayecto en funcionamiento 220, y el nodo B sirve como pasarela para implementar el reenvío del servicio protegido 200 entre el trayecto en funcionamiento 210 y el trayecto en funcionamiento 220, con el fin de implementar una conexión de extremo a extremo. El nodo B puede implementar el reenvío del servicio protegido 200 entre un trayecto en funcionamiento 210 y un trayecto en funcionamiento 220 al incorporar/excluir el servicio, o puede implementar el reenvío del servicio entre un trayecto en funcionamiento 210 y trayecto en funcionamiento 220 mediante una entrada de reenvío o una conexión cruzada.

En la presente memoria se utiliza como ejemplo una operación en el dominio 1. Los puntos extremo de mantenimiento de trayecto de protección 230 se pueden configurar en el nodo A, el nodo B, y el nodo C; especialmente para el nodo C, un punto extremo de mantenimiento configurado en ellos está en una dirección de cara al nodo A. Una máquina de estado de supervisión de conexión y una máquina de estado de conmutación de protección se ejecutan en estos puntos extremo de mantenimiento. En esta realización, se puede seleccionar una configuración de punto extremo de mantenimiento correspondiente según tecnologías de red del dominio 1 y del dominio 2: si el dominio 1 es una red Ethernet, se puede configurar un MEP (punto extremo de asociaciones de mantenimiento o punto extremo de grupo de entidades de mantenimiento) en un nodo A y un nodo B; si el dominio 1 es una red de conmutación por etiquetas multiprotocolo (conmutación por etiquetas multiprotocolo, MPLS), los MEP (punto extremo de grupo de entidades de mantenimiento) se pueden configurar en un nodo A y un nodo B; si el dominio 1 es una red de OTN, se pueden configurar puntos de supervisión TCM (supervisión de conexión en cascada) en un nodo A y un nodo B, tal y como una función ODUkT (unidad k de datos de canal óptico, subcapa de conexión escalonada).

El método específicamente incluye las siguientes etapas:

Etapa E201: El nodo B envía, en un trayecto de protección 230, un mensaje de supervisión de fallos que se utiliza para llevar segunda información de mantenimiento al nodo A, donde el mensaje de supervisión de fallos se puede utilizar para supervisar un fallo del trayecto de protección 230.

En esta realización, el nodo B puede seleccionar, según las tecnologías de red del dominio 1 y el dominio 2, un paquete o tara OAM como el mensaje de supervisión de fallos para supervisión de fallos.

Si el dominio 1 es una red Ethernet, se puede utilizar un paquete de verificación de continuidad Ethernet (verificación de continuidad, CC) para supervisar fallos. El nodo B envía, en un trayecto de protección 230, un paquete de verificación de continuidad que lleva la segunda información de mantenimiento al nodo A, donde la segunda información de mantenimiento incluye al menos la siguiente información:

1) un identificador de una asociación de mantenimiento (identificador de asociaciones de mantenimiento, MA ID) o un identificador de grupo de entidades de mantenimiento (identificador de grupo de entidades de mantenimiento, MEG ID) al cual pertenece un punto extremo de mantenimiento de trayecto de protección 230, donde el identificador se debe configurar con un mismo valor en puntos extremo de mantenimiento del nodo A y el nodo B; y

2) un identificador de punto extremo de asociaciones de mantenimiento (identificador de punto extremo de asociaciones de mantenimiento, MEP ID) o un identificador de punto extremo de grupo de entidades de mantenimiento (identificador de punto extremo de grupo de entidades de mantenimiento, MEP ID) de un punto extremo de trayecto de protección 230 en el nodo B, donde los MEP ID de los puntos extremo de mantenimiento en el nodo A y el nodo B son diferentes.

Si el dominio 1 es una red de conmutación por etiqueta multiprotocolo (conmutación por etiqueta multiprotocolo, MPLS), un paquete de verificación de continuidad y conectividad de (verificación de continuidad y conectividad, CC/CV) MPLS se pueden utilizar para supervisión de fallos. El nodo B envía, en un trayecto de protección 230, un paquete de verificación de continuidad y conectividad que lleva la segunda información de mantenimiento al nodo A, donde la segunda información de mantenimiento incluye al menos la siguiente información:

1) un identificador de un grupo de entidades de mantenimiento (identificador de grupo de entidades de mantenimiento) al cual pertenece un punto extremo de mantenimiento de trayecto de protección 230, donde el identificador se debe configurar con un mismo valor en puntos extremo de mantenimiento del nodo A y el nodo B; y

2) un identificador de punto extremo de grupo de entidades de mantenimiento de un punto extremo de mantenimiento de trayecto de protección 230 en el nodo B, donde los MEP ID de los puntos extremo de mantenimiento en el nodo A y el nodo B son diferentes.

Si el dominio 1 es una red de transporte óptico (red de transporte óptico, OTN), se puede utilizar un octeto de tara de supervisión de conexión en cascada (supervisión de conexión en cascada, TCM) para supervisión de fallos. Se debe establecer una supervisión de conexión en cascada (supervisión de conexión en cascada, TCM) para supervisar el trayecto de protección 230, y se debe configurar un identificador de traza de camino (identificador de traza de camino, TTI) de la supervisión de conexión en cascada. La segunda información de mantenimiento se completa en un octeto de tara en un bloque de datos que se envía en un trayecto de protección 230 por el nodo B al nodo A, donde la segunda información de mantenimiento que se lleva en el octeto de tara es un identificador de traza de camino, y el identificador de traza de camino puede ser uno de los siguientes identificadores:

1) un identificador de punto de acceso de origen (identificador de punto de acceso de origen, SAPI), es decir, un identificador de punto de acceso de nodo B;

2) un identificador de punto de acceso de destino (identificador de punto de acceso de destino, DAPI), es decir, un identificador de punto de acceso de nodo A; y

3) el identificador de punto de acceso de origen y el identificador de punto de acceso de destino, es decir, el identificador de punto de acceso de nodo B y el identificador del punto de acceso de nodo A.

Etapa E202: El nodo A recibe el mensaje de supervisión de fallos que es enviado en el trayecto de protección 230 por el nodo B, y supervisa el fallo del trayecto de protección 230 según el mensaje de supervisión de fallos.

En esta realización, el nodo C puede reenviar, al nodo A, el mensaje de supervisión de fallos recibido que es enviado en un trayecto de protección 230 por el nodo B.

El nodo A recibe el mensaje de supervisión de fallos que es enviado en el trayecto de protección 230 por el nodo B y puede llevar a cabo una determinación según un mecanismo de supervisión de fallos actual; si la segunda información de mantenimiento llevada en el mensaje de supervisión de fallos es correcta, se determina que el trayecto de protección 230 no falla; y, por el contrario, si el mensaje de supervisión de fallos no se recibe o si la segunda información de mantenimiento llevada en el mensaje de supervisión de fallos recibido es incorrecta, se determina que el trayecto de protección 230 falla.

Etapa E203: Después de detectar que el enlace B-C falla, el nodo C desconecta el trayecto de protección 230 en el nodo, y conecta el trayecto 250 y un trayecto que está dentro del dominio 2, utiliza el nodo C como un punto extremo, y se utiliza para llevar el servicio protegido 200.

En esta realización, cuando el enlace B-C falla, el nodo C detecta que el enlace B-C falla. El fallo del enlace B-C puede ser un fallo del nodo B o un fallo de un enlace entre el nodo B y el nodo C. El nodo C puede determinar que el trayecto de protección 230 ya no tiene una capacidad de protección, desconectar el trayecto de protección 230 en el nodo para dividirlo en un trayecto 250 y un trayecto 260, es decir, desconectar el empalme del trayecto 250 y el trayecto 260, y conectar el trayecto 250 y un trayecto que está dentro del dominio 2, utiliza un nodo C como un punto extremo, y se utiliza para portar un servicio protegido 200, con el fin de reconstruir un trayecto de protección.

Específicamente, el nodo C puede desconectar el trayecto de protección 230 y el trayecto de protección 240 en el nodo, y conectar el trayecto 250 y un trayecto 270.

El nodo C desconecta el empalme del trayecto 250 y el trayecto 260, y divide el trayecto de protección 230 en el trayecto 250 y el trayecto 260; y desconecta el empalme del trayecto 270 y el trayecto 280, y divide el trayecto de protección 240 en el trayecto 270 y el trayecto 280. El trayecto 270 es un trayecto que está dentro del dominio 2, utiliza el nodo C como un punto extremo, y se utiliza para portar un servicio protegido 200, y el nodo C puede conectar el trayecto 250 y el trayecto 270.

Si el trayecto 270 falla, el trayecto 280 también es un trayecto que está dentro del dominio 2, utiliza el nodo C como un punto extremo, y se utiliza para portar un servicio protegido 200, y el nodo C puede conectar el trayecto 250 y el trayecto 280.

Si el trayecto 280 también falla y también hay un dominio 3 que interseca con el dominio 2 en el nodo D y nodo H, el trayecto C-H también es un trayecto que está dentro del dominio 2, utiliza el nodo C como un punto extremo, y se utiliza para portar un servicio protegido 200, y el nodo C puede conectar el trayecto 250 y el trayecto C-H.

Etapa E204: Después de detectar que el enlace B-C falla, el nodo C envía, en el trayecto 250, un mensaje de supervisión de fallos que lleva la primera información de mantenimiento al nodo A, donde la primera información de mantenimiento es la misma que la segunda información de mantenimiento que se lleva en el mensaje de supervisión de fallos enviado en el trayecto de protección 230 por el nodo B al nodo A.

En condiciones normales, el nodo C puede llevar a cabo una supervisión de fallos en el enlace B-C. Específicamente, el nodo B puede enviar, en el enlace B-C, un mensaje de supervisión de fallos que lleva información de mantenimiento al nodo C, con el fin de que el nodo C supervise un fallo del enlace B-C, donde el contenido específico y un mecanismo de procesamiento de información de mantenimiento son similares a aquellos para el trayecto de protección 230. Se

ha de notar que, para implementar una rápida supervisión de fallos, en comparación con la detección de fallos en el trayecto de protección 230, se debe realizar la detección de fallos en el enlace B-C en un nivel de dominio de mantenimiento más bajo, un nivel de grupo de entidades de mantenimiento más bajo, o un ODU TCM de orden mayor.

En esta realización, el nodo C, en vez del nodo B, envía, al nodo A, el mensaje de supervisión de fallos que lleva la primera información de mantenimiento. La primera información de mantenimiento es la misma que la segunda información de mantenimiento. El nodo C puede obtener la segunda información de mantenimiento de dos maneras:

Antes de detectar que el enlace B-C falla, después de recibir un mensaje de supervisión de fallos que es enviado en el trayecto de protección 230 por el nodo B, el nodo C puede registrar la segunda información de mantenimiento que se lleva en el mensaje de supervisión de fallos.

El nodo C también puede preconfigurar la segunda información de mantenimiento en el nodo C. Se puede seleccionar una configuración de punto extremo de mantenimiento correspondiente según las tecnologías de red del dominio 1 y dominio 2: si el dominio 1 es una red Ethernet, se puede configurar un MEP (punto extremo de asociaciones de mantenimiento o punto extremo de grupo de entidades de mantenimiento) en el nodo C, donde para un punto extremo de mantenimiento en el nodo C y un punto extremo de mantenimiento en el nodo B, los MA ID o MEG ID son iguales y los MEP ID son iguales; si el dominio 1 es una red MPLS, se puede configurar un MEP (punto extremo de grupo de entidades de mantenimiento) en el nodo C, donde tanto los MEG ID como los MEP ID de un punto extremo de mantenimiento en un nodo C y un punto extremo de mantenimiento en un nodo B son iguales; si el dominio 1 es una red OTN, se puede configurar un punto de supervisión TCM, tal y como una función ODUkT, en el nodo C, donde un identificador de punto de acceso del nodo C es igual a un identificador de punto de acceso del nodo B.

Después de detectar que el enlace B-C falla, el nodo C, en vez del nodo B, envía un mensaje de supervisión de fallos que tiene la misma información de mantenimiento, de manera que se reconstruye un trayecto de protección cuando el nodo A ignora el fallo. El trayecto de protección en el dominio 1 se conmuta desde el trayecto de protección 230 al trayecto 250, y un trayecto de protección recién formado atraviesa dominios en el nodo C.

Antes de detectar que el enlace B-C falla, el nodo C no envía el mensaje de supervisión de fallos que lleva la primera información de mantenimiento.

Etapa E205: El nodo A recibe el mensaje de supervisión de fallos que se envía en el trayecto 250 por el nodo C, y supervisa un fallo del trayecto 250 según el mensaje de supervisión de fallos.

En esta realización, tal y como se muestra en la Figura 3, incluso si el enlace B-C falla, después de recibir el mensaje de supervisión de fallos que es enviado por el nodo C, el nodo A aun puede adquirir la primera información de mantenimiento que es la misma que la segunda información de mantenimiento, de manera que el nodo A ignore el fallo del enlace B-C, no es necesario que se reseleccione un trayecto de protección, y no es necesario realizar ninguna operación de conmutación.

En esta realización, una orden de ejecución de la etapa E203 y etapa E204 no está limitada. La etapa E204 se puede realizar después de la etapa E203, y viceversa.

Además, en condiciones normales, el nodo B puede además enviar, en un trayecto de protección 230, una segunda información de conmutación de protección automática (conmutación de protección automática, APS) al nodo A, donde la segunda información de conmutación de protección automática se utiliza por el nodo A para determinar si el trayecto de protección 230 está disponible y para coordinar una acción de conmutación de protección entre el nodo B y el nodo A; el nodo C reenvía la segunda información de APS recibida al nodo A; el nodo A recibe la segunda información de APS que es enviada en el trayecto de protección por el nodo B, mantiene la máquina de estado de conmutación de protección en el nodo A según la segunda información, y determina si el trayecto de protección 230 está disponible, o determina una acción de conmutación de protección para el nodo A.

Después de detectar que el enlace B-C falla, el nodo B deja de enviar la segunda información de APS y el mensaje de supervisión de fallos que lleva la segunda información de mantenimiento.

Después de detectar que el enlace B-C falla, el nodo C puede además enviar, en el trayecto de protección 250, una primera información de APS al nodo A, intercambia, en vez del nodo B, la información de APS con el nodo A, el nodo A recibe la primera información de APS que es enviada en el trayecto de protección 250 por el nodo C, e ignora el fallo del enlace B-C.

Antes de detectar que el enlace B-C falla, el nodo C no envía la primera información de APS.

Asimismo, el nodo A puede además enviar, en el trayecto de protección 230, una tercera información de APS al nodo B; antes de detectar que el enlace B-C falla, el nodo C recibe la tercera información de APS, mantiene la máquina de estado de conmutación de protección en el nodo C según la tercera información de APS, y reenvía la tercera información de APS al nodo B; el nodo B recibe la tercera información de APS, mantiene la máquina de estado de conmutación de protección en el nodo B según la tercera información de APS, e intercambia la información de APS

con el nodo A. Después de detectar que el enlace B-C falla, el nodo C puede además detener el reenvío del tercer mensaje de APS.

Además, si el trayecto en funcionamiento 210 también falla, el nodo A detecta que el trayecto en funcionamiento 210 falla, determina, según la primera información de mantenimiento, que el trayecto 250 no falla, y conmuta el servicio desde el trayecto en funcionamiento 210 al trayecto 250. La Figura 4 describe un escenario en el que tanto el trayecto en funcionamiento 210 como el enlace B-C falla debido a un fallo del nodo B. El nodo C detecta que el enlace B-C falla, desconecta el trayecto de protección 230 y el trayecto de protección 240, y conecta el trayecto 250 y el trayecto 270; el nodo A detecta que el trayecto en funcionamiento 210 falla, y conmuta el servicio protegido 200 al trayecto 250.

En condiciones normales, el nodo A puede llevar a cabo una supervisión de fallos en el trayecto en funcionamiento 210. Específicamente, el nodo B puede enviar, en el trayecto de funcionamiento 210, un mensaje de supervisión de fallos al nodo A, de modo que el nodo A supervise un fallo del trayecto en funcionamiento 210.

Después de que el trayecto en funcionamiento 210 también falla, el nodo A detecta que el trayecto en funcionamiento 210 falla, y el nodo A puede enviar una tercera información de APS que solicita la conmutación al trayecto de protección 230, coordina una acción de conmutación de protección entre el nodo A y el nodo C según la información de APS entre el nodo A y el nodo C, y conmuta el servicio desde el trayecto en funcionamiento 210 al trayecto 250. La información de APS puede ser un paquete de APS o una tara.

Además, después de detectar que el enlace B-C falla, cuando se recibe la tercera información de APS que es enviada por el nodo A y que solicita la conmutación al trayecto de protección, el nodo C puede además enviar un mensaje de notificación al dominio 2, donde el mensaje de notificación da la instrucción de que el nodo C se utilice para implementar una protección entre dominios en el servicio protegido 200. Específicamente, el mensaje de notificación puede instruir que el nodo C se ha de utilizar para conectar el dominio 1 y el dominio 2.

Como nodos intersecantes del dominio 1 y dominio 2, el nodo B y el nodo C pueden tener múltiples enlaces físicos entre medio, donde cada enlace puede portar uno o más trayectos:

1) cuando hay un enlace B-C, el enlace B-C puede ser un enlace intersecante entre el dominio 1 y el dominio 2, es decir, el enlace B-C está ubicado tanto en el dominio 1 como en el dominio 2 2, y tanto el trayecto de protección 230 como el trayecto de protección 240 pasan a través del enlace B-C; o

2) cuando hay múltiples enlaces, por ejemplo, y hay un enlace B-C y enlace B'-C', el enlace B-C puede estar ubicado solo en el dominio 1, y el enlace B'-C' está ubicado sólo en el dominio 2, el trayecto de protección 230 pasa a través del enlace B-C, y el trayecto de protección 240 pasa a través del enlace B'-C'.

En esta realización, el nodo C puede enviar el mensaje de notificación al nodo D en el dominio 2, y el nodo D puede realizar la correspondiente conmutación de protección para el servicio protegido 200 según el mensaje de notificación. Específicamente, si el trayecto 270 no falla, el nodo D conmuta el servicio protegido 200 al trayecto 270, y el servicio protegido 200 cruza dominios en el nodo C, con el fin de implementar una protección de servicio de extremo a extremo en un caso en que el nodo B falle.

Además, en base a la realización anterior, el nodo A puede además enviar, en el trayecto de protección 230, un mensaje de supervisión de fallo que lleva una tercera información de mantenimiento al nodo B; antes de detectar que el enlace B-C falla, el nodo C recibe el mensaje de supervisión de fallos, supervisa un fallo del trayecto 250 según el mensaje de supervisión de fallos, y reenvía el mensaje de supervisión de fallos al nodo B; el nodo B recibe el mensaje de supervisión de fallos, y supervisa un fallo del trayecto de protección 230 según el mensaje de supervisión de fallos. Después de detectar que el enlace B-C falla, el nodo C detiene el reenvío del mensaje de supervisión de fallos.

El procesamiento entre el nodo D en el dominio 2, y el nodo B y el nodo C es similar al de la realización anterior. Cuando se detecta que el enlace B-C falla (solo hay un enlace B-C entre el nodo B y el nodo C) o que el enlace B'-C' falla (hay enlace B-C y enlace B'-C' entre el nodo B y el nodo C, y el trayecto de protección 240 pasa a través del enlace B'-C'), el nodo C, en vez del nodo B, envía, en el trayecto de protección 270, un mensaje de supervisión de fallos al nodo D, donde la información de mantenimiento llevada en el mensaje de supervisión de fallos es igual a la información de mantenimiento llevada en el mensaje de supervisión de fallos que es enviada en el trayecto de protección 240 por el nodo B al nodo D, de manera que un trayecto de protección se reconstruye cuando el nodo D ignora el fallo, y el trayecto de protección en el dominio 2 se conmuta desde el trayecto de protección 240 al trayecto 270, y el recién formado trayecto de protección cruza dominios en el nodo C.

Según el método de protección para una red multidominio provista en esta realización de la presente invención, después de detectar un fallo de un trayecto entre nodos intersecantes, un nodo intersecante en un trayecto de protección, en vez de un nodo intersecante en un trayecto en funcionamiento, envía un mensaje de supervisión de fallos, de manera que los nodos no intersecantes ignoran un fallo del trayecto de protección y se reconstruye un trayecto de protección. De esta manera, se implementa la optimización de un trayecto de protección mediante el procesamiento de solo un nodo intersecante, y se reduce la complejidad de los nodos no intersecantes en una red

multidominio. Además, en un caso en que un trayecto en funcionamiento falla, la conmutación de protección se implementa para un servicio entre dominios sin procesamiento adicional en nodos no intersecantes.

En la Realización 2, esta realización de la presente invención ofrece un nodo. En la Figura 5 se muestra una estructura de un nodo 300, que incluye:

una unidad de detección 310, configurada para detectar un fallo de un primer enlace, donde el primer enlace es un enlace entre un primer nodo y el nodo;

una unidad de conmutación 320, configurada para: después de que se detecta que el primer enlace falla, desconectar un primer trayecto de protección en el nodo, y conectar un primer subtrayecto y un trayecto que está dentro del segundo dominio, utiliza el nodo como un punto extremo, y se utiliza para portar un servicio, donde:

el servicio es un servicio que pasa a través de un primer dominio y el segundo dominio; el primer dominio y el segundo dominio se intersecan en el primer nodo y el nodo; el primer trayecto de protección está formado por el empalme del primer subtrayecto y un segundo subtrayecto y es un trayecto de protección de un primer trayecto en funcionamiento; el primer trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo y un tercer nodo dentro del primer dominio; el primer subtrayecto es un trayecto entre el nodo y el tercer nodo; y el segundo subtrayecto es un trayecto que pasa a través del primer enlace y que está dentro del primer nodo y el nodo; y

una unidad de procesamiento 330, configurada para: después de que se detecta que el primer enlace falla, enviar, en el primer subtrayecto, un primer mensaje de supervisión de fallos que lleva una primera información de mantenimiento al tercer nodo, donde:

la primera información de mantenimiento es la misma que la segunda información de mantenimiento llevada en un segundo mensaje de supervisión de fallos; y el segundo mensaje de supervisión de fallos es un mensaje que es enviado en el primer trayecto de protección por el primer nodo al tercer nodo y que se utiliza para supervisar un fallo del primer trayecto de protección.

Además, la unidad de conmutación 320 puede estar específicamente configurada para: después de que se detecta que el primer enlace falla, desconectar el primer trayecto de protección y un segundo trayecto de protección en el nodo, y conectar el primer subtrayecto y un tercer subtrayecto, donde:

el segundo trayecto de protección está formado por el empalme del tercer subtrayecto y un cuarto subtrayecto y es un trayecto de protección de un segundo trayecto en funcionamiento; el segundo trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo y un cuarto nodo dentro del segundo dominio; el tercer subtrayecto es un trayecto entre el nodo y el cuarto nodo; y el cuarto subtrayecto es un trayecto entre el primer nodo y el nodo.

En una implementación específica, el primer trayecto de protección y el segundo trayecto de protección están desconectados en el nodo, y después se puede implementar un módulo de conmutación interna del nodo mediante el uso de un puente selectivo (puente selectivo) y un selector selectivo (selector selectivo).

Además, la unidad de conmutación 320 puede incluir específicamente un primer puente 321, un primer selector 322, y una unidad de control 323, tal y como se muestra en la Figura 6a, donde:

un extremo de salida del primer selector 322 está conectado al primer subtrayecto; un extremo de entrada 1 del primer selector 322 está conectado al segundo subtrayecto;

el extremo de entrada 2 del primer selector 322 está conectado al extremo de salida 2 del primer puente 321;

el extremo de salida 1 del primer puente 321 está conectado al cuarto subtrayecto; un extremo de entrada del primer puente 321 está conectado al tercer subtrayecto; y

la unidad de control 323 está configurada para: después de que se detecta que el primer enlace falla, controlar el extremo de entrada del primer puente 321 para desconectarlo del extremo de salida 1 del primer puente 321 y para conectarlo al extremo de salida 2 del primer puente 321, y controlar el extremo de salida del primer selector 322 para desconectarlo del extremo de entrada 1 del primer selector 322 y para conectarlo al extremo de entrada 2 del primer selector 322.

Asimismo, para un servicio bidireccional, la unidad de conmutación 320 puede incluir además un segundo puente 324 y un segundo selector 325, como se muestra en la Figura 6b, donde:

un extremo de entrada del segundo puente 324 está conectado al primer subtrayecto; un extremo de salida 1 del segundo puente 324 está conectado al segundo subtrayecto;

un extremo de salida 2 del segundo puente 324 está conectado al extremo de entrada 2 del segundo selector 325;

un extremo de entrada 1 del segundo selector 325 está conectado al cuarto subtrayecto; un extremo de salida del segundo selector 325 está conectado al tercer subtrayecto; y

la unidad de control 323 está configurada además para: después de que se detecta que el primer enlace falla, controlar el extremo de entrada del segundo puente 324 para desconectarlo del extremo de salida 1 del segundo puente 324 y para conectarlo al extremo de salida 2 del segundo puente 324, y controlar el extremo de salida del segundo selector 325 para desconectarlo del extremo de entrada 1 del segundo selector 325 y para conectarlo al extremo de entrada 2 del segundo selector 325.

Asimismo, la unidad de procesamiento 330 puede además estar configurada para: antes de que se detecte que el primer enlace falla, reenviar el segundo mensaje de supervisión de fallos recibido al tercer nodo.

Asimismo, la unidad de procesamiento 330 puede además estar configurada para: antes de que se detecte que el primer enlace falla, reenviar la segunda información de APS recibida al tercer nodo, donde la segunda información de APS es información enviada en el primer trayecto de protección por el primer nodo al tercer nodo; y después de que se detecta que el primer enlace falla, enviar, en el primer trayecto de protección, la primera información de APS al tercer nodo.

Asimismo, el nodo puede además incluir una unidad de registro 340 configurada para: antes de que se detecte que el primer enlace falla, registrar la segunda información de mantenimiento llevada en el segundo mensaje de supervisión de fallos recibido.

Asimismo, la unidad de procesamiento 330 puede además estar configurada para: antes de que se detecte que el primer enlace falla, reenviar un tercer mensaje de APS recibido al primer nodo, y mantener una máquina de estado de conmutación de protección según el tercer mensaje de APS, donde el tercer mensaje de APS es información enviada en el primer trayecto de protección por el tercer nodo al primer nodo; y después de que se detecta que el primer enlace falla, detener el reenvío del tercer mensaje de APS.

Asimismo, el nodo puede además incluir una unidad de notificación 350, configurada para: después de que se detecta que el primer enlace falla, cuando la tercera información de APS que se envía por parte del tercer nodo y que se reciben las solicitudes de conmutación al primer trayecto de protección, enviar un mensaje de notificación al cuarto nodo, donde el mensaje de notificación se utiliza para dar la instrucción de que el nodo se utilice para conectar el primer dominio y el segundo dominio para el servicio.

Asimismo, la unidad de procesamiento 330 puede además estar configurada: antes de que se detecte que el primer enlace falla, reenviar un tercer mensaje de supervisión de fallos recibido al primer nodo, y supervisar un fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos, donde el tercer mensaje de supervisión de fallos es un mensaje que es enviado en el primer trayecto de protección por el tercer nodo al primer nodo y que se utiliza para supervisar el primer trayecto de protección; y después de que se detecta que el primer enlace falla, detener el reenvío del tercer mensaje de supervisión de fallos.

Específicamente, la unidad de procesamiento 330 puede incluir:

un tercer puente, configurado para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática; y enviar el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática a una primera unidad de mantenimiento y un segundo conmutador;

la primera unidad de mantenimiento, configurada para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática que se emiten por parte del tercer puente, mantener la máquina de estado de conmutación de protección según el tercer mensaje de conmutación de protección automática, y supervisar el fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos; regenerar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática; y enviar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática regenerados a un primer conmutador;

el primer conmutador, configurado para: reenviar, al tercer nodo, el segundo mensaje de supervisión de fallos y una segunda información de conmutación de protección automática recibidos que son enviados por el primer nodo; antes de que se detecte que el primer enlace falla, prohibir el reenvío del primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y después de que se detecta que el primer enlace falla, enviar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y

el segundo conmutador, configurado para: antes de que se detecte que el primer enlace falla, enviar el tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática recibidos al primer nodo; y después de que se detecta que el primer enlace falla, detener el envío del tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática.

Tal y como se muestra en la Figura 7a, el tercer puente, la primera unidad de mantenimiento, el primer conmutador, y el segundo conmutador que están incluidos en la unidad de procesamiento 330 pueden ser específicamente un tercer puente, 331, una primera unidad de mantenimiento 333, un primer conmutador 332, y un segundo conmutador 335 en la Figura 7a.

En una implementación específica el tercer puente 331 puede ser un puente permanente, el primer conmutador 332 y el segundo conmutador 335 pueden ser conmutadores simples unipolares, y la primera unidad de mantenimiento 333 puede ser una unidad de función MEP que implementa una función MEP relacionada.

De manera alternativa, la unidad de procesamiento 330 puede incluir:

un tercer puente, configurado para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática; y enviar el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática a una primera unidad de mantenimiento y una segunda unidad de mantenimiento;

la primera unidad de mantenimiento, configurada para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática que se emiten por parte del tercer puente, mantener la máquina de estado de conmutación de protección según el tercer mensaje de conmutación de protección automática, y supervisar el fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos; regenerar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática; y enviar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática regenerados a un primer conmutador;

la segunda unidad de mantenimiento, configurada para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática que se emiten por parte del tercer puente, y enviar el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática a un segundo conmutador; y reenviar, al tercer nodo, el segundo mensaje de supervisión de fallos y la segunda información de conmutación de protección automática recibidos que son enviados por el primer nodo;

el primer conmutador, configurado para: antes de que se detecte que el primer enlace falla, prohibir el reenvío del primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y después de que se detecta que el primer enlace falla, enviar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y

el segundo conmutador, configurado para: antes de que se detecte que el primer enlace falla, enviar el tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática recibidos al primer nodo; y después de que se detecta que el primer enlace falla, detener el envío del tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática.

Tal y como se muestra en la Figura 7b, el tercer puente, la primera unidad de mantenimiento, la segunda unidad de mantenimiento, el primer conmutador, y el segundo conmutador que están incluidos en la unidad de procesamiento 330 pueden ser específicamente un tercer puente 331, una primera unidad de mantenimiento 333, una segunda unidad de mantenimiento 334, un primer conmutador 332, y un segundo conmutador 335 en la Figura 7b.

En una implementación específica, el tercer puente 331 puede ser un puente permanente, el primer conmutador 332 y el segundo conmutador 335 pueden ser conmutadores simples unipolares, la primera unidad de mantenimiento 333 puede ser una unidad de función MEP que implementa una función MEP relacionada, y la segunda unidad de mantenimiento 334 puede ser una unidad de función MIP que implementa una función relacionada con un MIP (punto intermedio de MEG o punto intermedio de MA, punto intermedio de grupo de entidades de mantenimiento o punto intermedio de asociaciones de mantenimiento).

De manera alternativa, la unidad de procesamiento 330 puede incluir:

un tercer puente, configurado para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática; antes de que se detecte que el primer enlace falla, enviar el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática a una segunda unidad de mantenimiento; y después de que se detecta que el primer enlace falla, enviar el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática a una primera unidad de mantenimiento;

la primera unidad de mantenimiento, configurada para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática que se emiten por parte del tercer puente, mantener la máquina de estado de conmutación de protección según el tercer mensaje de conmutación de protección automática, y supervisar el fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos; regenerar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática; y enviar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática regenerados a un primer conmutador;

la segunda unidad de mantenimiento, configurada para: recibir el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática que se emiten por parte del tercer puente, y enviar el tercer mensaje de supervisión de fallos y la tercera información de conmutación de protección automática a un segundo conmutador; y reenviar, al tercer nodo, el segundo mensaje de supervisión de fallos y la segunda información de conmutación de protección automática recibidos que son enviados por el primer nodo;

el primer conmutador, configurado para: antes de que se detecte que el primer enlace falla, prohibir el reenvío del primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y después de que se detecta que el primer enlace falla, enviar el primer mensaje de supervisión de fallos y la primera información de conmutación de protección automática al tercer nodo; y

el segundo conmutador, configurado para: antes de que se detecte que el primer enlace falla, enviar el tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática recibidos al primer nodo; y después de que se detecta que el primer enlace falla, detener el envío del tercer mensaje de supervisión de fallos y el tercer mensaje de conmutación de protección automática.

Tal y como se muestra en la Figura 7c, el tercer puente, la primera unidad de mantenimiento, la segunda unidad de mantenimiento, el primer conmutador, y el segundo conmutador que están incluidos en la unidad de procesamiento 330 pueden ser específicamente un tercer puente 331, una primera unidad de mantenimiento 333, una segunda unidad de mantenimiento 334, un primer conmutador 332, y un segundo conmutador 335 en la Figura 7c.

En una implementación específica, el tercer puente 331 puede ser un puente selectivo, el primer conmutador 332 y el segundo conmutador 335 pueden ser conmutadores simples unipolares, y la primera unidad de mantenimiento 333 puede ser una unidad de función MEP que implementa una función MEP relacionada, y la segunda unidad de mantenimiento 334 puede ser una unidad de función MIP que implementa una función relacionada con MIP.

En la Realización 3, esta realización de la presente invención ofrece otro nodo. En la Figura 8 se muestra una estructura de un nodo 800, que incluye:

un emisor 810, configurado para: después de que se detecta que un primer enlace falla, enviar, en un primer subtrayecto, un primer mensaje de supervisión de fallos que lleva una primera información de mantenimiento a un tercer nodo, donde:

el primer enlace es un enlace entre un primer nodo y un segundo nodo; la primera información de mantenimiento es la misma que la segunda información de mantenimiento llevada en un segundo mensaje de supervisión de fallos; y el segundo mensaje de supervisión de fallos es un mensaje que es enviado en un primer trayecto de protección por el primer nodo al tercer nodo y que se utiliza para supervisar un fallo del primer trayecto de protección;

una memoria 820, configurada para almacenar información que incluye una rutina programa; y

un procesador 830, acoplado con la memoria 820 y el emisor 810 y configurado para controlar la ejecución de la rutina programa, que específicamente incluye:

detectar un fallo del primer enlace; y

después de que se detecta que el primer enlace falla, desconectar el primer trayecto de protección en el nodo, y conectar el primer subtrayecto y un trayecto que está dentro de un segundo dominio, utiliza el nodo como un punto extremo, y se utiliza para portar un servicio, donde:

el servicio es un servicio que pasa a través de un primer dominio y el segundo dominio; el primer dominio y el segundo dominio se intersecan en el primer nodo y el nodo; el primer trayecto de protección está formado por el empalme del primer subtrayecto y un segundo subtrayecto y es un trayecto de protección de un primer trayecto en funcionamiento; el primer trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo y el tercer nodo dentro del primer dominio; el primer subtrayecto es un trayecto entre el nodo y el tercer nodo; y el segundo subtrayecto es un trayecto que pasa a través del primer enlace y que está dentro del primer nodo y el segundo nodo.

El nodo provisto en esta realización de la presente invención puede ser un aparato de red, tal y como un conmutador Ethernet, un enrutador, y un dispositivo de transmisión OTN, o puede ser un módulo en el aparato de red, que no está limitado en la presente memoria.

Según el nodo provisto en esta realización de la presente invención, es decir, un nodo intersecante en un trayecto de protección, después de detectar un fallo de un trayecto entre nodos intersecantes, el nodo intersecante en el trayecto de protección, en vez de un nodo intersecante en un trayecto en funcionamiento, envía un mensaje de supervisión de fallos, de manera que los nodos no intersecantes ignoren un fallo del trayecto de protección y se reconstruya un trayecto de protección. De esta manera, se implementa la optimización de un trayecto de protección mediante el procesamiento de solo un nodo intersecante, y se reduce la complejidad de los nodos no intersecantes en una red multidominio. Además, en un caso en que un trayecto en funcionamiento falla, la conmutación de protección se implementa para un servicio entre dominios sin procesamiento adicional en nodos no intersecantes.

Para el nodo en las Realizaciones 2 y 3 precedentes, debido a que el contenido, tal y como intercambio de información y procesos de ejecución entre sus unidades internas, está basado en una misma idea que el método de realización de la presente invención, para un contenido detallado, se puede hacer referencia a la descripción en la realización de método de la presente invención, y no se describirán detalles nuevamente en la presente memoria.

En la Realización 4, esta realización de la presente invención ofrece un sistema de protección para una red multidominio. Tal y como se muestra en la Figura 9, una red multidominio en la que está ubicado un sistema 900 incluye un primer dominio y un segundo dominio, donde el primer dominio y el segundo dominio intersecan en un primer nodo 910 y un segundo nodo 920; y el sistema 900 incluye:

el primer nodo 910, configurado para enviar, en un primer trayecto de protección, un segundo mensaje de supervisión de fallos que se utiliza para supervisar un fallo del primer trayecto de protección a un tercer nodo 930, donde el segundo mensaje de supervisión de fallos lleva una segunda información de mantenimiento;

el segundo nodo 920, configurado para: después de que se detecta que un primer enlace falla, desconectar el primer trayecto de protección en el nodo, y conectar un primer subtrayecto y un trayecto que está dentro del segundo dominio, utiliza el segundo nodo 920 como un punto extremo, y se utiliza para portar un servicio; y enviar, en el primer subtrayecto, un primer mensaje de supervisión de fallos que lleva la primera información de mantenimiento al tercer nodo 930, donde la primera información de mantenimiento es la misma que la segunda información de mantenimiento llevada en el segundo mensaje de supervisión de fallos, el primer enlace es un enlace entre el primer nodo 910 y el segundo nodo 920, y el servicio es un servicio que pasa a través del primer dominio y el segundo dominio; y

el primer trayecto de protección está formado por el empalme del primer subtrayecto y un segundo subtrayecto y es un trayecto de protección de un primer trayecto en funcionamiento; el primer trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo 910 y el tercer nodo 930 dentro del primer dominio; el primer subtrayecto es un trayecto entre el segundo nodo 920 y el tercer nodo 930; y el segundo subtrayecto es un trayecto que pasa a través del primer enlace y está entre el primer nodo 910 y el segundo nodo 920; y

el tercer nodo 930, configurado para: recibir el primer mensaje de supervisión de fallos o el segundo mensaje de supervisión de fallos; y supervisar el fallo del primer trayecto de protección según el primer mensaje de supervisión de fallos o el segundo mensaje de supervisión de fallos.

Asimismo, la desconexión del primer trayecto de protección en el nodo, y la conexión de un primer subtrayecto y un trayecto que está dentro del segundo dominio, utiliza el segundo nodo 920 como un punto extremo, y se utiliza para portar un servicio que específicamente incluye:

desconectar el primer trayecto de protección y un segundo trayecto de protección en el nodo; y conectar el primer subtrayecto y un tercer subtrayecto, donde:

el segundo trayecto de protección está formado por el empalme del tercer subtrayecto y un cuarto subtrayecto y es un trayecto de protección de un segundo trayecto en funcionamiento; el segundo trayecto en funcionamiento es un trayecto en funcionamiento del servicio entre el primer nodo 910 y un cuarto nodo 940 dentro del segundo dominio; el tercer subtrayecto es un trayecto entre el segundo nodo 920 y el cuarto nodo 940; y el cuarto subtrayecto es un trayecto entre el primer nodo 910 y el segundo nodo 920.

Asimismo, el segundo nodo 920 puede además estar configurado para: antes de que se detecte que el primer enlace falla, reenviar el segundo mensaje de supervisión de fallos recibido al tercer nodo 930.

Asimismo, el segundo nodo 920 está además configurado para: antes de que se detecte que el primer enlace falla, registrar la segunda información de mantenimiento llevada en el segundo mensaje de supervisión de fallos recibido.

Asimismo, el primer nodo 910 está además configurado para enviar, en el primer trayecto de protección, una segunda información de APS al tercer nodo 930; y

el segundo nodo 920 está además configurado para: antes de que se detecte que el primer enlace falla, reenviar la segunda información de APS recibida al tercer nodo 930; y después de que se detecta que el primer enlace falla, enviar, en el primer trayecto de protección, la primera información de APS al tercer nodo 930.

Asimismo, el tercer nodo 930 está además configurado para enviar, en el primer trayecto de protección, una tercera información de APS al primer nodo 910; y

el segundo nodo 920 está además configurado para: antes de que se detecte que el primer enlace falla, reenviar la tercera información de APS recibida al primer nodo 910, y mantener una máquina de estado de conmutación de protección según el tercer mensaje de APS; y después de que se detecta que el primer enlace falla, detener el reenvío de la tercera información de APS.

Asimismo, el segundo nodo 920 está además configurado para: después de que se detecta que el primer enlace falla, cuando la tercera información de APS que se envía por parte del tercer nodo 930 y que se reciben las solicitudes de conmutación al primer trayecto de protección, enviar un mensaje de notificación al segundo dominio, donde el mensaje

de notificación se utiliza para dar la instrucción de que el segundo nodo se utilice para conectar el primer dominio y el segundo dominio para el servicio.

Asimismo, el tercer nodo 930 está además configurado para enviar, en el primer trayecto de protección, un tercer mensaje de supervisión de fallos que se utiliza para supervisar el primer trayecto de protección al primer nodo 910. El segundo nodo 920 está además configurado para: antes de que se detecte que el primer enlace falla, reenviar el tercer mensaje de supervisión de fallos recibido al primer nodo 910, y supervisar un fallo del primer subtrayecto según el tercer mensaje de supervisión de fallos; y después de que se detecta que el primer enlace falla, detener el reenvío del tercer mensaje de supervisión de fallos. El primer nodo 910 está además configurado para recibir el tercer mensaje de supervisión de fallos, y supervisar el fallo del primer trayecto de protección según el tercer mensaje de supervisión de fallos.

Para la implementación del aparato interno del segundo nodo 920, se puede hacer referencia al nodo en la Realización 2 o Realización 3, y no se describirán detalles nuevamente en la presente memoria.

Para el sistema de protección para una red multidominio en la Realización 4 precedente, debido a que el contenido, tal y como intercambio de información y procesos de ejecución entre sus nodos internos, está basado en una misma idea que la realización de método y realizaciones de aparato de la presente invención, para un contenido detallado, se puede hacer referencia a la descripción en la realización de método y realizaciones de aparato de la presente invención, y no se describirán detalles nuevamente en la presente memoria.

Según el sistema de protección para una red multidominio provista en esta realización de la presente invención, después de detectar un fallo en un trayecto entre nodos intersecantes, un nodo intersecante en un trayecto de protección, en vez de un nodo intersecante en un trayecto en funcionamiento, envía un mensaje de supervisión de fallos, de manera que los nodos no intersecantes ignoren un fallo del trayecto de protección y se reconstruya un trayecto de protección. De esta manera, se implementa la optimización de un trayecto de protección mediante el procesamiento de solo un nodo intersecante, y se reduce la complejidad de los nodos no intersecantes en una red multidominio. Además, en un caso en que un trayecto en funcionamiento falla, la conmutación de protección se implementa para un servicio entre dominios sin procesamiento adicional en nodos no intersecantes.

Una persona con experiencia ordinaria en la técnica puede comprender que algunas o todas las etapas en las realizaciones de método se pueden implementar mediante un programa informático que instruye un hardware relevante. El programa se puede almacenar en un medio de almacenamiento legible por ordenador. Cuando se ejecuta el programa, se llevan a cabo los procesos de las realizaciones de método. El medio de almacenamiento puede incluir: un disco magnético, un disco óptico, una memoria de solo lectura (memoria de solo lectura, ROM), o una memoria de acceso aleatorio (memoria de acceso aleatorio, RAM).

Las descripciones anteriores son meramente realizaciones específicas de la presente invención, pero no están concebidas para limitar el alcance de protección de la presente invención. Cualquier modificación o reemplazo claramente descubierto por un experto en la técnica dentro del alcance técnico descrito en la presente invención estará comprendido dentro del alcance de protección de la presente invención. Por lo tanto, el alcance de protección de la presente invención estará sujeto al alcance de protección de las reivindicaciones.

REIVINDICACIONES

1. Un método de protección para una red multidomionio, en donde la red multidominio comprende un primer dominio y un segundo dominio, en donde el primer dominio y el segundo dominio interconectado por un primer nodo (B) y un segundo nodo (C), y el método comprende:

detectar, por parte del segundo nodo, un fallo en un primer enlace (B-C) entre el primer nodo y el segundo nodo;

desconectar, por parte del segundo nodo, un primer trayecto (230) de protección, en donde el primer trayecto (230) de protección es un trayecto de protección de un trayecto (210) en funcionamiento y está formado por el empalme del primer subtrayecto (250) y un segundo subtrayecto (260), y el trayecto (210) en funcionamiento es un trayecto entre el primer nodo (B) y un tercer nodo (A) dentro del primer dominio; el primer subtrayecto (250) es un trayecto entre el segundo nodo (C) y el tercer nodo (A), y el segundo subtrayecto (260) es un trayecto que pasa a través del primer enlace (B-C) y que está entre el primer nodo (B) y el segundo nodo (C);

conectar, por parte del segundo nodo, el primer subtrayecto (250) y un trayecto que está dentro del segundo dominio para reconstruir un nuevo trayecto de protección; y

enviar, por parte del segundo nodo, un primer mensaje de supervisión de fallos que lleva la primera información de mantenimiento al tercer nodo (A), en donde la primera información de mantenimiento es la misma que una segunda información de mantenimiento, y la segunda información de mantenimiento es llevada en un segundo mensaje de supervisión de fallos que se utiliza para supervisar un fallo del primer trayecto (230) de protección que se envía desde el primer nodo (B) al tercer nodo (A).

2. El método según la reivindicación 1, en donde el segundo nodo está configurado como un punto extremo de grupo de entidades de mantenimiento, MEP.

3. El método según la reivindicación 1 o 2 , en donde el segundo nodo está configurado con el mismo identificador de grupo de entidades de mantenimiento, MEG ID, e identificador de punto extremo de grupo de entidades de mantenimiento, MEP ID, como la segunda información de mantenimiento del primer nodo.

4. El método según cualquiera de las reivindicaciones 1 a 3, en donde la detección, por parte del segundo nodo, de un fallo en un primer enlace entre el primer nodo y el segundo nodo, comprende:

detectar, por parte del segundo nodo, el fallo en el primer enlace en un nivel de grupo de entidades de mantenimiento, MEG, más bajo que la supervisión de fallos en el primer trayecto de protección.

5. El método según cualquiera de las reivindicaciones 1 a 4, en donde la desconexión del primer trayecto de protección en el segundo nodo se implementa utilizando un puente selectivo y un selector selectivo.

6. El método según cualquiera de las reivindicaciones 1 a 5, en donde la desconexión de un primer trayecto (230) de protección en el segundo nodo comprende:

empalmar, por parte del segundo nodo, el primer trayecto de protección al primer subtrayecto y a un segundo subtrayecto (260), en donde el primer subtrayecto y el segundo subtrayecto están conectados por el segundo nodo.
7. Un nodo, que comprende una unidad de detección, una unidad de conmutación, y una unidad de emisión, en donde:

la unidad de detección está configurada para detectar un fallo en un primer enlace (B-C) entre un primer nodo (B) y el nodo (C);

la unidad de conmutación está configurada para desconectar un primer trayecto (230) de protección, en el nodo, en donde el primer trayecto (230) de protección es un trayecto de protección de un trayecto (210) en funcionamiento y está formado por el empalme del primer subtrayecto (250) y un segundo subtrayecto (260), y el trayecto (210) en funcionamiento es un trayecto entre el primer nodo (B) y un tercer nodo (A) dentro del primer dominio, el primer subtrayecto (250) es un trayecto entre el segundo nodo (C) y el tercer nodo (A), y el segundo subtrayecto (260) es un trayecto que pasa a través del primer enlace (B-C) y que está entre el primer nodo (B) y el segundo nodo (C), y que conecta el primer subtrayecto (250) y un trayecto que está dentro de un segundo dominio para reconstruir un nuevo trayecto de protección; y

la unidad de emisión está configurada para enviar un primer mensaje de supervisión de fallos que lleva la primera información de mantenimiento al tercer nodo (A), en donde la primera información de mantenimiento es la misma que una segunda información de mantenimiento, y la segunda información de mantenimiento es llevada en un segundo mensaje de supervisión de fallos que se utiliza para supervisar un fallo del primer trayecto (230) de protección que se envía desde el primer nodo (B) al tercer nodo (A).

8. El nodo según la reivindicación 7, en donde el nodo está configurado como un punto extremo de grupo de entidades de mantenimiento, MEP.

9. El nodo según la reivindicación 7 u 8 , en donde el nodo está configurado con el mismo identificador de grupo de entidades de mantenimiento, MEG ID, e identificador de punto extremo de grupo de entidades de mantenimiento MEP ID, como la segunda información de mantenimiento del primer nodo.

10. El nodo según cualquiera de las reivindicaciones 7 a 9, en donde la unidad de detección está configurada para:

detectar un fallo en el primer enlace en un nivel de grupo de entidades de mantenimiento , MEG, más bajo que la supervisión de fallos en el primer trayecto de protección.

11. El nodo según cualquiera de las reivindicaciones 7 a 10, en donde la unidad de conmutación se implementa utilizando un puente selectivo y un selector selectivo.

12. El nodo según cualquiera de las reivindicaciones 7 a 11, en donde la unidad de conmutación está configurada para:

empalmar el primer trayecto de protección al primer subtrayecto y a un segundo subtrayecto (260), en donde el primer subtrayecto y el segundo subtrayecto están conectados por el nodo.
13. Un sistema de protección para una red multidomionio, en donde la red multidominio comprende un primer dominio y un segundo dominio, en donde el primer dominio y el segundo dominio se intersecan en un primer nodo (B) y un segundo nodo (C), y el sistema comprende:

el primer nodo (B), configurado para enviar, en un primer trayecto (230) de protección, un segundo mensaje de supervisión de fallos que se utiliza para supervisar un fallo del primer trayecto de protección a un tercer nodo, en donde el segundo mensaje de supervisión de fallos lleva una segunda información de mantenimiento;

el segundo nodo (C), que es el nodo según cualquiera de las reivindicaciones 7 a 12;

el tercer nodo (A), configurado para: recibir el primer mensaje de supervisión de fallos y supervisar el fallo del primer trayecto de protección según el primer mensaje de supervisión de fallos; o recibir el segundo mensaje de supervisión de fallos y supervisar el fallo del primer trayecto de protección según el segundo mensaje de supervisión de fallos.

14. El sistema según la reivindicación 13, en donde:

el segundo nodo está configurado para reenviar un segundo mensaje de conmutación de protección automática al tercer nodo, en donde el segundo mensaje de conmutación de protección automática es enviado en el primer trayecto de protección por parte del primer nodo al tercer nodo; y

después de que el segundo nodo detecta el fallo del primer enlace, enviar, en el primer trayecto de protección, un primer mensaje de conmutación de protección automática al tercer nodo.

15. El sistema según la reivindicación 13 o 14, en donde:

el segundo nodo está configurado para reenviar un tercer mensaje de conmutación de protección automática al primer nodo, en donde el tercer mensaje de conmutación de protección automática es enviado en el primer trayecto de protección por parte del tercer nodo al primer nodo; y

después de que el segundo nodo detecta el fallo en el primer enlace, detener el reenvío del tercer mensaje de conmutación de protección automática.

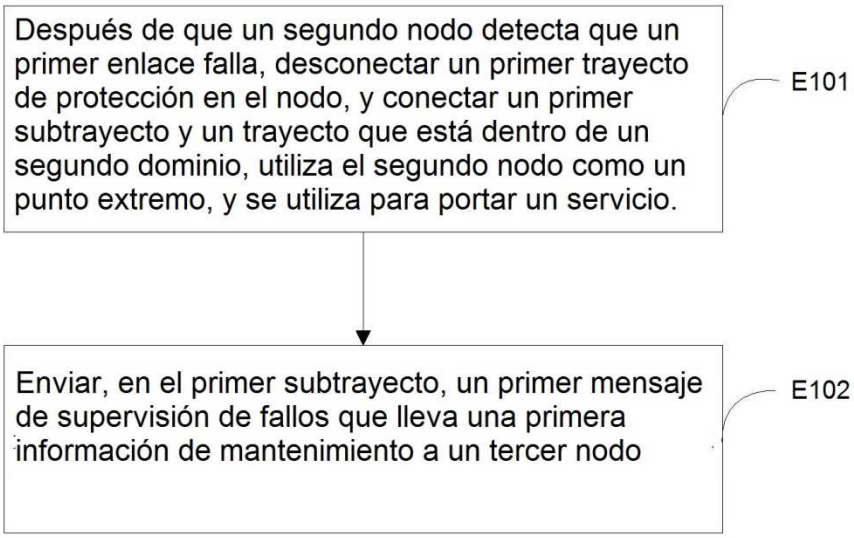
Después de que un segundo nodo detecta que un primer enlace falla, desconectar un primer trayecto de protección en el nodo, y conectar un primer subtrayecto y un trayecto que está dentro de un segundo dominio, utiliza el segundo nodo como un punto extremo, y se utiliza para portar un servicio.
E101
Enviar, en el primer subtrayecto, un primer mensaje de supervisión de fallos que lleva una primera información de mantenimiento a un tercer nodo
E102

FIG. 1

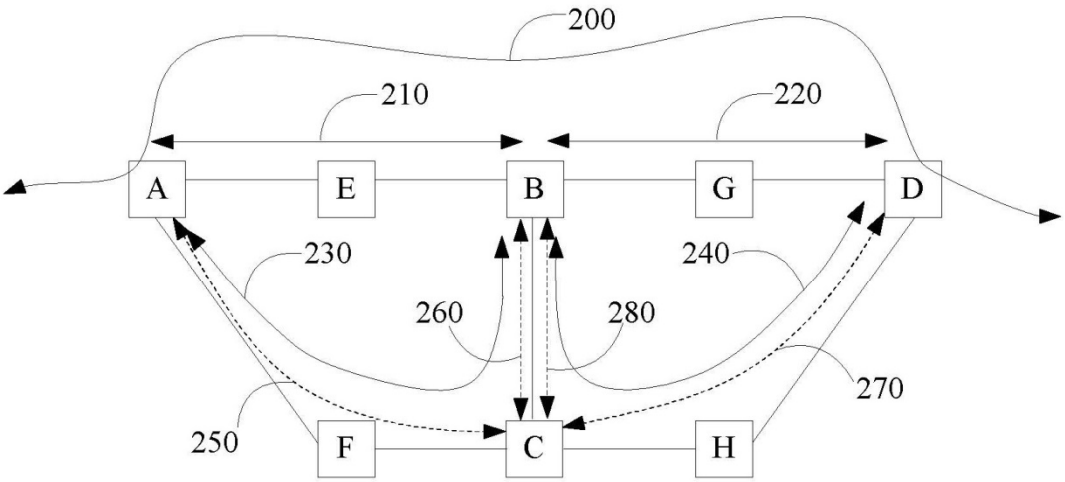
200
210
220
A
E
B
G
D
230
240
260
280
270
250
F
C
H

FIG. 2

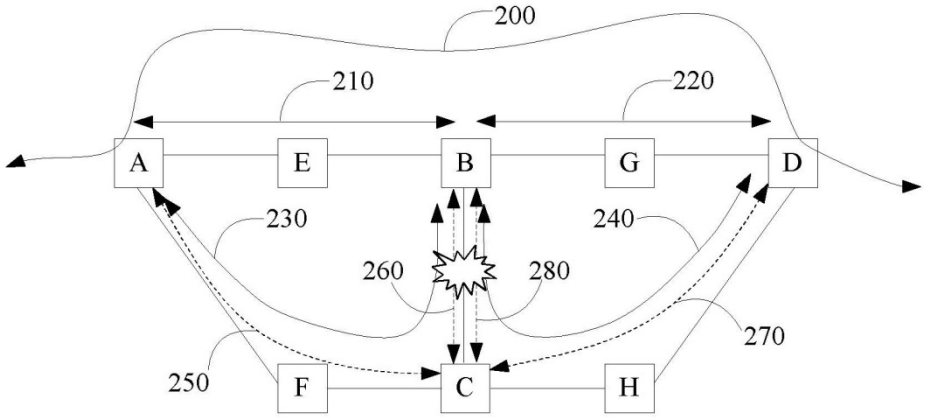
200
210
220
A
E
B
G
D
230
240
260
280
270
250
F
C
H

FIG. 3

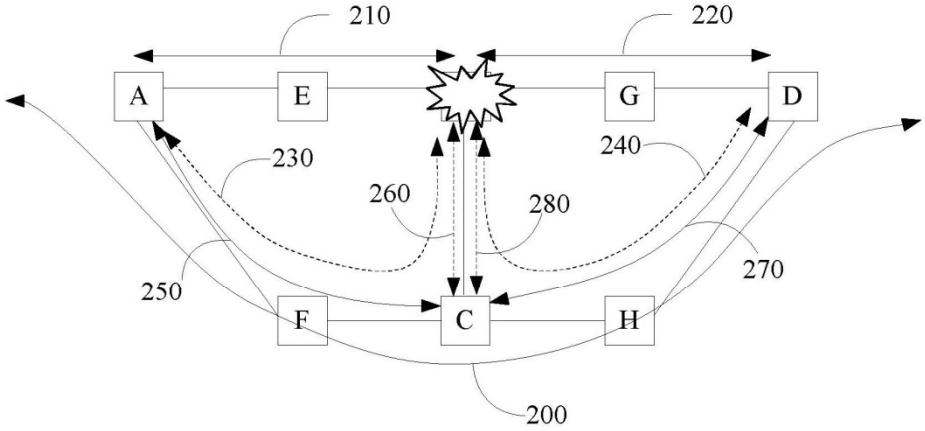
210
220
A
E
G
D
230
240
260
280
270
250
F
C
H
200

FIG. 4

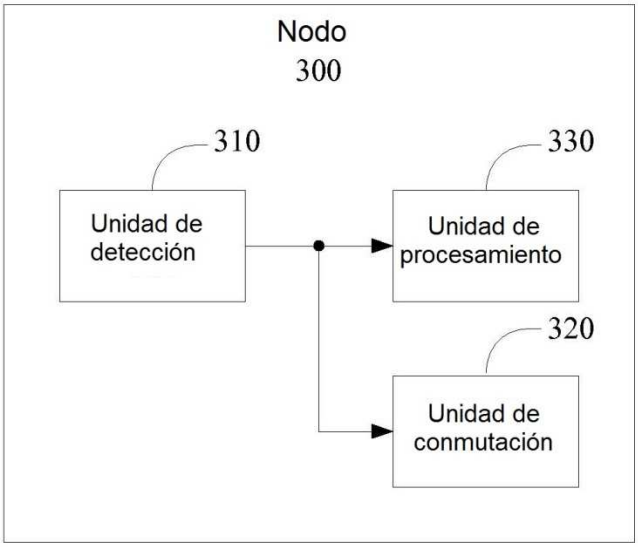
Nodo
300
310
330
Unidad de detección
Unidad de procesamiento
320
Unidad de conmutación

FIG. 5

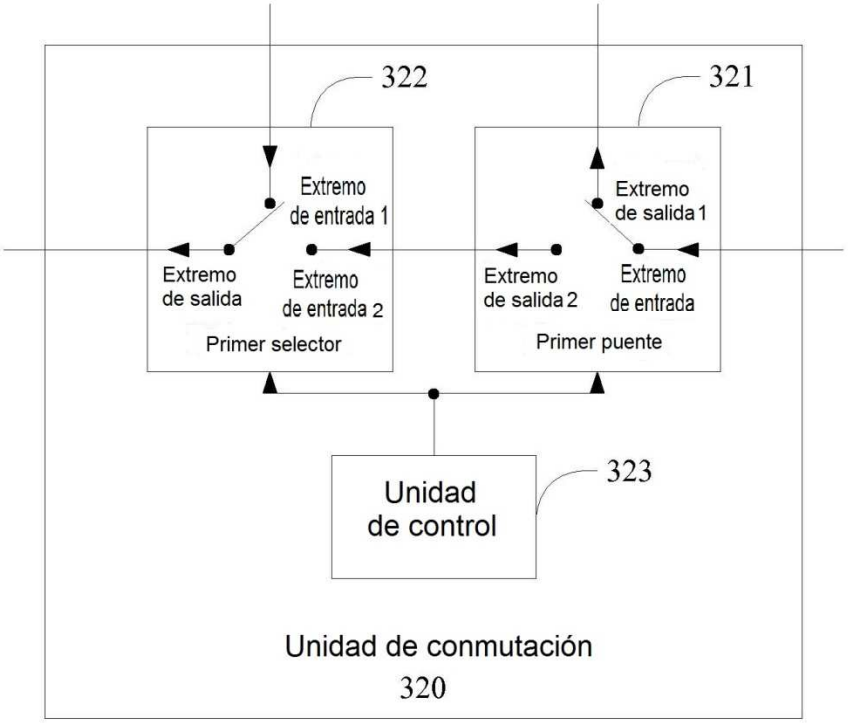
322
321
Extremo de entrada 1
Extremo de salida 1
Extremo de salida
Extremo de entrada 2
Extremo de salida 2
Extremo de entrada
Primer selector
Primer puente
323
Unidad de control
Unidad de conmutación
320

FIG. 6a

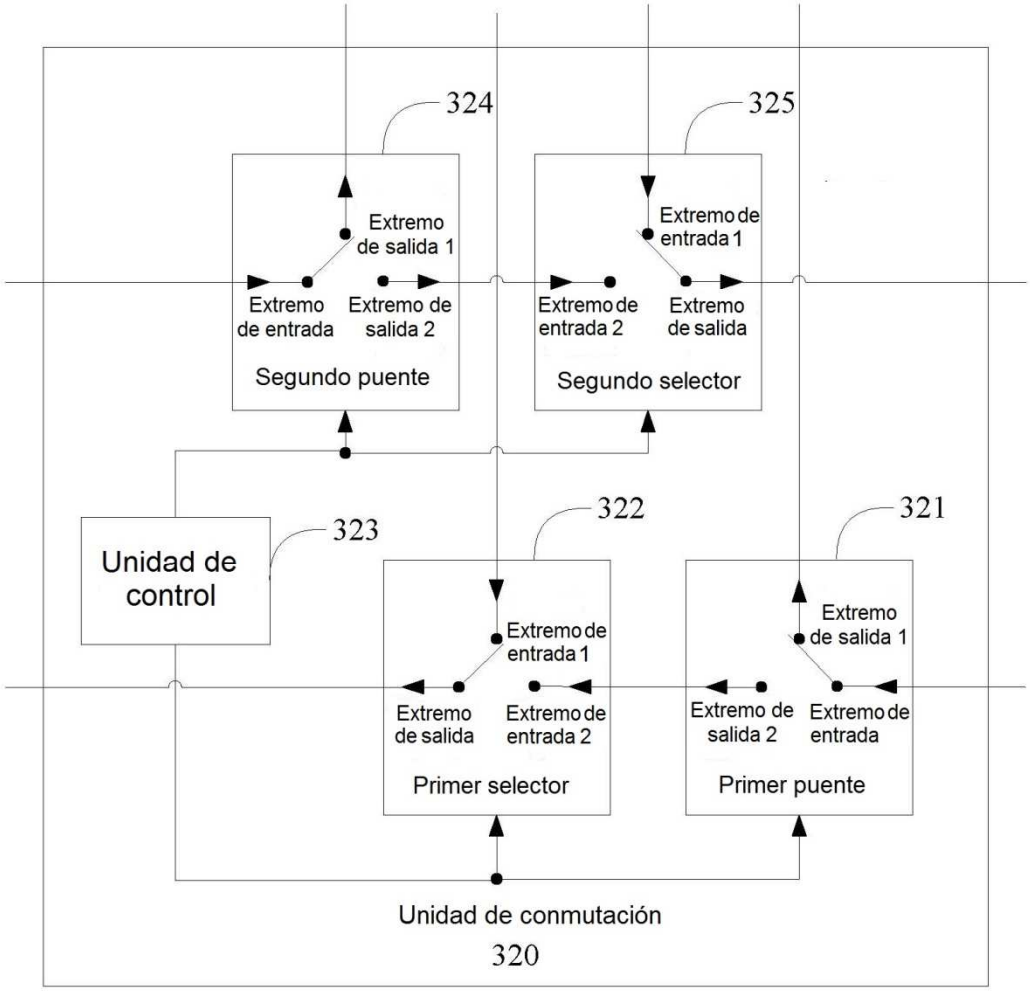
324
325
Extremo de salida 1
Extremo de entrada
Extremo de salida 2
Segundo puente
Extremo de entrada 1
Extremo de entrada 2
Extremo de salida
Segundo selector
Unidad de control
323
322
321
Extremo de entrada 1
Extremo de salida
Extremo de entrada 2
Primer selector
Extremo de salida 1
Extremo de salida 2
Extremo de entrada
Primer puente
Unidad de conmutación
320

FIG. 6b

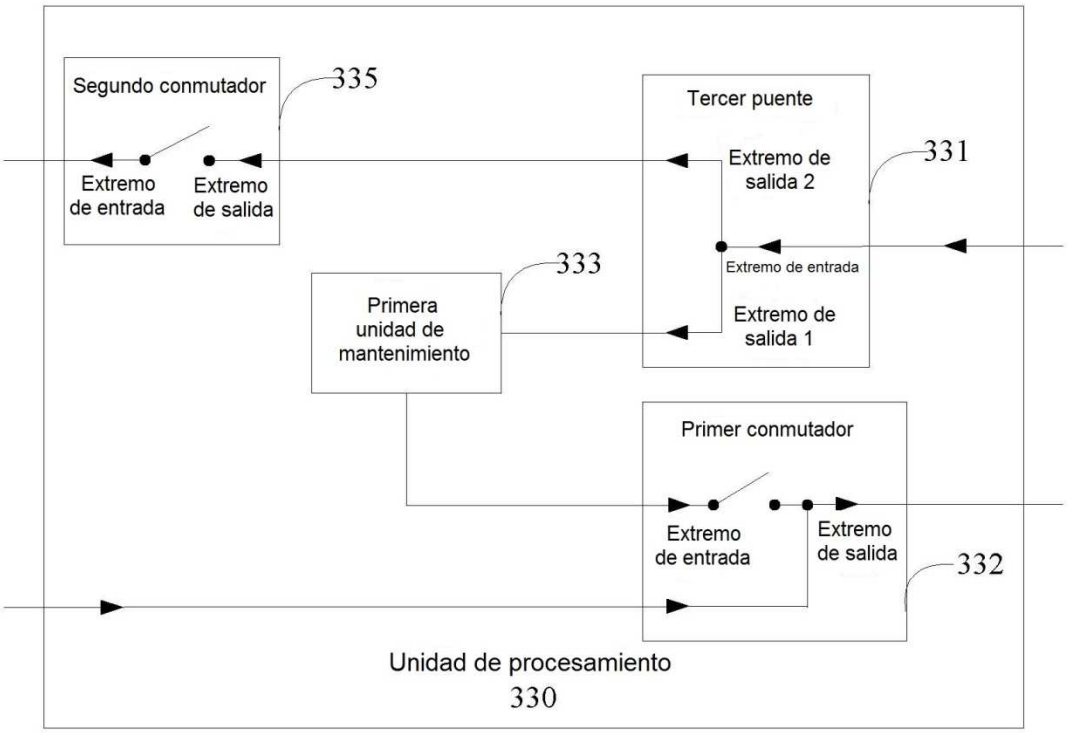
Segundo conmutador
335
Extremo de entrada
Extremo de salida
Tercer puente
Extremo de salida 2
331
Extremo de entrada
Extremo de salida 1
333
Primera unidad de mantenimiento
Primer conmutador
Extremo de entrada
Extremo de salida
332
Unidad de procesamiento
330

FIG. 7a

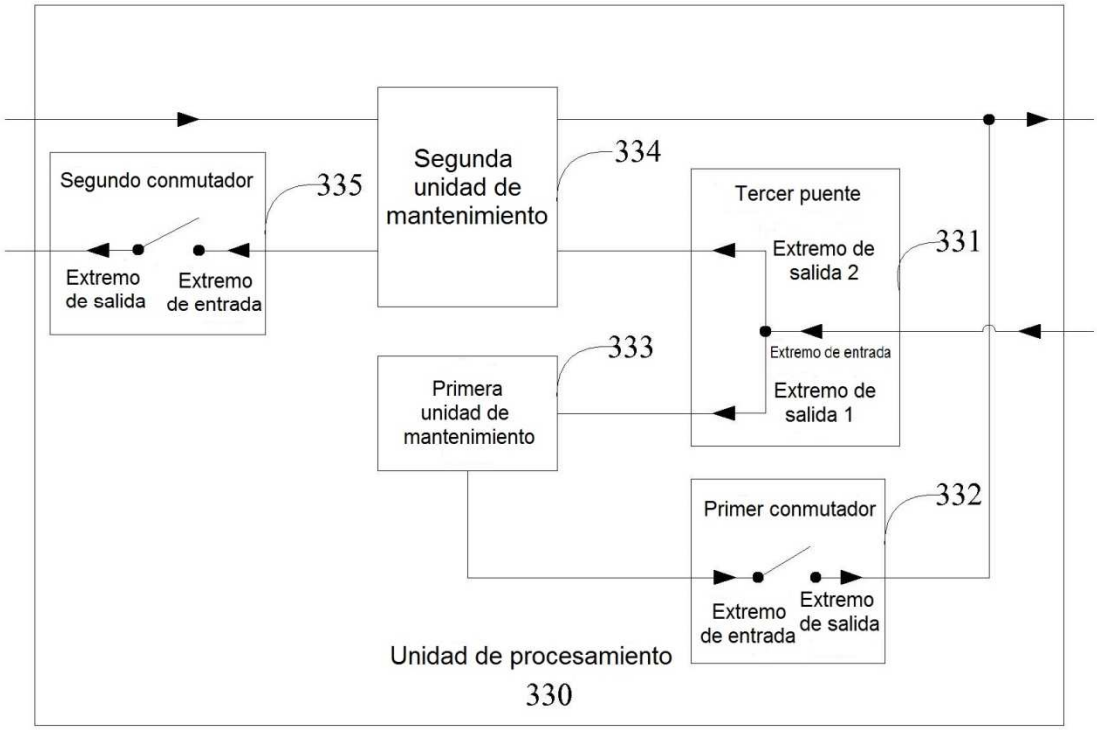
Segundo conmutador
335
Extremo de salida
Extremo de entrada
Segunda unidad de mantenimiento
334
Tercer puente
Extremo de salida 2
331
Extremo de entrada
Extremo de salida 1
333
Primera unidad de mantenimiento
Primer conmutador
332
Extremo de entrada
Extremo de salida
Unidad de procesamiento
330

FIG. 7b

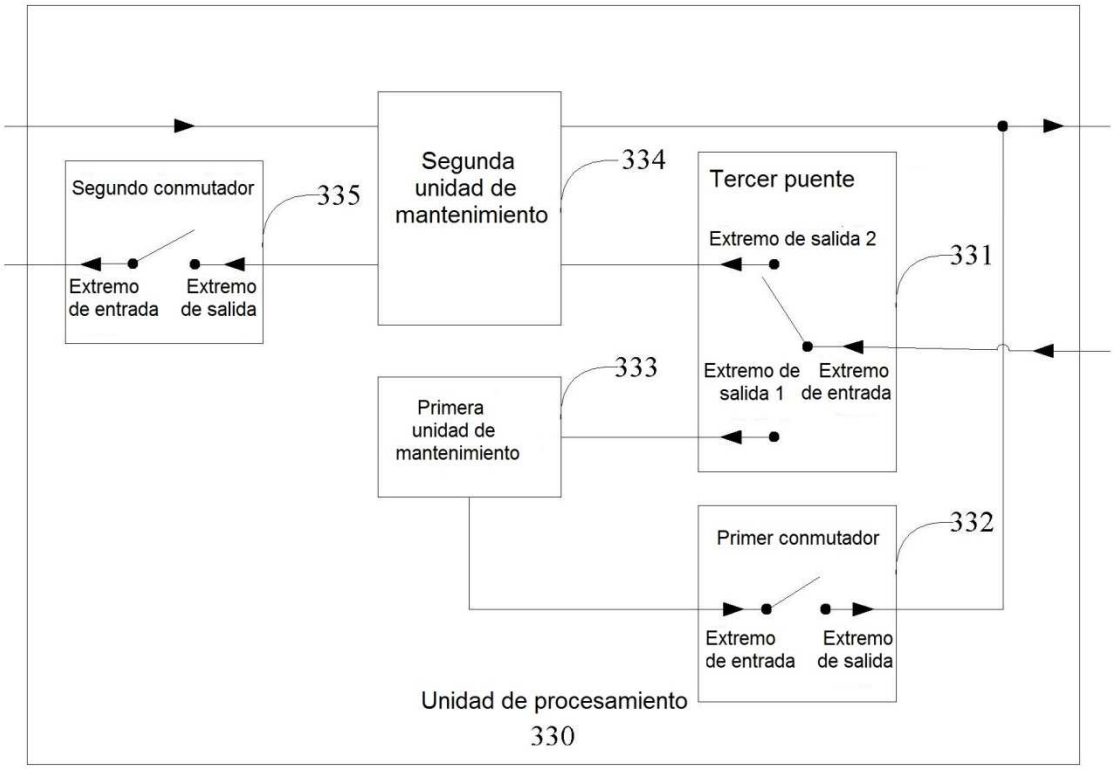
Segundo conmutador
335
Extremo de entrada
Extremo de salida
Segunda unidad de mantenimiento
334
Tercer puente
Extremo de salida 2
331
Extremo de salida 1
Extremo de entrada
333
Primera unidad de mantenimiento
Primer conmutador
332
Extremo de entrada
Extremo de salida
Unidad de procesamiento
330

FIG. 7c

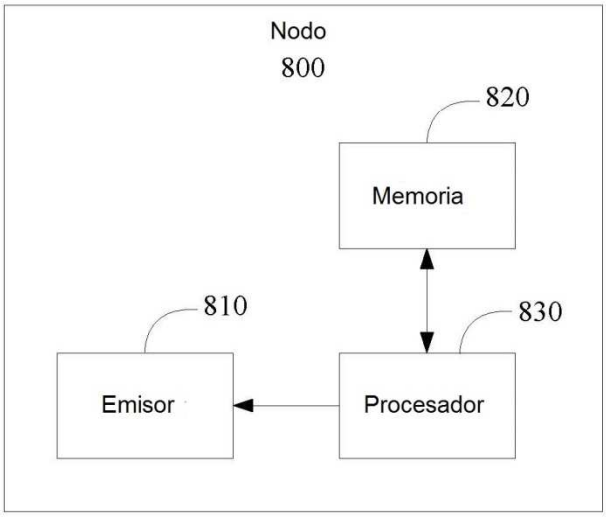
Nodo
800
820
Memoria
810
830
Emisor
Procesador

FIG. 8

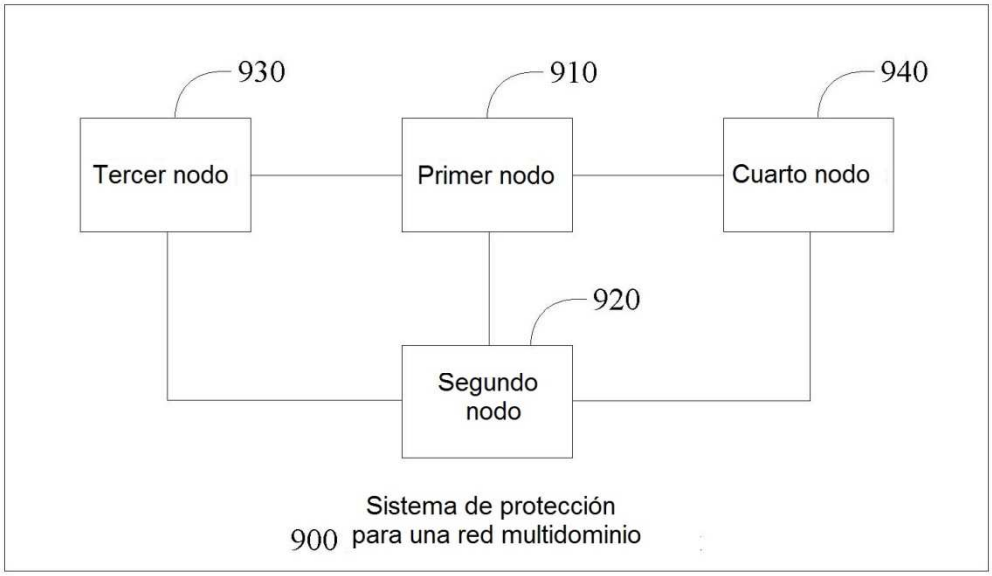
930
910
940
Tercer nodo
Primer nodo
Cuarto nodo
920
Segundo nodo
Sistema de protección
900 para una red multidominio

FIG. 9