(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 731 352**

(51) Int. CI.:

H04L 12/26 (2006.01)
H04L 12/703 (2013.01)
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **24.11.2014 PCT/CN2014/092067**

(87) Fecha y número de publicación internacional: **10.12.2015 WO15184739**

(96) Fecha de presentación y número de la solicitud europea: **24.11.2014 E 14894164 (4)**

(97) Fecha y número de publicación de la concesión europea: **20.03.2019 EP 3211832**

(54) Título: **Método y dispositivo de detección de fallos**

(30) Prioridad:

21.10.2014 CN 201410564306

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
15.11.2019

(73) Titular/es:

ZTE CORPORATION (100.0%)
ZTE Plaza, Keji Road South, Hi-Tech Industrial Park, Nanshan
Shenzhen, Guangdong 518057, CN

(72) Inventor/es:

MENG, WEI y
WANG, CUI

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y dispositivo de detección de fallos

Campo técnico

La divulgación se refiere al campo de las comunicaciones, y en particular a un método y a un dispositivo de detección de fallos.

Antecedentes

El encadenamiento de funciones de servicio (SFC) es una tecnología de red que actualmente se estudia y estandariza. Dado que una red de centro de datos se convierte en una red de superposición, un borde de la red se ha convertido en un punto de demarcación entre una red virtual y una red física. El borde de la red puede ser un servidor o un conmutador ToR o una puerta de enlace. Sin embargo, la tecnología de superposición no puede resolver todos los problemas. Hay muchos middlewares en un centro de datos, tales como, un cortafuegos o equilibrador de carga. Estos dispositivos se procesan en función de los servicios del usuario. Obviamente, es inviable si estos dispositivos se atraviesan a través de un túnel.

Este modelo de implementación en el centro de datos requiere que un cortafuegos virtual o un equilibrador de carga se pueda implementar arbitrariamente en una red, es decir, independientemente de una topología de red; un inconveniente del modelo de implementación es que si el tráfico se puede procesar de manera flexible a través de un cortafuegos virtual o un equilibrador de carga, se generará un nuevo middleware, tal como un cortafuegos virtual o un equilibrador de carga. Estos cortafuegos virtuales o equilibradores de carga se implementan en un borde de una red y pueden lograrse mediante un servidor estándar.

En la técnica relacionada, una función de procesamiento de servicios tal como un cortafuegos virtual, equilibrador de carga o puerta de enlace se conoce como una función de servicio y, después de procesarse a través de una serie de funciones de servicio, el tráfico formará el SFC.

Actualmente, un marco SFC en la técnica relevante se puede clasificar en los siguientes componentes:

1. Servicio de superposición, que es la tecnología de superposición que cada nodo de borde de red necesita para comunicarse;
2. Plano de control de servicio genérico (GSCP), que es un controlador que forma el SFC;
3. Clasificación de servicio, en el que se requiere la identificación del flujo, y luego, un procesamiento de SFC específico se realiza en un flujo específico;
4. Metadatos de plano de datos, que es una característica importante del marco SFC, en el que los metadatos permiten que cada nodo de procesamiento de servicios perimetral intercambie información entre sí, para lograr fines específicos de procesamiento de servicios;
5. Ruta de función de servicios (SFP), en el que la figura 1 es un diagrama esquemático de una ruta de función de servicios de acuerdo con la técnica relacionada; como se muestra en la figura 1, el SFP se inicia desde un clasificador, y luego pasa a través de varias instancias de funciones de servicio, y finalmente llega a una ruta de procesamiento de servicio de destino;
6. El reenviador de funciones de servicio (SFF) en el que los paquetes de datos se transmiten entre los nodos del SFC y encapsulan una capa del encabezado de servicio de red (NSH) del paquete de funciones de servicio fuera de una trama de datos. Este NSH es analizado, encapsulado y desencapsulado por un componente del SFF en un nodo de función de servicio.

En resumen, el SFC es una tecnología de separación de funciones de servicio de dispositivo de red y reenvío, que implementa una operación y procesamiento independiente de las funciones de servicio y mejora el rendimiento de reenvío de un dispositivo de red.

Para proteger aplicaciones críticas, se puede diseñar un cierto número de enlaces de respaldo redundantes en una red. Cuando la red falla, se requiere un dispositivo de red para detectar rápidamente un fallo y cambiar el tráfico a al menos un enlace de respaldo para acelerar la velocidad de convergencia de la red. Actualmente, algunos enlaces logran una detección rápida de fallos a través de un mecanismo de detección de hardware. Sin embargo, algunos enlaces (por ejemplo, enlaces de Ethernet) no tienen tal mecanismo de detección. En este punto, las aplicaciones se basarán en un mecanismo de un protocolo de capa superior para realizar una detección de fallos. Un tiempo de detección del protocolo de la capa superior es de más de 1 segundo, y dicho tiempo de detección de fallos es intolerable para algunas aplicaciones. Aunque algunos protocolos de enrutamiento, como abrir primero la ruta más corta (OSPF), el Protocolo de enrutamiento de estado de enlace (ISIS), tienen una función de saludo rápido para acelerar la velocidad de detección, el tiempo de detección de fallos solo puede alcanzar una precisión de 1 segundo, y la función de saludo rápido es solo para este protocolo y no puede proporcionar una detección rápida de fallos para otros protocolos.

Se genera un protocolo de detección de reenvío bidireccional (BFD) en este contexto, que proporciona un mecanismo de detección rápida de fallos independiente del protocolo e independiente del medio estandarizado común. La BFD establece una sesión en dos dispositivos de red para detectar una ruta de reenvío bidireccional entre estos dos dispositivos de red y proporciona servicios para aplicaciones de capa superior. La BFD no tiene un mecanismo de descubrimiento vecino, pero se basa en aplicaciones de capa superior servidas para informar de la información del vecino de la BFD para establecer una sesión. Una vez establecida la sesión, los paquetes de BFD serán enviados periódicamente. Si los paquetes de BFD no se reciben dentro del tiempo de detección, se considera que la ruta de reenvío bidireccional falla y se informa a las aplicaciones de la capa superior servida de realizar un procesamiento correspondiente.

Sin embargo, hay una falta de un mecanismo de detección de fallos basado en la conectividad de BFD entre varias instancias de funciones de servicio en el SFC en una tecnología SFC existente.

El documento 'Detección de reenvío bidireccional (BFD)' de D. Kartz y D. Ward (XP015070820) divulga un protocolo destinado a detectar fallos en la ruta bidireccional entre dos motores de reenvío, incluyendo interfaces, enlace(s) de datos, y en la medida de lo posible los propios motores de reenvío, con una latencia potencialmente muy baja. El documento US 2007/0180105 divulga una técnica para distinguir entre fallo de enlace y nodo mediante la detección de reenvío bidireccional. El documento US 7.860.981 B1 divulga sistemas y métodos para mantener activa una sesión de Protocolo de Internet (IP) utilizando protocolos de BFD. Sin embargo, el problema mencionado anteriormente sigue sin resolverse.

Sumario

La presente invención proporciona un método de acuerdo con la reivindicación 1 y un dispositivo de acuerdo con la reivindicación 6 para la detección de fallos para resolver un problema de que falte un mecanismo de detección de fallos basado en una conectividad de BFD entre varias instancias de funciones de servicio en un SFC en la técnica relacionada.

En una realización de la divulgación, se proporciona un método para la detección de fallos, que incluye: crear una sesión de detección de reenvío bidireccional (BFD) en una ruta de función de servicio establecida entre una primera instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo local y una segunda instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo opuesto; y realizar la detección de fallos de conectividad mediante la interacción de un paquete de control de BFD entre el nodo de función de servicio de extremo local y el nodo de función de servicio de extremo opuesto.

En una realización a modo de ejemplo, la detección de fallos de conectividad mediante la interacción del paquete de control de BFD incluye: recibir el paquete de control de BFD desde el nodo de la función de servicio del extremo opuesto dentro de un período de tiempo predeterminado especificado por un temporizador, en el que el paquete de control de BFD lleva un número de identificación de la primera instancia de función de servicio; y mantener la sesión de BFD en un estado abierto y restablecer el temporizador en el caso de determinar, según el número de identificación, que la primera instancia de la función de servicio correspondiente al número de identificación en el dominio de administración del nodo de la función de servicio de extremo local está en un estado activo.

En una realización a modo de ejemplo, antes de determinar, según el número de identificación, que la primera instancia de la función de servicio está en el estado activo, el método incluye además: adquirir que un estado de sesión actual local rellenado en un campo de estado de una BFD en el paquete de control de BFD está en el estado abierto actualmente del paquete de control de BFD.

En una realización a modo de ejemplo, la realización de la detección de fallos de conectividad mediante la interacción del paquete de control de BFD incluye: esperar el paquete de control de BFD enviado por el nodo de la función de servicio del extremo opuesto dentro de un período de tiempo predeterminado especificado por un temporizador; y cerrar la sesión de BFD y realizar una operación de cambio de ruta de la función de servicio cuando el paquete de control de BFD no se recibe dentro del período de tiempo preestablecido, e informar al nodo de la función de servicio del extremo opuesto que se produce un fallo de enlace.

En una realización a modo de ejemplo, la realización de la detección de fallos de conectividad mediante la interacción del paquete de control de BFD incluye: cerrar la sesión de BFD y configurar el paquete de control de BFD en el caso de determinar que la primera instancia de la función de servicio en el dominio de administración del nodo de la función de servicio de extremo local ha fallado o se ha cerrado, en el que un estado de sesión actual local rellenado en un campo de estado de una BFD en el paquete de control de BFD se establece en estado cerrado y un número de identificación de la segunda instancia de función de servicio está encapsulado en el paquete de control de BFD; y enviar el paquete de control de BFD al nodo de la función de servicio de extremo opuesto.

En una realización a modo de ejemplo, la creación de la sesión de BFD incluye: agregar un módulo de función de BFD en el dominio de administración del nodo de la función de servicio de extremo local; e informar, mediante el nodo de la función de servicio de extremo local donde se encuentra la primera instancia de la función de servicio, el módulo de

función de BFD de la información de creación de sesión de BFD, en el que la información de creación de sesión de BFD se utiliza para crear, mediante el módulo de función de BFD, la sesión de BFD y la información de creación de sesión de BFD incluye al menos uno de un número de identificación de la primera instancia de función de servicio, un número de identificación de la segunda instancia de la función de servicio, información de identificación del nodo de función de servicio de extremo local, e información de identificación del nodo de función de servicio de extremo local.

En otra realización de la divulgación, se proporciona un dispositivo para la detección de fallos, que incluye: un componente de establecimiento dispuesto para crear una sesión de detección de reenvío bidireccional (BFD) en una ruta de función de servicio establecida entre una primera instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo local y una segunda instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo opuesto; y un componente de detección dispuesto para realizar la detección de fallos de conectividad mediante la interacción de un paquete de control de BFD entre el nodo de función de servicio de extremo local y el nodo de función de servicio de extremo opuesto.

En una realización a modo de ejemplo, el componente de detección incluye: un elemento de recepción dispuesto para recibir el paquete de control de BFD desde el nodo de función de servicio del extremo opuesto dentro de un período de tiempo preestablecido especificado por un temporizador, en el que el paquete de control de BFD lleva un número de identificación de la primera instancia de función de servicio; y un primer elemento de ejecución dispuesto para mantener la sesión de BFD en un estado abierto y restablecer el temporizador en el caso de determinar, según el número de identificación, que la primera instancia de la función de servicio correspondiente al número de identificación en el dominio de administración del nodo de la función de servicio de extremo local está en un estado activo.

En una realización a modo de ejemplo, el componente de detección incluye además: un elemento de adquisición dispuesto para adquirir que un estado de sesión actual local completado en un campo de estado de una BFD en el paquete de control de BFD está actualmente en estado abierto desde el paquete de control de BFD.

En una realización a modo de ejemplo, el componente de detección incluye: un elemento de procesamiento dispuesto para esperar el paquete de control de BFD enviado por el nodo de función de servicio de extremo opuesto dentro de un período de tiempo preestablecido especificado por un temporizador; y un segundo elemento de ejecución dispuesto para cerrar la sesión de BFD y realizar una operación de cambio de ruta de la función de servicio cuando el paquete de control de BFD no se recibe dentro del período de tiempo preestablecido e informar al nodo de la función de servicio del extremo opuesto que se produce un fallo de enlace.

En una realización a modo de ejemplo, el componente de detección incluye: un elemento de configuración dispuesto para cerrar la sesión de BFD y configurar el paquete de control de BFD en el caso de determinar que la primera instancia de función de servicio en el dominio de administración del nodo de función de servicio de extremo local ha fallado o se ha cerrado, en el que un estado de sesión actual local rellenado en un campo de estado de una BFD en el paquete de control de BFD se establece en estado cerrado y un número de identificación de la segunda instancia de función de servicio está encapsulado en el paquete de control de BFD; y un elemento de envío dispuesto para enviar el paquete de control de BFD al nodo de función de servicio de extremo opuesto.

En una realización a modo de ejemplo, el componente de establecimiento incluye: un elemento de adición dispuesto para agregar un módulo de función de BFD en el dominio de administración del nodo de función de servicio de extremo local; y un elemento de información dispuesto para informar, mediante el nodo de la función de servicio de extremo local donde se encuentra la primera instancia de la función de servicio, el módulo de función de BFD de la información de creación de sesión de BFD, en el que la información de creación de sesión de BFD se utiliza para crear, mediante el módulo de función de BFD, la sesión de BFD y la información de creación de sesión de BFD incluye al menos uno de un número de identificación de la primera instancia de función de servicio, un número de identificación de la segunda instancia de la función de servicio, información de identificación del nodo de función de servicio de extremo local, e información de identificación del nodo de función de servicio de extremo local.

De acuerdo con al menos una realización de la divulgación, creando la sesión de BFD en la ruta de la función de servicio establecida entre la primera instancia de la función de servicio en el dominio de administración del nodo de la función de servicio del extremo local y la segunda instancia de la función de servicio en el dominio de administración del nodo de la función de servicio del extremo opuesto; y realizar la detección de fallos de conectividad mediante la interacción con el paquete de control de BFD entre el nodo de función de servicio de extremo local y el nodo de función de servicio de extremo opuesto, se resuelve el problema de que falta el mecanismo de detección de fallos basado en la conectividad de BFD entre varias instancias de funciones de servicio en el SFC en la técnica relacionada, para lograr realizar la detección de conectividad entre instancias de función de servicio en una ruta de función de servicio.

Breve Descripción de los Dibujos

Los dibujos se describen aquí para proporcionar una comprensión adicional de la divulgación y forman parte de la presente solicitud. Las realizaciones esquemáticas ya la descripción de la divulgación se adoptan para explicar la divulgación, y no forman límites inapropiados para la divulgación. En los dibujos:

La figura 1 es un diagrama esquemático de una ruta de función de servicios de acuerdo con la técnica relacionada;
La figura 2 es un diagrama de flujo de un método para la detección de fallos de acuerdo con una realización de la divulgación;
La figura 3 es un diagrama esquemático de la configuración de un número de identificación de una instancia de función de servicio en un paquete de control de BFD de acuerdo con una realización de ejemplo de la divulgación;
La figura 4 es un diagrama de flujo de un nodo de función de servicio en el que una primera instancia de función de servicio está situada como un extremo de recepción de un paquete de control de BFD de acuerdo con una realización de ejemplo de la divulgación;
La figura 5 es un diagrama de flujo de un nodo de función de servicio en el que una primera instancia de función de servicio está situada como un extremo de envío de un paquete de control de BFD de acuerdo con una realización de ejemplo de la divulgación;
La figura 6 es un diagrama esquemático de la realización de una detección de conectividad basada en una ruta de función de servicio de una instancia de función de servicio 1 y una instancia de función de servicio 2 de acuerdo con una primera realización de ejemplo de la divulgación;
La figura 7 es un diagrama esquemático de la realización de una detección de conectividad basada en una ruta de función de servicio de una instancia de función de servicio 1 y una instancia de función de servicio 2 de acuerdo con una segunda realización de ejemplo de la divulgación;
La figura 8 es un diagrama de bloques estructural de un dispositivo para la detección de fallos de acuerdo con una realización de la divulgación; y
La figura 9 es un diagrama de bloques estructural de un dispositivo para la detección de fallos de acuerdo con una realización de ejemplo de la divulgación.

Descripción detallada

La divulgación se describe a continuación con referencia a los dibujos y las realizaciones en detalle. Debe indicarse que las realizaciones en la presente solicitud y las características en las realizaciones pueden combinarse entre sí bajo la condición de que no haya conflictos.

La figura 2 es un diagrama de flujo de un método para la detección de fallos de acuerdo con una realización de la divulgación. Como se muestra en la figura 2, el método puede incluir las siguientes etapas de procedimiento.

Etapa S202: Se crea una sesión de BFD en una ruta de función de servicio establecida entre una primera instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo local y una segunda instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo opuesto.

Etapa S204: La detección de fallos de conectividad se realiza mediante la interacción de un paquete de control de BFD entre el nodo de función de servicio de extremo local y el nodo de función de servicio de extremo opuesto.

Existe una falta de un mecanismo de detección de fallos basado en una conectividad de BFD entre varias instancias de funciones de servicio en un SFC en la técnica relacionada. El método que se muestra en la figura 2 se utiliza para crear la sesión de BFD en la ruta de la función de servicio establecida entre la primera instancia de la función de servicio en el dominio de administración del nodo de la función de servicio de extremo local y la segunda instancia de la función de servicio en el dominio de administración del nodo de función de servicio de extremo opuesto; y ejecutar la detección de fallos de conectividad mediante la interacción del paquete de control de BFD entre el nodo de función de servicio de extremo local y el nodo de función de servicio de extremo opuesto, para resolver el problema que existe la falta de un mecanismo de detección de fallos basado en la conectividad de BFD entre varias instancias de funciones de servicio en el SFC en la técnica relacionada, para lograr realizar la detección de conectividad entre instancias de función de servicio en una ruta de función de servicio.

En una realización a modo de ejemplo, en la Etapa S204, la detección de fallos de conectividad mediante la interacción del paquete de control de BFD puede incluir las siguientes operaciones:

Etapa S1: El paquete de control de BFD se recibe desde el nodo de la función de servicio de extremo opuesto dentro de un período de tiempo predeterminado especificado por un temporizador, en el que el paquete de control de BFD lleva un número de identificación de la primera instancia de la función de servicio.
Etapa S2: La sesión de BFD se mantiene en un estado abierto y el temporizador se restablece en el caso de que el nodo de la función de servicio de extremo local determine, según el número de identificación, que la primera instancia de la función de servicio correspondiente al número de identificación en el dominio de administración del nodo de la función de servicio de extremo local está en un estado activo.

En una realización a modo de ejemplo, en la Etapa S2, antes de determinar, según el número de identificación, que la primera instancia de la función de servicio está en el estado activo, el método también incluye la siguiente etapa.

Etapa S3: Se ha adquirido que un campo de estado de una BFD en el paquete de control de BFD se encuentra actualmente en estado abierto desde el paquete de control de BFD. Por lo tanto, se determina que la segunda instancia de la función de servicio en el segundo nodo de función de servicio no tiene una anomalía o está cerrada. Por lo tanto, la sesión de BFD puede mantenerse continuamente en el caso de determinar al mismo tiempo que la primera instancia de función de servicio en el dominio de administración del nodo de función de servicio de extremo local también se encuentra en el estado activo (es decir, no se produce ninguna anomalía o no está cerrada).

En una realización a modo de ejemplo, la figura 3 es un diagrama esquemático de la configuración de un número de identificación de una instancia de función de servicio en un paquete de control de BFD de acuerdo con una realización de ejemplo de la divulgación. Como se muestra en la figura 3, después del establecimiento de la sesión y la negociación del temporizador se completan para la BFD, cada nodo de función de servicio enviará el paquete de control de BFD en un intervalo negociado y agregará un número de identificación de una instancia de función de servicio de destino en una parte opcional del paquete de control de BFD. Cuando cada nodo de función de servicio recibe el paquete de control de BFD y la instancia de función de servicio representada por el número de identificación de la instancia de función de servicio de destino en el paquete de control de BFD está en el estado activo, se reiniciará un temporizador de detección y la sesión se mantendrá en estado abierto.

En una realización a modo de ejemplo, en la Etapa S204, la realización de la detección de fallos de conectividad mediante la interacción del paquete de control de BFD puede incluir las siguientes etapas:

Etapa S4: El paquete de control de BFD enviado por el nodo de la función de servicio de extremo opuesto se espera dentro de un período de tiempo predeterminado especificado por un temporizador.
Etapa S5: La sesión de BFD se cierra y se realiza una operación de cambio de ruta de la función de servicio cuando el paquete de control de BFD no se recibe dentro del período de tiempo preestablecido, y se informa al nodo de la función de servicio del extremo opuesto que se produce un fallo de enlace.

Cuando el fallo de enlace se produce entre los nodos de la función de servicio, si cada nodo de función de servicio no recibe el paquete de control de BFD dentro del tiempo de detección, la sesión de BFD se moverá al estado cerrado y se informará a las aplicaciones relevantes de que el enlace de extremo opuesto falla para cerrar la sesión e informar a un componente de gestión sobre la toma de medidas, tal como conmutación de ruta de SFP.

La figura 4 es un diagrama de flujo de un nodo de función de servicio en el que una primera instancia de función de servicio está situada como un extremo de recepción de un paquete de control de BFD de acuerdo con una realización de ejemplo de la divulgación. Como se muestra en la figura 4, el flujo puede incluir las siguientes etapas de procedimiento:

Etapa S402: El paquete de control de BFD enviado por el nodo de función de servicio de extremo opuesto se espera dentro del período de tiempo preestablecido especificado por el temporizador para determinar si el paquete de control de BFD anterior se recibe dentro del tiempo preestablecido; si el paquete de control de BFD anterior se recibe dentro del tiempo preestablecido, el flujo pasa a la Etapa S404; si el paquete de control de BFD anterior no se recibe dentro del tiempo preestablecido, el flujo vuelve a la Etapa S408.
Etapa S404: El paquete de control de BFD enviado por el nodo de la función de servicio de extremo opuesto se recibe dentro del período de tiempo preestablecido especificado por el temporizador.
Etapa S406: Se determina si el campo de estado de la BFD en el paquete de control de BFD está configurado para estar en un estado cerrado y un número de identificación de la segunda instancia de función de servicio está encapsulado en el paquete de control de BFD; si el campo de estado de la BFD en el paquete de control de BFD está configurado para estar en estado cerrado y el número de identificación de la segunda instancia de la función de servicio está encapsulado en el paquete de control de BFD, el flujo pasa a la Etapa S408; si el campo de estado de la BFD en el paquete de control de BFD no está configurado para estar en un estado cerrado o el número de identificación de la segunda instancia de la función de servicio no está encapsulado en el paquete de control de BFD, el flujo vuelve a la Etapa S412.
Etapa S408: La sesión de BFD se mueve al estado cerrado y, a continuación, la sesión de BFD se cierra.
Etapa S410: El componente de gestión está informado de tomar medidas como la conmutación de ruta del SFP; y el flujo termina.
Etapa S412: Cuando la instancia de función de servicio representada por el número de identificación de la instancia de función de servicio de destino en el paquete de control de BFD está en el estado activo, se reiniciará el temporizador de detección y la sesión se mantendrá en un estado abierto; y el flujo termina.

En una realización a modo de ejemplo, en la Etapa S204, la realización de la detección de fallos de conectividad mediante la interacción del paquete de control de BFD puede incluir las siguientes operaciones:

Etapa S6: La sesión de BFD se cierra y el paquete de control de BFD se configura en el caso de determinar que la primera instancia de la función de servicio en el dominio de administración del nodo de la función de servicio de

extremo local ha fallado o se ha cerrado, además, un campo de estado de una BFD en el paquete de control de BFD está configurado para estar en un estado cerrado y un número de identificación de la segunda instancia de la función de servicio está encapsulado en el paquete de control de BFD.
Etapa S7: El paquete de control de BFD se envía al nodo de la función de servicio de extremo opuesto.

Cuando una instancia de la función de servicio de uno de los nodos de la función de servicio falla o se cierra, el nodo de la función de servicio cierra la sesión. Y cuando se envía el paquete de control de BFD, un estado de sesión actual local se completará en el campo de estado de la BFD, el estado se establece para cerrarse, el número de identificación de la instancia de la función de servicio de destino está encapsulado y se envía al nodo de la función de servicio de extremo opuesto. Después de recibir el paquete de control de BFD, el nodo de la función de servicio de extremo opuesto cerrará la sesión e informará al componente de administración de tomar medidas como el cambio de ruta del SFP.

La figura 5 es un diagrama de flujo de un nodo de función de servicio en el que una primera instancia de función de servicio está situada como un extremo de envío de un paquete de control de BFD de acuerdo con una realización de ejemplo de la divulgación. Como se muestra en la figura 5, el flujo puede incluir las siguientes etapas de procedimiento:

Etapa S502: Se determina si la primera instancia de la función de servicio dentro del nodo de la función de servicio de extremo local ha fallado o se ha cerrado; si la primera instancia de la función de servicio ha fallado o se ha cerrado, el flujo pasa a la Etapa S504; si la primera instancia de la función de servicio no falla y no se cierra, el flujo vuelve a la Etapa S508.
Etapa S504: La sesión de BFD se cierra cuando se determina que la primera instancia de la función de servicio ha fallado o se ha cerrado.
Etapa S506: El campo de estado de BFD en el paquete de control de BFD está configurado para estar en el estado cerrado.
Etapa S508: El paquete de control de BFD se envía al nodo de la función de servicio de extremo opuesto; y el flujo termina.

En un ejemplo, en la Etapa S202, la creación de la sesión de BFD puede incluir las siguientes etapas.

Etapa S7: Se agrega un componente de función de BFD en el dominio de administración del nodo de función de servicio de extremo local.

Etapa S8: El nodo de la función de servicio de extremo local donde se ubica la primera instancia de la función de servicio informa al componente de la función de BFD de la información de creación de sesión de BFD, además, la información de creación de sesión de BFD se utiliza para crear, mediante el componente de función de BFD, la sesión de BFD y la información de creación de sesión de BFD pueden incluir, pero no limitado a, al menos uno de:

(1) un número de identificación de la primera instancia de función de servicio;
(2) un número de identificación de la segunda instancia de la función de servicio;
(3) información de identificación del nodo de función de servicio de extremo local; y
(4) información de identificación del nodo de función de servicio de extremo opuesto.

Una entidad par se forma entre dos instancias de función de servicio que requieren detección de BFD, y la configuración del protocolo de BFD asociado y el enlace del SFP y de BFD están vinculados. Cuando se establece un nuevo SFP y el SFP contiene las dos instancias de funciones de servicio anteriores, el nodo de la función de servicio donde se ubica la instancia de la función de servicio puede informar a BFD de la información de dos instancias de la función de servicio y las rutas de la función de servicio.

La información anterior puede incluir, pero no limitado a, el número de identificación de la instancia de la función de servicio de origen, el número de identificación de la instancia de la función de servicio de destino, la ruta de la función de servicio, la dirección de Protocolo de Internet (IP) del nodo de función de servicio de origen y la dirección IP del nodo de función de servicio de destino.

La dirección IP del nodo de la función de servicio de origen anterior es la dirección IP del nodo de la función de servicio donde se encuentra la instancia de la función de servicio anterior; la dirección IP del nodo de la función de servicio de destino anterior es la dirección IP del nodo de la función de servicio donde se encuentra la instancia de la función de servicio del extremo opuesto.

Además, la BFD establece una sesión basada en la información del vecino recibido. La información de sesión puede incluir, pero no limitado a, el número de identificación de la instancia de la función de servicio de origen, el número de identificación de la instancia de la función de servicio de destino, la dirección IP del nodo de función de servicio de origen y la dirección IP del nodo de función de servicio de destino.

Las realizaciones de ejemplo descritas anteriormente se describirán adicionalmente a continuación con referencia a las realizaciones preferidas mostradas en las figuras 6 y 7.

En general, el error de conectividad entre las instancias de la función de servicio suele deberse a los dos motivos siguientes:

una primera razón: un enlace entre los nodos de la función de servicio falla, es decir, falla un enlace físico o virtual entre los nodos de la función de servicio; y
una segunda razón: una instancia de función de servicio falla o se cierra, es decir, un enlace entre los nodos de la función de servicio puede estar intacto, pero la instancia de la función de servicio no puede funcionar correctamente debido a un hecho que la instancia de la función de servicio está cerrada de manera iniciática por un usuario, la instancia de la función de servicio se suspende, etc.

La figura 6 es un diagrama esquemático de la realización de una detección de conectividad basada en una ruta de función de servicio de una instancia de función de servicio 1 y una instancia de función de servicio 2 de acuerdo con una primera realización de ejemplo de la divulgación. Como se muestra en la figura 6, se establece un mecanismo de detección basado en la conectividad de BFD entre la instancia de la función de servicio 1 y la instancia de la función de servicio 2. Después de un período de operación estable, un nodo 1 daña una tarjeta de red, resultando en un fallo de enlace. Específicamente, Se pueden incluir las siguientes etapas de procesamiento.

Etapa 1: Se configura un mecanismo de detección de BFD y se configura un SFC de enlace en un nodo de función de servicio 1 donde se encuentra la instancia de función de servicio 1 y un nodo de función de servicio 2 donde se ubica la instancia de función de servicio 2.
Etapa 2: Después de crear un SFP que contiene la instancia de la función de servicio 1 y la instancia de la función de servicio 2, la instancia de la función de servicio 1 informa a un componente de BFD del nodo 1 de la función de servicio que requiere la creación de una sesión. Al mismo tiempo, la instancia de la función de servicio 2 informa al componente BFD del nodo 2 de la función de servicio que también requiere la creación de una sesión.
Etapa 3: La BFD crea con éxito una sesión basada en las dos instancias de función de servicio. El número de identificación de la instancia de función de servicio 1 es 1000, el número de identificación de la instancia de función de servicio 2 es 2000, la dirección IP del nodo 1 de la función de servicio es 192.168.1.1, y la dirección IP del nodo 2 de la función de servicio es 192.178.1.1.
Etapa 4: El nodo 1 de la función de servicio comprueba que el proceso de la instancia 1 de la función de servicio funciona normalmente, envía el paquete de control de BFD al nodo de la función de servicio 2 periódicamente y encapsula el elemento opcional en el que el número de identificación de la instancia de la función de servicio 2 es 2000; el nodo 2 de la función de servicio comprueba que el proceso de la instancia 2 de la función de servicio opera normalmente, envía el paquete de control de BFD al nodo de la función de servicio 1 regularmente y encapsula el elemento opcional en el que el número de identificación de la instancia de la función de servicio 1 es 1000.
Etapa 5: El nodo 1 de la función de servicio recibe el paquete de control BFD enviado por la otra parte en el tiempo configurado, determina que la instancia de la función de servicio con el número de identificación de 1000 opera normalmente, restablece el temporizador y mantiene la sesión en el estado activo; y el nodo de función de servicio 2 recibe el paquete de control BFD enviado por la otra parte en el tiempo configurado, determina que la instancia de la función de servicio con el número de identificación de 2000 opera normalmente, restablece el temporizador y mantiene la sesión en el estado activo.
Etapa 6: El nodo de función de servicio 1 tiene un fallo de enlace. Etapa 7: El nodo 2 de la función de servicio no puede recibir el paquete de control de BFD enviado por la otra parte en el tiempo configurado. Por lo tanto, la sesión se cierra y se informa a la aplicación relevante de realizar el cambio de ruta de SFP.

La figura 7 es un diagrama esquemático de la realización de una detección de conectividad basada en una ruta de función de servicio de una instancia de función de servicio 1 y una instancia de función de servicio 2 de acuerdo con una segunda realización de ejemplo de la divulgación. Como se muestra en la figura 7, se establece un mecanismo de detección basado en la conectividad de BFD entre la instancia de la función de servicio 1 y la instancia de la función de servicio 2. Después de un período de operación estable, un operador cierra manualmente la instancia de función de servicio 2. Específicamente, Se pueden incluir las siguientes etapas de procesamiento.

Etapa 1: Se configura un mecanismo de detección de BFD y se configura un SFC de enlace en un nodo de función de servicio 1 donde se encuentra la instancia de función de servicio 1 y un nodo de función de servicio 2 donde se ubica la instancia de función de servicio 2.
Etapa 2: Después de crear un SFP que contiene la instancia de la función de servicio 1 y la instancia de la función de servicio 2, la instancia de la función de servicio 1 informa a un componente de BFD del nodo 1 de la función de servicio que requiere la creación de una sesión. Al mismo tiempo, la instancia de la función de servicio 2 informa al componente BFD del nodo 2 de la función de servicio que también requiere la creación de una sesión.
Etapa 3: La BFD crea con éxito una sesión basada en las dos instancias de función de servicio. El número de identificación de la instancia de función de servicio 1 es 1000, el número de identificación de la instancia de función de servicio 2 es 2000, la dirección IP del nodo 1 de la función de servicio es 192.168.1.1, y la dirección IP del nodo 2 de la función de servicio es 192.178.1.1.
Etapa 4: El nodo 1 de la función de servicio comprueba que el proceso de la instancia 1 de la función de servicio funciona normalmente, envía el paquete de control de BFD al nodo de la función de servicio 2 periódicamente y encapsula el elemento opcional en el que el número de identificación de la instancia de la función de servicio 2 es

2000; el nodo 2 de la función de servicio comprueba que el proceso de la instancia 2 de la función de servicio opera normalmente, envía el paquete de control de BFD al nodo de la función de servicio 1 regularmente y encapsula el elemento opcional en el que el número de identificación de la instancia de la función de servicio 1 es 1000.

Etapa 5: El nodo 1 de la función de servicio recibe el paquete de control BFD enviado por la otra parte en el tiempo configurado, determina que la instancia de la función de servicio con el número de identificación de 1000 opera normalmente, restablece el temporizador y mantiene la sesión en el estado activo; y el nodo de función de servicio 2 recibe el paquete de control BFD enviado por la otra parte en el tiempo configurado, determina que la instancia de la función de servicio con el número de identificación de 2000 opera normalmente, restablece el temporizador y mantiene la sesión en el estado activo.

Etapa 6: El operador cierra manualmente la instancia de función de servicio 2.

Etapa 7: El nodo 2 de la función de servicio comprueba que el proceso de la instancia 2 de la función de servicio está cerrado, establece el campo de estado del paquete de control de BFD como inactivo, envía el paquete de control de BFD al nodo 1 de la función de servicio y cierra la sesión al mismo tiempo.

Etapa 8: El nodo 1 de la función de servicio no puede recibir el paquete de control de BFD enviado por la otra parte en el tiempo configurado, pero un valor del campo de estado del paquete se ha configurado para cerrarse.

Etapa 9: El nodo de función de servicio 1 cierra la sesión e informa a las aplicaciones relevantes sobre cómo realizar el cambio de ruta de SFP.

La figura 8 es un diagrama de bloques estructural de un dispositivo para la detección de fallos de acuerdo con una realización de la divulgación. Como se muestra en la figura 8, el dispositivo de detección de fallos puede incluir un componente de establecimiento 10 dispuesto para crear una sesión de BFD en una ruta de función de servicio establecida entre una primera instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo local y una segunda instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo opuesto; y un componente de detección 20 dispuesto para realizar la detección de fallos de conectividad mediante la interacción de un paquete de control de BFD entre el nodo de función de servicio de extremo local y el nodo de función de servicio de extremo opuesto.

El dispositivo como se muestra en la figura 8 se usa para resolver el problema de que falta un mecanismo de detección de fallos basado en la conectividad de BFD entre varias instancias de funciones de servicio en el SFC en la técnica relacionada, para lograr realizar la detección de conectividad entre instancias de función de servicio en una ruta de función de servicio.

Preferentemente, como se muestra en la figura 9, el componente de detección 20 puede incluir: un elemento de recepción 200 dispuesto para recibir el paquete de control de BFD desde el nodo de función de servicio del extremo opuesto dentro de un período de tiempo preestablecido especificado por un temporizador, en el que el paquete de control de BFD lleva un número de identificación de la primera instancia de función de servicio; y un primer elemento de ejecución 202 dispuesto para mantener la sesión de BFD en un estado abierto y restablecer el temporizador en el caso de determinar, según el número de identificación, que la primera instancia de la función de servicio correspondiente al número de identificación en el dominio de administración del nodo de la función de servicio de extremo local está en un estado activo.

En una realización a modo de ejemplo, como se muestra en la figura 9, el componente de detección 20 puede incluir: un elemento de adquisición 204 dispuesto para adquirir que un campo de estado de una BFD en el paquete de control de BFD está actualmente en estado abierto desde el paquete de control de BFD.

En una realización a modo de ejemplo, como se muestra en la figura 9, el componente de detección 20 puede incluir: un elemento de procesamiento 206 dispuesto para esperar el paquete de control de BFD enviado por el nodo de función de servicio de extremo opuesto dentro de un período de tiempo preestablecido especificado por un temporizador; y un segundo elemento de ejecución 208 dispuesto para cerrar la sesión de BFD y realizar una operación de cambio de ruta de la función de servicio cuando el paquete de control de BFD no se recibe dentro del período de tiempo preestablecido e informar al nodo de la función de servicio del extremo opuesto que se produce un fallo de enlace.

En una realización a modo de ejemplo, como se muestra en la figura 9, el componente de detección 20 puede incluir: un elemento de configuración 210 dispuesto para cerrar la sesión de BFD y configurar el paquete de control de BFD en el caso de determinar que la primera instancia de función de servicio en el dominio de administración del nodo de función de servicio de extremo local ha fallado o se ha cerrado, además, un campo de estado de una BFD en el paquete de control de BFD está configurado para estar en un estado cerrado y un número de identificación de la segunda instancia de la función de servicio está encapsulado en el paquete de control de BFD; y un elemento de envío 212 dispuesto para enviar el paquete de control de BFD al nodo de función de servicio de extremo opuesto.

En una realización a modo de ejemplo, como se muestra en la figura 9, el componente de establecimiento 10 puede incluir: un elemento de adición 100 dispuesto para agregar un componente de función de BFD en el dominio de administración del nodo de función de servicio de extremo local; y un elemento de información 102 dispuesto para informar, mediante el nodo de la función de servicio de extremo local donde se encuentra la primera instancia de la función de servicio, el componente de función de BFD de la información de creación de sesión de BFD, En el que la información de creación de sesión de BFD se utiliza para crear, mediante el componente de función de BFD, la sesión de BFD y la información de creación de sesión de BFD incluye al menos uno de un número de identificación de la primera instancia de función de servicio, un número de identificación de la segunda instancia de la función de servicio, información de identificación del nodo de función de servicio de extremo local, e información de identificación del nodo de función de servicio de extremo local.

A partir de la descripción anterior, se puede ver que las realizaciones anteriores logran los siguientes efectos técnicos (debe observarse que estos efectos son los que pueden lograrse mediante ciertas realizaciones preferidas): la solución técnica proporcionada por las realizaciones de la divulgación proporciona una manera del enlace de tecnología de detección de SFC y BFD para lograr la detección de fallos entre los nodos de la función de servicio.

Obviamente, los expertos en la materia deben saber que cada uno de los componentes anteriores o etapa de la divulgación puede implementarse mediante un dispositivo informático universal, y los componentes o etapas pueden concentrarse en un solo dispositivo informático o distribuirse en una red formada por una pluralidad de dispositivos informáticos, y puede implementarse opcionalmente mediante códigos programables ejecutables para los dispositivos informáticos, para que los componentes o etapas puedan almacenarse en un dispositivo de almacenamiento para su ejecución con los dispositivos informáticos, y, en algunos casos, las etapas mostradas o descritas pueden realizarse en un orden diferente del orden en el presente documento, o los componentes o etapas pueden formar cada componente del circuito integrado, o múltiples componentes o etapas en el mismo pueden formar un solo componente de circuito integrado para su implementación. Como consecuencia, la divulgación no se limita a ninguna combinación específica de hardware y software.

Lo anterior son solamente realizaciones de ejemplo de la divulgación y no pretende limitar la divulgación, y para los técnicos en el campo, la divulgación puede tener diversas modificaciones y variaciones.

Aplicabilidad industrial

Como se ha descrito anteriormente, un método y dispositivo para la detección de fallos proporcionado de acuerdo con al menos una realización de la divulgación tienen los siguientes efectos ventajosos: se crea una sesión de detección de reenvío bidireccional (BFD) en una ruta de función de servicio establecida entre una primera instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo local y una segunda instancia de función de servicio en un dominio de gestión de un nodo de función de servicio de extremo opuesto; y la detección de fallos de conectividad se realiza mediante la interacción de un paquete de control de BFD entre el nodo de la función de servicio del extremo local y el nodo de la función de servicio del extremo opuesto para lograr la detección de conectividad entre las instancias de la función de servicio en una ruta de la función de servicio.

REIVINDICACIONES

1. Un método para detección de fallos, que comprende:

crear una sesión de detección de reenvío bidireccional (BFD) en una ruta de función de servicio establecida entre una primera instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo local y una segunda instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo opuesto (S202); y
realizar la detección de fallos de conectividad mediante la interacción de un paquete de control de BFD entre el nodo de función de servicio de extremo local y el nodo de función de servicio de extremo opuesto (S204);
caracterizado porque realizar la detección de fallos de conectividad mediante la interacción del paquete de control de BFD (S204) comprende: recibir el paquete de control de BFD desde el nodo de función de servicio del extremo opuesto dentro de un período de tiempo predeterminado especificado por un temporizador, en el que el paquete de control de BFD lleva un número de identificación de la primera instancia de función de servicio; y mantener la sesión de BFD en un estado abierto y restablecer el temporizador en el caso de determinar que la primera instancia de función de servicio correspondiente al número de identificación en el dominio de administración del nodo de función de servicio de extremo local está en un estado activo.

2. El método de acuerdo con la reivindicación 1, en el que antes de determinar, que la primera instancia de la función de servicio está en el estado activo, el método comprende además: adquirir que un estado de sesión actual local rellenado en un campo de estado de una BFD en el paquete de control de BFD está en el estado abierto actualmente del paquete de control de BFD.

3. El método de acuerdo con la reivindicación 1, en el que realizar la detección de fallos de conectividad mediante la interacción del paquete de control de BFD (S204) comprende:

esperar el paquete de control de BFD enviado por el nodo de la función de servicio de extremo opuesto dentro de un período de tiempo preestablecido especificado por un temporizador; y
cerrar la sesión de BFD y realizar una operación de cambio de ruta de la función de servicio cuando el paquete de control de BFD no se recibe dentro del período de tiempo preestablecido, e informar al nodo de la función de servicio del extremo opuesto que se produce un fallo de enlace.

4. El método de acuerdo con la reivindicación 1, en el que realizar la detección de fallos de conectividad mediante la interacción del paquete de control de BFD (S204) comprende:

cerrar la sesión de BFD y configurar el paquete de control de BFD en el caso de determinar que la primera instancia de la función de servicio en el dominio de administración del nodo de la función de servicio de extremo local ha fallado o se ha cerrado, en el que un estado de sesión actual local rellenado en un campo de estado de una BFD en el paquete de control de BFD se establece en estado cerrado y un número de identificación de la segunda instancia de función de servicio está encapsulado en el paquete de control de BFD; y
enviar el paquete de control de BFD al nodo de la función de servicio de extremo opuesto.

5. El método de acuerdo con la reivindicación 1, en el que crear la sesión de BFD comprende:

agregar un módulo de función de BFD en el dominio de administración del nodo de la función de servicio de extremo local; e
informar, mediante el nodo de la función de servicio de extremo local donde se encuentra la primera instancia de la función de servicio, el módulo de función de BFD de la información de creación de sesión de BFD, en el que la información de creación de sesión de BFD se utiliza para crear, mediante el módulo de función de BFD, la sesión de BFD y la información de creación de sesión de BFD comprende al menos uno de un número de identificación de la primera instancia de función de servicio, un número de identificación de la segunda instancia de la función de servicio, información de identificación del nodo de función de servicio de extremo local, e información de identificación del nodo de función de servicio de extremo local.

6. Un dispositivo de detección de fallos, que comprende:

un componente de establecimiento (10) dispuesto para crear una sesión de detección de reenvío bidireccional (BFD) en una ruta de función de servicio establecida entre una primera instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo local y una segunda instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo opuesto; y
un componente de detección (20) dispuesto para realizar la detección de fallos de conectividad mediante la interacción de un paquete de control de BFD entre el nodo de función de servicio de extremo local y el nodo de función de servicio de extremo opuesto;
caracterizado por que el componente de detección comprende: un elemento de recepción dispuesto para recibir el paquete de control de BFD desde el nodo de función de servicio del extremo opuesto dentro de un período de tiempo preestablecido especificado por un temporizador, en el que el paquete de control de BFD lleva un número

de identificación de la primera instancia de función de servicio; y un primer elemento de ejecución dispuesto para mantener la sesión de BFD en un estado abierto y reiniciar el temporizador en el caso de determinar que la primera instancia de función de servicio correspondiente al número de identificación en el dominio de administración del nodo de función de servicio de extremo local está en una estado activo.

7. El dispositivo según la reivindicación 6, en el que el componente de detección (20) comprende además:
un elemento de adquisición (204) dispuesto para adquirir que un estado de sesión actual local rellenado en un campo de estado de una BFD en el paquete de control de BFD está actualmente en estado abierto desde el paquete de control de BFD.

8. El dispositivo según la reivindicación 6, en el que el componente de detección (20) comprende:

un elemento de procesamiento (206) dispuesto para esperar el paquete de control de BFD enviado por el nodo de función de servicio de extremo opuesto dentro de un período de tiempo preestablecido especificado por un temporizador; y
un segundo elemento de ejecución (208) dispuesto para cerrar la sesión de BFD y realizar una operación de cambio de ruta de la función de servicio cuando el paquete de control de BFD no se recibe dentro del período de tiempo preestablecido e informar al nodo de la función de servicio del extremo opuesto que se produce un fallo de enlace.

9. El dispositivo según la reivindicación 6, en el que el componente de detección (20) comprende:

un elemento de configuración (210) dispuesto para cerrar la sesión de BFD y configurar el paquete de control de BFD en el caso de determinar que la primera instancia de función de servicio en el dominio de administración del nodo de función de servicio de extremo local ha fallado o se ha cerrado, en el que un estado de sesión actual local rellenado en un campo de estado de una BFD en el paquete de control de BFD se establece en estado cerrado y un número de identificación de la segunda instancia de función de servicio está encapsulado en el paquete de control de BFD; y
un elemento de envío (212) dispuesto para enviar el paquete de control de BFD al nodo de función de servicio de extremo opuesto.

10. El dispositivo según la reivindicación 6, en el que el componente de establecimiento (10) comprende:

un elemento de adición (100) dispuesto para agregar un módulo de función de BFD en el dominio de administración del nodo de función de servicio de extremo local; y
un elemento de información (102) dispuesto para informar, mediante el nodo de la función de servicio de extremo local donde se encuentra la primera instancia de la función de servicio, el módulo de función de BFD de la información de creación de sesión de BFD, en el que la información de creación de sesión de BFD se utiliza para crear, mediante el módulo de función de BFD, la sesión de BFD y la información de creación de sesión de BFD comprende al menos uno de un número de identificación de la primera instancia de función de servicio, un número de identificación de la segunda instancia de la función de servicio, información de identificación del nodo de función de servicio de extremo local, e información de identificación del nodo de función de servicio de extremo local.

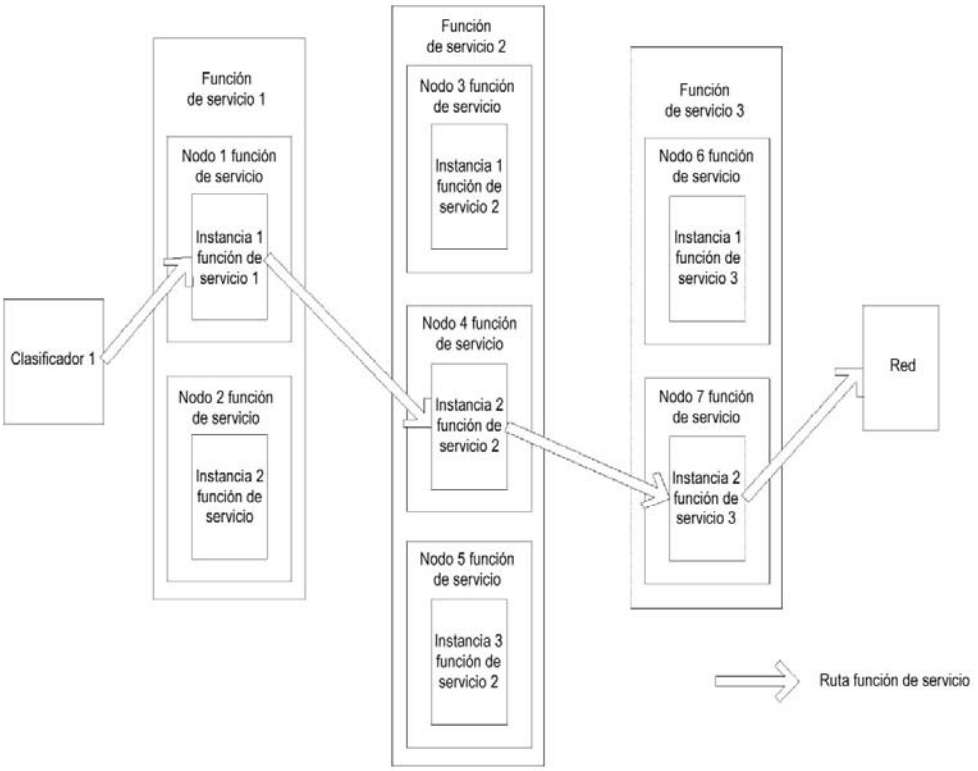
Función de servicio 1
Nodo 1 función de servicio
Instancia 1 función de servicio 1
Nodo 2 función de servicio
Instancia 2 función de servicio
Función de servicio 2
Nodo 3 función de servicio
Instancia 1 función de servicio 2
Nodo 4 función de servicio
Instancia 2 función de servicio 2
Nodo 5 función de servicio
Instancia 3 función de servicio 2
Función de servicio 3
Nodo 6 función de servicio
Instancia 1 función de servicio 3
Nodo 7 función de servicio
Instancia 2 función de servicio 3
Clasificador 1
Red
Ruta función de servicio

Fig. 1

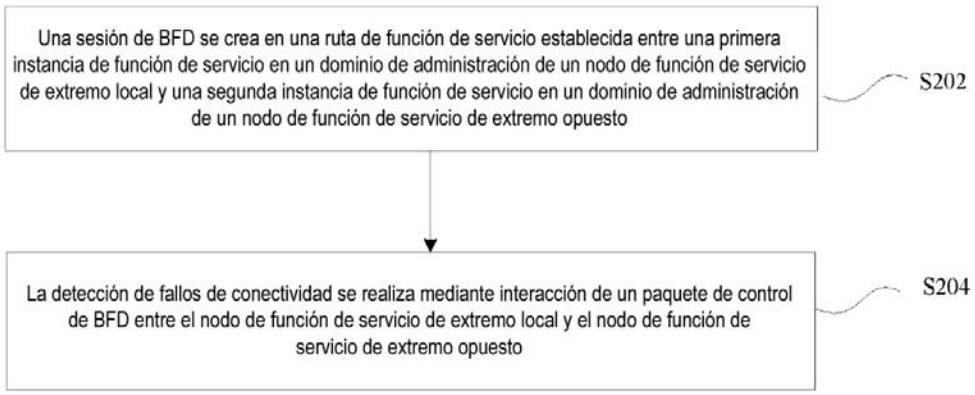
Una sesión de BFD se crea en una ruta de función de servicio establecida entre una primera instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo local y una segunda instancia de función de servicio en un dominio de administración de un nodo de función de servicio de extremo opuesto
S202
La detección de fallos de conectividad se realiza mediante interacción de un paquete de control de BFD entre el nodo de función de servicio de extremo local y el nodo de función de servicio de extremo opuesto
S204

Fig. 2

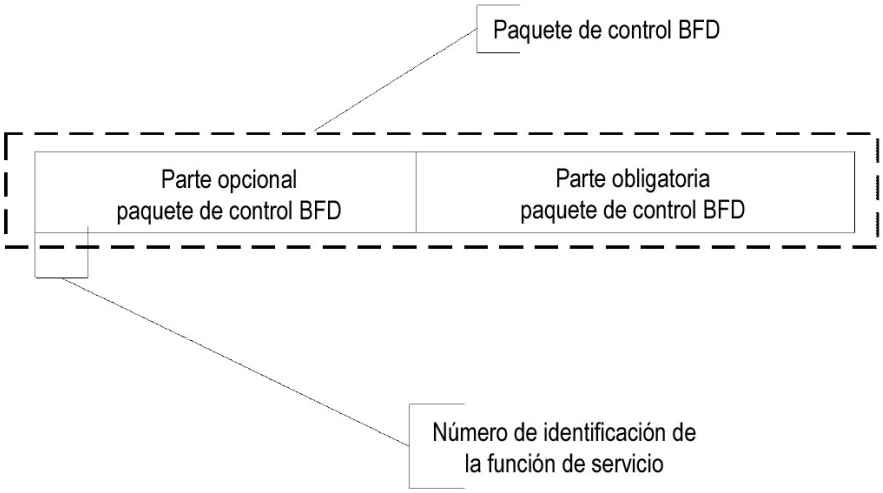
Paquete de control BFD
Parte opcional
paquete de control BFD
Parte obligatoria
paquete de control BFD
Número de identificación de
la función de servicio

Fig. 3

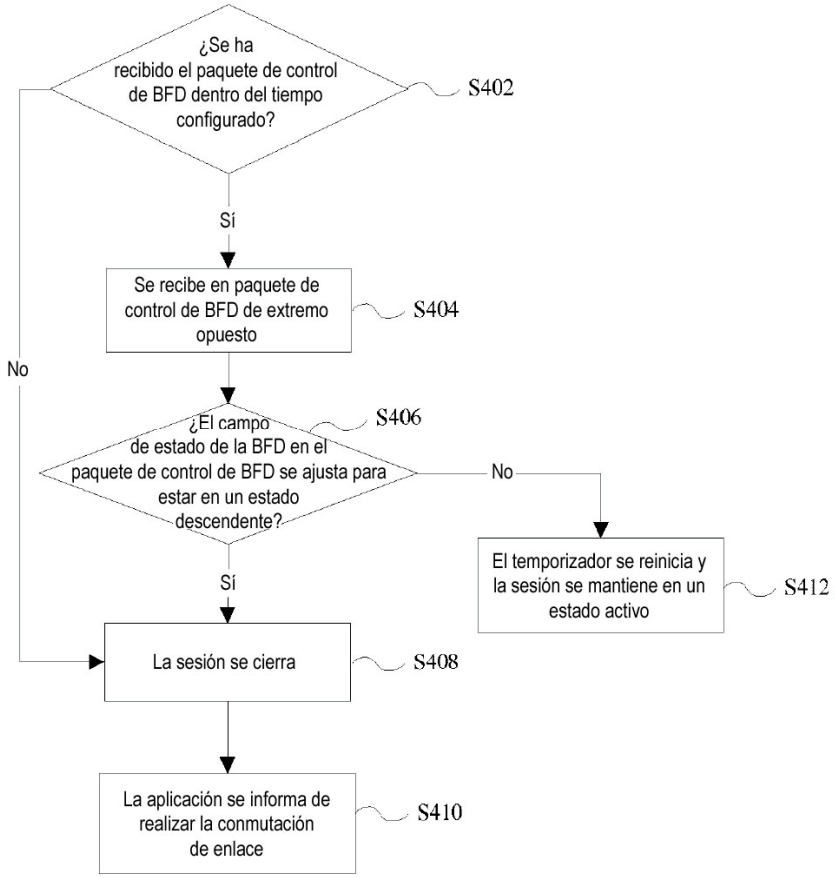
¿Se ha
recibido el paquete de control
de BFD dentro del tiempo
configurado?
S402
Sí
Se recibe en paquete de
control de BFD de extremo
opuesto
S404
No
¿El campo
de estado de la BFD en el
paquete de control de BFD se ajusta para
estar en un estado
descendente?
S406
No
El temporizador se reinicia y
la sesión se mantiene en un
estado activo
S412
Sí
La sesión se cierra
S408
La aplicación se informa de
realizar la conmutación
de enlace
S410

Fig. 4

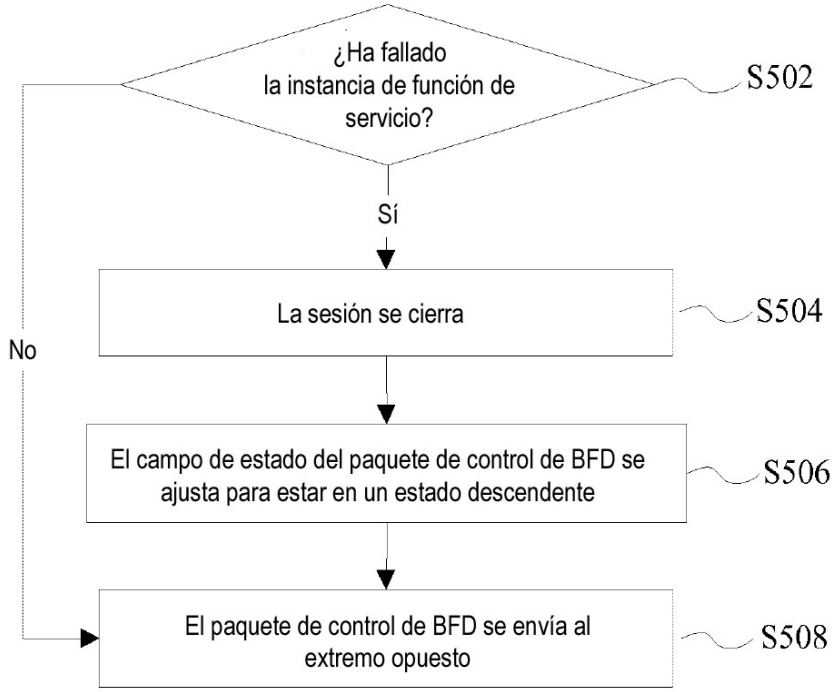
¿Ha fallado la instancia de función de servicio?
S502
Sí
No
La sesión se cierra
S504
El campo de estado del paquete de control de BFD se ajusta para estar en un estado descendente
S506
El paquete de control de BFD se envía al extremo opuesto
S508

Fig. 5

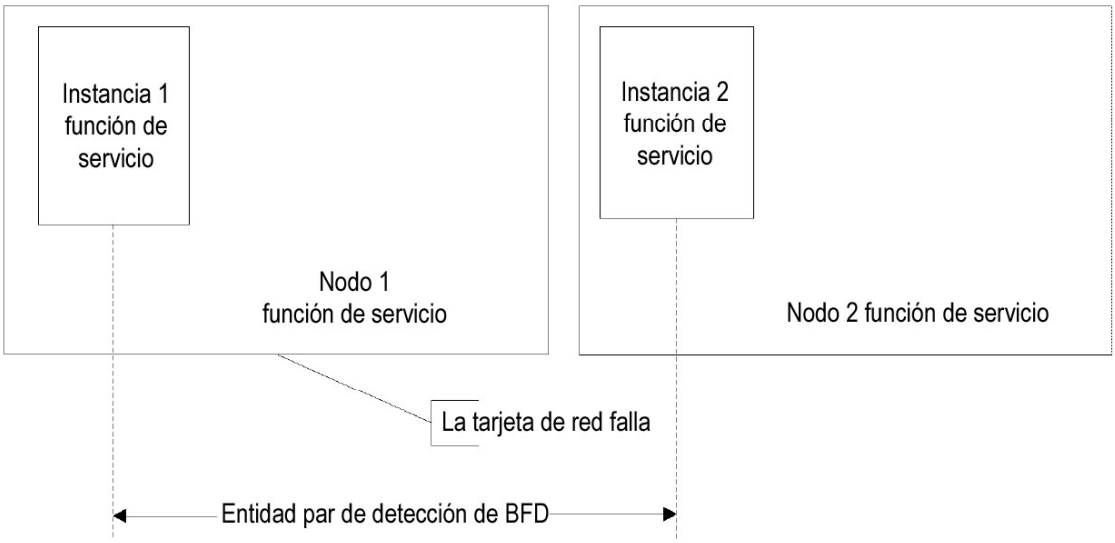
Instancia 1 función de servicio
Nodo 1 función de servicio
Instancia 2 función de servicio
Nodo 2 función de servicio
La tarjeta de red falla
Entidad par de detección de BFD

Fig. 6

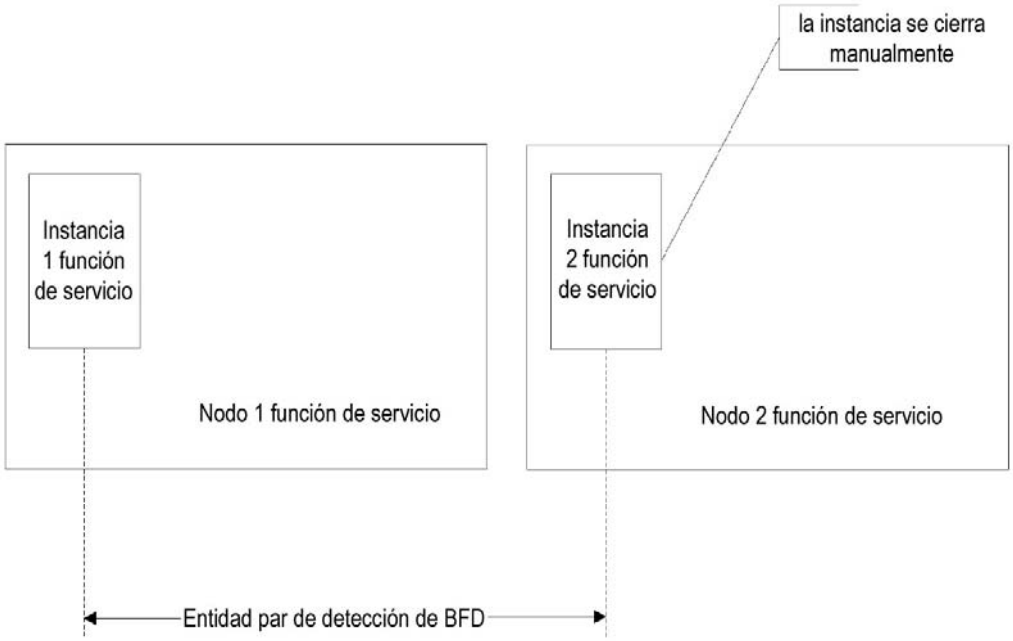
la instancia se cierra manualmente
Instancia 1 función de servicio
Instancia 2 función de servicio
Nodo 1 función de servicio
Nodo 2 función de servicio
Entidad par de detección de BFD

Fig. 7

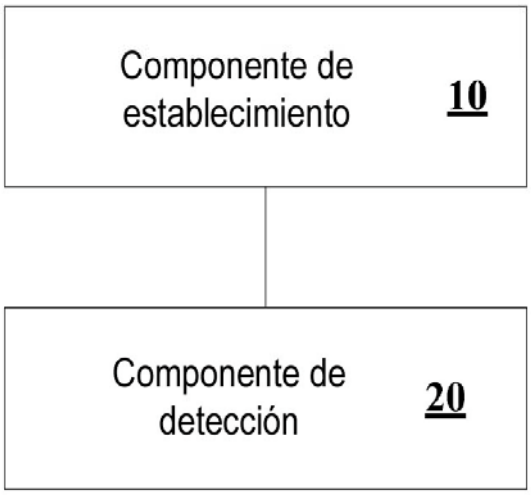
Componente de establecimiento
10
Componente de detección
20

Fig. 8

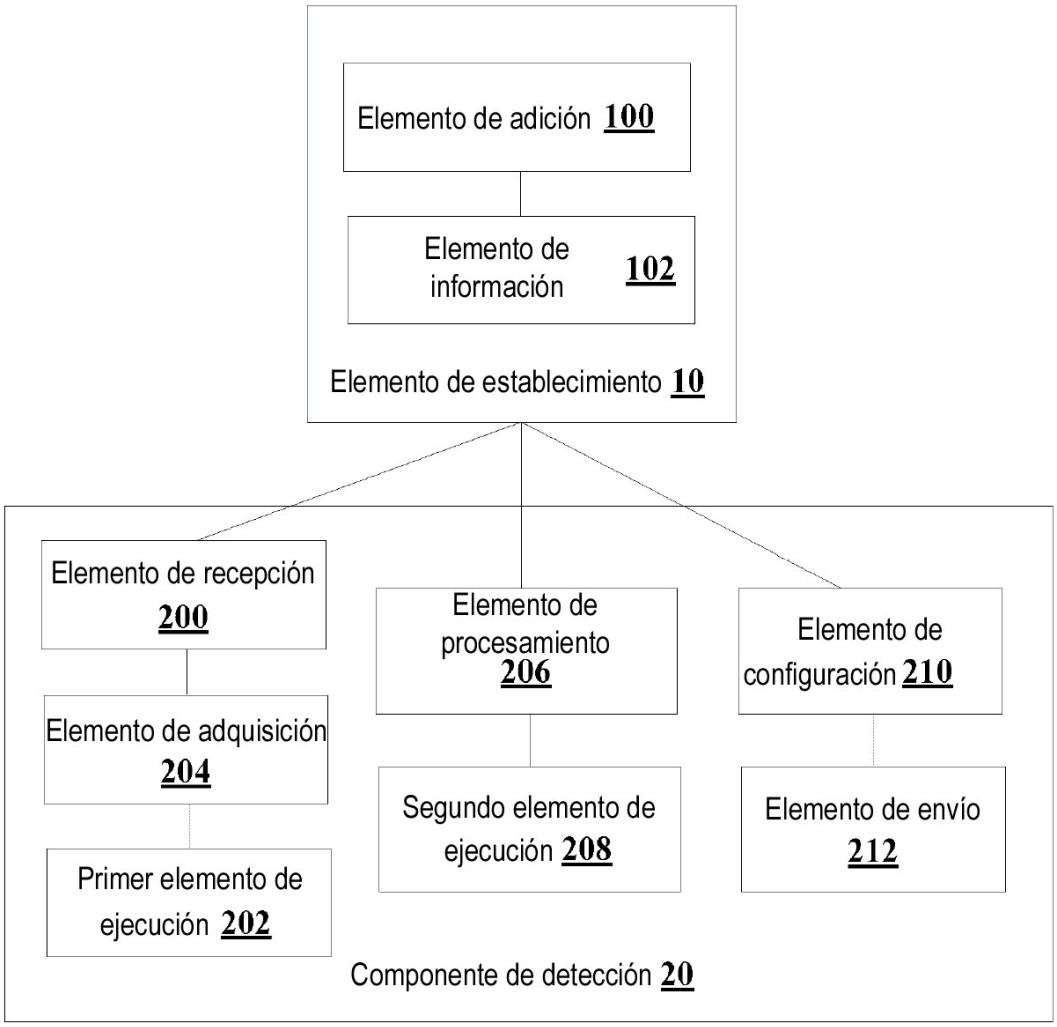
Elemento de adición 100
Elemento de información 102
Elemento de establecimiento 10
Elemento de recepción 200
Elemento de adquisición 204
Primer elemento de ejecución 202
Elemento de procesamiento 206
Segundo elemento de ejecución 208
Elemento de configuración 210
Elemento de envío 212
Componente de detección 20

Fig. 9