(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 365 866**

(51) Int. Cl.:
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06742040 .6**
(96) Fecha de presentación : **30.05.2006**
(97) Número de publicación de la solicitud: **1914939**
(97) Fecha de publicación de la solicitud: **23.04.2008**

(54) Título: **Método para desencadenar la detección de fallos en la detección de reenvío bidireccional.**

(30) Prioridad: **10.08.2005 CN 2005 1 0089888**

(45) Fecha de publicación de la mención BOPI:
11.10.2011

(45) Fecha de la publicación del folleto de la patente:
11.10.2011

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

(72) Inventor/es: **Tan, Xuefei**

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

DESCRIPCIÓN

Método para desencadenar la detección de fallos en la detección de reenvío bidireccional

Campo de la invención

La presente invención está relacionada con tecnologías de detección de enlaces y, en particular, con un método para desencadenar la detección de fallos en una Detección de Reenvío Bidireccional (BFD).

Antecedentes de la invención

Con el desarrollo de las tecnologías de comunicaciones, el problema de cómo garantizar la calidad de la transmisión de datos y de cómo localizar rápidamente un fallo cuando ocurre este fallo en la transmisión de datos, se ha convertido en un problema urgente que ha de resolverse. Por tanto, la BFD, como mecanismo de detección rápida, emerge como requieren los tiempos. En la BFD, se detecta un enlace por medio de un mecanismo rápido de “Hola” con una velocidad que puede ser negociada.

La BFD puede utilizarse para detectar la corrección de diversos tipos de transmisión, incluyendo Ethernet, el Camino de Conmutación de Etiquetas Multi-protocolo (MPLS), la encapsulación de enrutamiento común y el túnel de protocolos de seguridad de la red IP (IPsec).

La BFD se desarrolla a partir de la tecnología básica de transmisión paso a paso, de manera que con la BFD, puede detectarse el fallo en cada capa de una red. El objeto de la BFD es proporcionar un mecanismo de detección de fallos con una baja sobrecarga y un corto periodo de detección sobre un camino entre enrutadores contiguos. Los enrutadores contiguos se refieren a enrutadores conectados a través de uno o más enlaces lógicos, y no está limitado a un salto entre los enrutadores. La BFD puede realizar la detección sobre un interfaz, un enlace de datos e incluso extenderse al propio motor de reenvío.

La figura 1 es un diagrama esquemático que muestra la red formada por un entorno global de aplicaciones de BFD. En la red, el enrutador A, el enrutador B y el enrutador C se implementan todos ellos con la función BFD. El enrutador A y el enrutador C están conectados a través de un enlace AC, el enrutador B y el enrutador C están conectados a través de un enlace BC. La BFD puede ser aplicada a los enlaces AC y BC para detectar el estado del fallo de los enlaces.

La BFD puede ser resumida como un servicio sencillo, y lo básico del servicio suministrado incluye: crear, eliminar y modificar una sesión BFD bajo la premisa de una dirección de destino dada y otros parámetros. En la BFD, se proporciona una señal al operador para indicar el inicio o terminación de una sesión BFD, o para informar al operador del resultado de la negociación de la sesión BFD o el resultado de la modificación, etc., y para proporcionar la información de estado de un enlace detectado a la capa de aplicación, por ejemplo, la información UP indica que el enlace está en estado normal, mientras que la información DOWN indica un fallo del enlace.

La BFD es similar al protocolo “Hola”. Después de establecer una sesión BFD, las dos partes de la sesión BFD envían periódicamente paquetes BFD a la parte opuesta sobre un enlace sobre el cual se aplica la BFD, y detectan periódicamente el estado de llegada de los paquetes desde la parte opuesta en el enlace. Si una parte no recibe un paquete BFD desde el lado opuesto dentro de un intervalo de tiempo, se considera que tiene lugar un fallo en el enlace, para encontrar rápidamente el fallo en el enlace.

En la red ilustrada en la figura 1, se supone que el enrutador A y el enrutador C son mutuamente vecinos en una sesión BFD, y no se establece una sesión BFD sobre el enlace AC inicialmente. El ciclo de vida de una sesión BFD tiene principalmente las etapas siguientes:

1) Establecimiento inicial de una sesión BFD.

En primer lugar, se crea un ejemplo de BFD en el enrutador A y en el enrutador C, respectivamente. Después, el enrutador A y el enrutador C obtienen las direcciones IP de sus vecinos. La BFD no tiene un mecanismo automático de búsqueda de vecinos, de manera que un ejemplo de BFD puede obtener la dirección IP de un vecino a través de una configuración estática o dependiendo de otros protocolos de aplicación.

Tras obtener la dirección IP de un vecino, el ejemplo de BFD obtiene un discriminador asignado por la parte opuesta y asigna un discriminador localmente. El discriminador puede ser configurado manualmente, o ser obtenido a través de una negociación automática en la banda o una negociación fuera de la banda. En otras palabras, la negociación del discriminador se realiza a través de otro protocolo de aplicaciones y después se notifica al ejemplo de BFD. Si se emplea el modo de negociación automática en la banda, la secuencia de tiempos de la sesión BFD se establece entre los enrutadores a través de tres saludos, cuya negociación específica es irrelevante para la invención y se puede hacer referencia a los documentos relacionados con el protocolo BFD.

2) Negociación de parámetros de una sesión BFD.

Después de haber establecido una sesión BFD entre casos de BFD de los vecinos a través de tres saludos, se necesita negociar los parámetros de la sesión BFD para ser conforme con la velocidad de la transmisión-recepción de paquetes BFD, tiempo de determinación del fallo y modo de la sesión (tal como el modo asíncrono o el modo síncrono) de las dos partes.

Antes de comenzar la negociación de parámetros de la sesión BFD, cada enrutador estima su capacidad para enviar y recibir paquetes BFD basados en las condiciones preestablecidas, tales como la influencia sobre la anchura de banda y la ocupación de la CPU. Después negocia el tiempo más corto para detectar un fallo, es decir, el tiempo de determinación del fallo, con un enrutador vecino. El tiempo de determinación del fallo negociado puede ser modificado en tiempo real.

Una vez negociados los diversos parámetros de la sesión BFD y establecida la sesión BFD, se provoca esta sesión BFD como una etapa de detección de fallos.

3) Detección de fallos de BFD.

En la invención, se ilustra la etapa de detección de fallos de BFD en el caso de que el modo de la sesión BFD sea un modo asíncrono. Después de haber establecido la sesión BFD y haber negociado los parámetros relacionados, las partes de la sesión BFD envían periódicamente un paquete de control de BFD al lado opuesto, de acuerdo con el modo asíncrono en un intervalo de tiempo que es negociado. El paquete de control de BFD se adapta para realizar la detección de impulsos. La función y el modo de funcionamiento del paquete de control de BFD son los mismos que el de un paquete HOLA de otros protocolos de enrutamiento, pero la frecuencia de envío es normalmente más alta.

Cuando una parte de la sesión BFD envía el paquete de control de BFD al lado opuesto, detecta periódicamente el paquete BFD enviado por el lado opuesto. Si detecta que se pierden consecutivamente un número prefijado de paquetes BFD desde un vecino, declara que ocurre un fallo en el enlace e informa a otras aplicaciones, tales como módulos de enrutamiento, con un mensaje de fallo de enlace. El número de paquetes BFD perdidos consecutivamente cuando se declara que ocurre un fallo en el enlace, se determina de acuerdo con el resultado de la negociación de la sesión BFD, y este parámetro se define en el formato del paquete de control de BFD a través de un campo de detección múltiple (Detect Mult).

En el borrador de la BFD, no se especifica ningún protocolo para transportar paquetes BFD; en su lugar, solamente propone encapsular un paquete BFD utilizando el Protocolo de Datagramas de Usuario (UDP), y el paquete BFD se identifica empleando un puerto de destino de UDP con el número 3784. El formato de un paquete BFD encapsulado en UDP está ilustrado en la Tabla 1:

<table>
<tr><td colspan="3">0 1 2</td><td colspan="5">3 4 5 6 7</td><td colspan="2">8 9</td><td colspan="5">0 1 2 3 4</td><td colspan="5">5 6 7 8 9</td><td colspan="5">0 1 2 3 4</td><td colspan="5">5 6 7 8 9</td><td colspan="2">0 1</td></tr>
<tr><td colspan="3">Vers</td><td colspan="5">Diag</td><td colspan="2">Sta</td><td>P</td><td>F</td><td>C</td><td>A</td><td>D</td><td>R</td><td colspan="10">Detect Mult</td><td colspan="7">Longitud</td></tr>
<tr><td colspan="32">Discriminador generado por el sistema de envío (Mi discriminador)</td></tr>
<tr><td colspan="32">Discriminador recibido desde el correspondiente sistema remoto (Tu discriminador)</td></tr>
<tr><td colspan="32">Intervalo mínimo de envío de paquetes de control de BFD deseado por el sistema local (Intervalo Min TX deseado)</td></tr>
<tr><td colspan="32">Intervalo mínimo de recepción de BFD admitido por el sistema (Intervalo Min RX requerido)</td></tr>
<tr><td colspan="32">Intervalo mínimo del paquete de eco recibido de BFD, admitido por el sistema (Intervalo Min Eco RX requerido)</td></tr>
<tr><td colspan="32">Los datos de autentificación siguientes son opcionales</td></tr>
<tr><td colspan="8">Tipo de autentificación (AuthType)</td><td colspan="12">Longitud de la autentificación (AuthLen)</td><td colspan="12">Datos de autentificación (AuthenticationData)</td></tr>
</table>

Tabla 1

El significado de cada campo del paquete BFD de la Tabla 1 está ilustrado en la Tabla 2:

Nombre del dominio	Significado
Versión (vers)	Número de la versión del protocolo BFD, el número de la versión actual es 1
Diagnóstico (Diag)	El código del diagnóstico describe las causas por las que el sistema local vuelve a otros estado desde el último estado UP. El significado es como sigue:

	0 representa No hay diagnóstico 1 representa Tiempo de detección de Control expirado 2 representa Fallo en la función de Eco 3 representa Sesión señalizada por el vecino caída 4 representa Reposición del plano de reenvío 5 representa Pathdown (camino caído) 6 representa Camino concatenado caído 7 representa Caída administrativa 8 - 31 representan Reservados para uso futuro
Estado (Sta)	"Estado" representa el estado actual de la sesión BFD, visto por el sistema de transmisión. Los valores son: 0 representa Sesión fijada por administrador DOWN (caída) (AdminDown) 1 representa estado de la sesión BFD es DOWN (caída) 2 representa un estado inicial (Init) 3 representa Estado de la sesión BFD funcionando (UP)
Consulta (P)	Si está fijado en 1, indica que necesita verificarse la conectividad o se requiere variación de parámetros; si es 0, no se necesita verificación
Final (F)	1: Para un paquete BFD recibido, si Poll (consulta) está activada, responder a la consulta; 0: No responder a la consulta.
Independiente del plano de control (C)	1: BFD solamente se ejecuta en el plano de datos, y no está influenciada incluso cuando se colapsa el plano de control; 0: La aplicación BFD comparte el estado del plano de control (en otras palabras, se colapsa cuando lo hace el plano de control).
Autentificación presente (A)	1: La sesión necesita ser autentificada.
Demanda (D)	Cuando está fijada como 1, indica que el sistema espera funcionar en modo de demanda; en otro caso, el sistema no espera o no puede funcionar en el modo anterior
Reservado (R)	Deben ser todos cero, y la parte receptora ignora estos bits.
Detect Mult	Multiplicador de tiempo de detección: cuando se negocia el intervalo de transmisión, necesita ser multiplicado por este valor. Este valor se utiliza en modo asíncrono. En el modo asíncrono, Detect_Mult requiere el periodo de detección de la parte opuesta; en el modo de Demanda, el Detect_Mult notifica a la parte opuesta su propio periodo de detección.
Longitud	Longitud de un paquete de control de BFD en unidades de byte.
Mi discriminador	Es un discriminador exclusivo distinto de cero entre dos sistemas generados por el sistema de envío, y utilizado para la desmultiplexación (identificación) de múltiples conexiones de BFD.
Tu discriminador	(Valor de) discriminador recibido desde el sistema remoto correspondiente, y este campo es devuelto desde el Mi discriminador recibido. Se rellenan como todos ceros si la situación del lado opuesto es desconocida.
Intervalo de TX mínimo	Intervalo mínimo deseado de envío del paquete de control de BFD por el sistema local,

deseado	en unidades de microsegundos.
Intervalo mínimo requerido de RX	Intervalo mínimo de envío de BFD admitido por el sistema, en unidades de microsegundos.
Intervalo mínimo requerido de RX de eco	Intervalo mínimo de paquetes de eco de BFD admitido por el sistema, en unidades de microsegundos. Si está fijado en 0, el sistema de transmisión no admite el paquete de eco de BFD.
Auth Type	Si está fijada como A, el campo representa el tipo de autentificación. El significado es como sigue: 0 representa Reservado (Reserved) 1 representa Autentificación de Contraseña Simple (Simple password) 2 representa Autentificación MD5 con clave (Keyed MD5) 3 representa Autentificación meticulosa de MD5 con clave (Meticulous Keyed MD5) 4 - 255 representa Reservado para uso futuro
Auth Len	Longitud de la parte de autentificación en unidades de bytes, incluyendo el Auth Type y el Auth Len

Tabla 2

En el modo asíncrono, debido a que la BFD necesita enviar y detectar un paquete BFD rápidamente, el envío y detección del paquete BFD se realizan ambos a través de un hardware lógicamente sencillo, que se configura usualmente sobre un plano de reenvío. El establecimiento y proceso de negociación de una sesión compleja de BFD debe ser conseguido por software o hardware universal con lógica más compleja, etc.

En esta divulgación, el módulo de establecimiento y negociación de una sesión BFD se abrevia como módulo de negociación, y el módulo de envío y detección de un paquete BFD se abrevia como módulo de detección.

En la técnica anterior, hay un método para realizar la detección de fallos en una sesión BFD como sigue:

Después de que se ha establecido una sesión BFD y se han negociado diversos parámetros de la sesión BFD, los diversos parámetros de la sesión BFD negociados, tal como el intervalo de envío y el intervalo de detección, son notificados a un módulo de detección. Al recibir la información de los parámetros, el módulo de detección inicia un temporizador de envío inmediatamente, y envía periódicamente paquetes BFD al lado opuesto y, al mismo tiempo, se inicia inmediatamente un temporizador para la detección y se detecta el estado de llegada del paquete BFD desde la parte opuesta. De acuerdo con la información de parámetros negociada, si se detecta que se pierden consecutivamente un número predeterminado de paquetes BFD desde la parte opuesta, se declara que ocurre un fallo en el enlace. La figura 2 es un diagrama esquemático que muestra una secuencia de tiempos de detección de fallos de una sesión BFD en la técnica anterior. Como se ilustra en la figura 2, siempre que, de acuerdo con el resultado negociado de la etapa de negociación de parámetros, el enrutador A envía un paquete BFD en un intervalo de tiempo de 10 ms, como se ilustra con la línea bidireccional de puntos y rayas de la figura 2, y el enrutador B envía un paquete BFD en un intervalo de tiempo de 15 ms, como se ilustra por la línea bidireccional de rayas de la figura 2. Si el enrutador A detecta que se pierden consecutivamente 3 paquetes BFD enviados desde el enrutador B, es decir, cuando la cuenta de pérdidas es 3, el enrutador A declara que ocurre un fallo en el enlace y envía información de estado del enlace detectada como información DOWN a la capa de aplicaciones.

El método anterior para detectar la transmisión de un paquete BFD tiene las desventajas siguientes: en aplicaciones prácticas, el módulo de negociación necesita emplear un periodo de tiempo para notificar al módulo de detección el resultado de la negociación de parámetros, la longitud del periodo de tiempo está normalmente influenciada por muchos factores. Uno de los factores es el estado de ocupación del módulo de negociación. Debido a que el módulo de negociación soporta tareas normalmente de muchas otras sesiones BFD, tal como el establecimiento, la negociación y el enrutamiento, el módulo de negociación está normalmente muy ocupado. Otro factor es el estado de congestión del canal entre el módulo de negociación y el módulo de detección. Por tanto, el retardo que necesita el módulo de negociación para entregar el parámetro BFD al módulo de detección es impredecible. Algunas veces, puede ser muy largo y algunas veces puede ser muy corto. Especialmente, cuando existe una diferencia de rendimiento o una diferencia de carga entre los vecinos de una sesión BFD, la diferencia del retardo es más aparente. Cuando el retardo alcanza un valor, es inevitable que un lado de la sesión BFD informe en falso que tiene lugar un fallo en el enlace.

La figura 3 es un diagrama esquemático que muestra que un lado de una sesión BFD informa en falso que ocurre un

fallo en el enlace. Como se ilustra en la figura 3, en el proceso de detección, el enrutador A envía un paquete BFD en el intervalo de tiempo de 10 ms, como se ilustra por la línea bidireccional de puntos y rayas de la figura 3, de acuerdo con el resultado de la negociación de la sesión BFD de la etapa de negociación, y el enrutador B envía un paquete BFD en un intervalo de tiempo de 15 ms, como se ilustra con la línea bidireccional de rayas de la figura 3. Sin embargo, debido a diversas causas, el enrutador B no puede entregar el parámetro de la sesión BFD al módulo de detección durante un tiempo largo. Después de que el enrutador A detecta que se pierden consecutivamente 3 paquetes BFD enviados desde el enrutador B, en otras palabras, cuando la cuenta de pérdidas es 3, el enrutador A declara que ocurre un fallo en el enlace y envía la información de estado del enlace detectada como información DOWN a la capa de aplicación. En la figura 3, el tiempo en el que termina la etapa de negociación de las dos partes es T0, el consumo de tiempo para entregar el parámetro de la sesión BFD al módulo de detección por el módulo de negociación del enrutador A es Ta, como se ilustra con la línea gruesa bidireccional de rayas, y el consumo de tiempo para entregar el parámetro de la sesión BFD al módulo de detección por el módulo de negociación del enrutador B es Tb, como se ilustra con la doble línea bidireccional de puntos y rayas.

Puede observarse por la figura 3, que si Tb es mayor que la suma de Ta y del tiempo de detección de 45 ms del enrutador A, el enrutador informa en falso de que ocurre un fallo en el enlace. En este caso, debido a que se detecta que se pierden 3 paquetes consecutivamente y que el tiempo de envío de cada paquete BFD es 15 ms, el tiempo de detección es 45 ms.

En vista del método actual para la detección de fallos sobre el reenvío bidireccional, después de haber negociado diversos parámetros de la sesión BFD y haber establecido la sesión BFD, las dos partes de la sesión BFD son activadas a una etapa de detección de fallos. Debido a que existe una diferencia entre los retardos que necesitan los módulos de negociación en enrutadores de las dos partes de la sesión BFD, para entregar parámetros de la sesión BFD al módulo de detección, el enrutador puede informar en falso que ocurre un fallo en el enlace durante la detección de fallos.

El documento “Detección de Reenvío Bidireccional; draft-ietf-bfd-base-02.txt” (1 de Marzo 2005, BORRADOR ESTÁNDAR DE TRABAJO DEL IEFT, GRUPO DE TRABAJO DE INGENIERÍA DE INTERNET, IETF, CH) divulga un protocolo destinado a detectar fallos en el camino bidireccional entre dos motores de reenvío.

El documento “BFD para MPLS LSPs; draft-raggarwa-mpls-bfd-00.txt” (1 de Octubre 2003, BORRADOR ESTÁNDAR DE TRABAJO DEL IEFT, GRUPO DE TRABAJO DE INGENIERÍA DE INTERNET, IETF, CH) divulga la aplicabilidad de la BFD con respecto a LSP-Ping y procedimientos para usar la BFD en este entorno.

La patente de Estados Unidos núm. 6.314.512 B1 divulga la detección de un fallo en una aplicación multi-sistema.

El documento “BFD para IPv4 e IPv6 (Un solo salto); draft-ietf-bfd-v4v6-1hop-02.txt” (1 de Marzo de 2005, BORRADOR ESTÁNDAR DE TRABAJO DEL IEFT, GRUPO DE TRABAJO DE INGENIERÍA DE INTERNET, IETF, CH) divulga el uso del protocolo de Detección de Reenvío Bidireccional sobre IPv4 e IPv6 para saltos únicos de IP.

Sumario de la invención

Por tanto, es un objeto de la presente invención proporcionar un método para desencadenar la detección de fallos en la BFD, resolviendo con ello el problema de que un sistema para la detección de una sesión BFD informe en falso del fallo del enlace.

Para conseguir el objeto anterior, la invención proporciona las siguientes soluciones técnicas.

Un método para iniciar la función de detección de la sesión BFD, en el cual se establece una sesión BFD entre dos lados de un enlace de reenvío bidireccional, que incluye además:

enviar, por uno de los lados de la sesión BFD, un paquete BFD al lado opuesto, y recibir un paquete BFD desde el lado opuesto; e iniciar, por un lado de la sesión BFD, la función de detección de la sesión BFD al recibir un primer paquete BFD desde el lado opuesto.

Durante el establecimiento de la sesión BFD, los dos lados de la sesión BFD negocian para determinar los parámetros de la sesión BFD, incluyendo la longitud de tiempo de un temporizador de detección de la sesión BFD, y fijar el valor inicial de una etiqueta prefijada que indique si se ha recibido un primer paquete desde el lado opuesto, para indicar que no se ha recibido un primer paquete enviado por el lado opuesto de la sesión BFD.

Si un lado de la sesión BFD recibe un primer paquete BFD desde el lado opuesto, el método incluye además: fijar el valor de la etiqueta que indique si se ha recibido un primer paquete desde el lado opuesto, para indicar que se ha recibido el primer paquete BFD enviado por el lado opuesto de la sesión BFD.

El método incluye específicamente:

A) enviar, por uno de los lados de la sesión BFD, un paquete BFD al lado opuesto periódicamente, de acuerdo con

la longitud de tiempo del temporizador de envío de paquetes de BFD en el parámetro de la sesión BFD;

B) determinar, por un lado de la sesión BFD; si el valor de la etiqueta que indica si se ha recibido un primer paquete desde el lado opuesto, indica que no se ha recibido un primer paquete BFD enviado por el lado opuesto de la sesión BFD, y si es afirmativo, volver al proceso A; en otro caso, se ejecuta el proceso C; y

C) desencadenar la detección de fallos de acuerdo con el inicio del temporizador de detección de la sesión BFD prefijado por la longitud de tiempo del temporizador de la sesión BFD, y enviar, por un lado de la sesión BFD, un paquete BFD al lado opuesto periódicamente, de acuerdo con la longitud de tiempo del temporizador de envío de paquetes BFD.

Después del proceso A y antes del proceso B, el método incluye además: fijar la longitud de tiempo de expiración, y fijar la longitud de tiempo del temporizador de detección de la sesión BFD, como longitud de tiempo de expiración, e iniciar el temporizador de detección de la sesión de BFD.

Cuando en el proceso B se determina que el valor de la etiqueta que indica si se ha recibido un primer paquete desde el lado opuesto es FALSO, se determina además si expira el temporizador de detección de la sesión BFD, y si es afirmativo, un lado de la sesión BFD informa de que ocurre un fallo en un motor de reenvío del lado opuesto, y el procedimiento termina; si es negativo, el procedimiento vuelve al proceso A.

Después del proceso A y antes del proceso B, el método incluye además: fijar la longitud del tiempo de expiración y un temporizador de expiración, y fijar la longitud de tiempo del temporizador de expiración como longitud de tiempo de expiración, e iniciar el temporizador de expiración;

Cuando se determina en el proceso B que el valor de la etiqueta que indica si se ha recibido un primer paquete desde el lado opuesto es FALSO, se determina además si expira el temporizador de expiración; si es afirmativo, un lado de la sesión BFD informa de que ocurre un fallo en un motor de reenvío del lado puesto, y el proceso termina; si es negativo, el procedimiento vuelve al proceso A.

El modo de la sesión de los dos lados de una sesión BFD es asíncrono.

Los dos lados de la sesión BFD son sistemas para implementar las funciones BFD.

Puede observarse a partir de las soluciones anteriores que, en la presente invención, la detección de fallos se inicia solamente después de que un lado de la sesión BFD reciba un primer paquete BFD enviado desde el lado opuesto. Se puede evitar que un enrutador informe en falso de un fallo en el enlace debido a la diferencia entre retardos que necesitan los módulos de negociación en enrutadores de las dos partes de una sesión BFD, para entregar los parámetros de la sesión BFD a los módulos de detección. La invención incluye además la detección de si ocurre un fallo en un motor de reenvío de un lado de una sesión BFD, para evitar que un lado de la sesión BFD inicie un ataque malicioso para hacer que el lado atacado informe en falso de un fallo del enlace.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático que ilustra la red formada en un entorno global de aplicaciones de BFD;

La figura 2 es un diagrama esquemático que ilustra la secuencia de detección de fallos de una sesión BFD de la técnica anterior;

La figura 3 es un diagrama esquemático que ilustra que un lado de la sesión BFD informa en falso que ocurre un fallo en un enlace;

La figura 4 es un diagrama de flujo del método para desencadenar la detección de fallos, de acuerdo con la invención; y

La figura 5 es un diagrama esquemático de un modo de realización de la invención.

Descripción detallada de los modos de realización

El concepto básico de la invención reside en que, después de que dos partes de un enlace de reenvío bidireccional establece una sesión BFD, un lado de la sesión BFD envía un paquete BFD al lado opuesto y recibe un paquete BFD desde el lado opuesto; y cuando un lado de la sesión BFD recibe un primer paquete BFD desde el lado opuesto, desencadena la detección de fallos.

Para hacer más evidentes los objetos, las soluciones técnicas y las ventajas de la invención, se ilustra ahora con más detalle la invención conjuntamente con los dibujos y los modos de realización preferidos.

La figura 4 es un diagrama de flujo del método para desencadenar la detección de fallos de acuerdo con la invención. Tomando como ejemplo que el sistema para implementar la detección de la sesión BFD es un enrutador,

como se ilustra en la figura 4, el método incluye los procesos siguientes:

Proceso 401: Las dos partes de un enlace de reenvío bidireccional establecen una sesión BFD y negocian los parámetros de la sesión BFD.

Después de que los módulos de negociación de los enrutadores de los dos lados de la sesión BFD negocian los parámetros de la sesión BFD, los módulos de negociación de los enrutadores de los dos lados entregan respectivamente los parámetros de la sesión BFD a los módulos de detección de los enrutadores de los dos lados, de manera que se establece una sesión BFD. Los parámetros de la sesión BFD entregados incluyen el periodo de detección de la sesión BFD y el periodo de envío de paquetes BFD, etc.

Al recibir los parámetros de la sesión BFD entregados por un módulo de negociación, un módulo de detección realiza diversas operaciones de inicialización inmediatamente, que incluyen: fijar de la longitud de tiempo de un temporizador de envío de paquetes BFD, construir un paquete BFD, y fijar la longitud del tiempo de un temporizador de detección de una sesión BFD. Además, la invención incluye también: fijar el valor inicial de una etiqueta (bHasReceivedFirstPacket) que indica si se ha recibido como FALSO un primer paquete desde el lado opuesto, lo cual indica que no se ha recibido un primer paquete BFD enviado por el lado opuesto de la sesión BFD.

Proceso 402: Un lado de la sesión BFD envía periódicamente un paquete BFD al lado opuesto y recibe un paquete BFD desde el lado opuesto.

Después de realizar diversas operaciones de inicialización, el módulo de detección de la sesión BFD envía periódicamente un paquete BFD al lado opuesto de la sesión BFD inmediatamente, de acuerdo con la longitud de tiempo prefijado del temporizador de envío de paquetes BFD. Pero, en ese momento, no se inicia la función de detección de la sesión BFD.

Proceso 403: Determinar si el valor de la etiqueta “bHasReceivedFirstPacket” del parámetro de la sesión BFD es FALSO, y si es afirmativo, volver al proceso 402; en otro caso, ejecutar el proceso 404.

Si el módulo de detección de la sesión BFD recibe un primer paquete BFD enviado desde el lado opuesto de la sesión BFD, fija el valor de la etiqueta “bHasReceivedFirstPacket” como VERDADERO inmediatamente, lo cual indica que se ha recibido un primer paquete BFD enviado por el lado opuesto de la sesión BFD, y el módulo de detección de la sesión BFD desencadena la función de detección de la sesión BFD y continúa enviando periódicamente paquetes BFD al lado opuesto.

Proceso 404: Se desencadena la función de detección de fallos y los paquetes BFD son enviados periódicamente a la parte opuesta.

Cuando el valor de la etiqueta “bHasReceivedFirstPacket” es VERDADERO, el módulo de detección de la sesión BFD desencadena la función de detección de fallos, es decir, inicia un temporizador de detección de la sesión BFD de acuerdo con la longitud de tiempo del temporizador de detección de la sesión BFD que está fijada, y detecta periódicamente si se recibe un paquete BFD enviado por el lado opuesto. Si el número de paquetes BFD enviados por el lado opuesto que se pierden consecutivamente alcanza un valor predeterminado, envía la información de estado del enlace detectado como información DOWN a la capa de aplicación, informando con ello de que ocurre un fallo en el enlace de la sesión BFD. Debe indicarse que el método de la invención enfatiza que el momento para desencadenar la detección de fallos, es cuando se recibe el primer paquete BFD desde el lado opuesto, al tiempo que el método para la detección de fallos es consistente con el método existente.

La figura 5 es un diagrama esquemático de un modo de realización de la invención. Como se ilustra en la figura 5, se supone que el enrutador A y el enrutador B completan la negociación de los parámetros de la sesión BFD simultáneamente en T0. El consumo de tiempo que necesita el módulo de negociación del enrutador A para entregar los parámetros de la sesión BFD al módulo de detección es Ta, como se ilustra con la línea gruesa bidireccional de rayas. Después de la operación de inicialización, el módulo de detección fija el valor de la etiqueta “bHasReceivedFirstPacket” como FALSO. El enrutador A comienza a enviar un paquete BFD al enrutador B en el instante TA. Debido a que el valor de la etiqueta “bHasReceivedFirstPacket” es FALSO en ese momento, incluso si el enrutador A no recibe un paquete BFD enviado desde el enrutador B, no lleva la cuenta del contador de pérdidas debido a que no recibe un paquete BFD desde el enrutador B. Incluso cuando expira el tiempo de detección, no informa de que ocurre un fallo en el enlace; en lugar de eso, sigue enviando paquetes BFD al enrutador B periódicamente.

El consumo de tiempo del módulo de negociación del enrutador B para entregar los parámetros de la sesión BFD al módulo de detección es Tb, como se ilustra con la doble línea bidireccional de puntos y rayas. En el instante Tb, el enrutador A recibe el primer paquete BFD enviado por el enrutador B y fija la etiqueta “bHasReceivedFirstPacket” como VERDADERA, indicando que se inicie la función de detección de fallos, y fija la longitud de tiempo del temporizador de detección de la sesión BFD como el valor determinado durante la negociación BFD, por ejemplo, 45 ms (el tiempo durante el cual se pierden consecutivamente tres paquetes). Después, durante el proceso de detección subsiguiente, si el enrutador A no recibe un paquete BFD desde el enrutador B después de que haya

expirado el temporizador de detección de la sesión BFD, el contador de pérdidas se aumenta en 1; cuando el contador alcanza un valor predeterminado durante la negociación BFD, el enrutador A informa de que ocurre un fallo en el enlace BFD.

Puede observarse a partir de este modo de realización que, incluso si la diferencia entre retardos que necesitan los vecinos de una sesión BFD para entregar los parámetros de la sesión BFD es muy grande, no origina que un lado de la sesión BFD informe en falso de que ocurre un fallo en el enlace.

Más aún, cuando el módulo de detección de la sesión BFD inicializa el temporizador de la detección de la sesión BFD, primero fija la longitud de tiempo del temporizador de detección de la sesión BFD con un valor que es suficientemente grande, en lugar del valor determinado durante la negociación, o fija la longitud del tiempo de otro temporizador de expiración en un valor que es suficientemente grande. Este valor puede asegurar que el módulo de negociación puede entregar los parámetros de la sesión BFD al módulo de detección en este intervalo de tiempo en el caso peor; o este valor es el valor máximo dentro de una gama tolerable. En otras palabras, si el módulo de negociación del lado opuesto no entrega parámetros de la sesión BFD al módulo de detección en este intervalo de tiempo, se considera que ocurre un fallo en el motor de reenvío del lado opuesto.

En este punto, el método para desencadenar la función de detección de fallos es como sigue: después de haber establecido una sesión BFD, se inicia el temporizador antes mencionado de detección de la sesión BFD o el temporizador de expiración cuya longitud de tiempo se fija como un valor suficientemente grande; si no se recibe un primer paquete enviado desde el lado opuesto, cuando expira la longitud del tiempo del temporizador de detección de la sesión BFD/temporizador de expiración, se informa de que ocurre un fallo en el motor de reenvío del lado opuesto; si el primer paquete BFD enviado desde el lado opuesto se recibe antes de que expire la longitud de tiempo de temporizador de detección de la sesión BFD/temporizador de expiración, la longitud de tiempo del temporizador de detección de la sesión BFD se fija como el valor determinado durante la negociación BFD, o se detiene el temporizador de expiración y se inicia el temporizador de detección de la sesión BFD, de acuerdo con la longitud de tiempo del temporizador de detección de la sesión BFD determinada durante la negociación BFD, y la sesión BFD continúa, de manera que se desencadena la detección de fallos.

Así, si ocurre un fallo en un lado de una sesión BFD o en el enlace de la sesión BFD inmediatamente después de haber establecido la sesión BFD, el módulo de detección del otro lado de la sesión BFD no espera permanentemente al primer paquete BFD enviado desde el lado opuesto.

Además, se impiden los ataques iniciados por un lado opuesto malicioso. Por ejemplo, cuando el lado opuesto malicioso no envía un paquete BFD al lado atacado y deshace la sesión BFD local sin notificar al lado atacado después de haber completado la negociación de la sesión BFD, el lado atacado no está en estado de espera permanente.

Los anteriormente ilustrados son solamente modos de realización preferidos de la invención, y no son para uso limitativo de la invención. Consecuentemente, se pueden hacer diversas modificaciones y variaciones sin apartarse del alcance de la invención, como se define en las reivindicaciones anexas y sus equivalentes.

REIVINDICACIONES

1. Un método para iniciar una función de detección de una sesión de Detección de Reenvío Bidireccional, en el que la sesión de Detección de Reenvío Bidireccional se establece (401) entre dos lados de un enlace de reenvío bidireccional, y el método está caracterizado porque comprende:

durante el establecimiento de la sesión de Detección de Reenvío Bidireccional, negociar por los dos lados de la sesión de Detección de Reenvío Bidireccional para determinar los parámetros de la sesión de Detección de Reenvío Bidireccional, incluyendo una longitud de tiempo de un temporizador de detección de la sesión de Detección de Reenvío Bidireccional, y fijar el valor inicial de una etiqueta predeterminada que indica si se ha recibido un primer paquete desde el lado opuesto, para indicar que no se ha recibido el primer paquete de Detección de Reenvío Bidireccional enviado por el lado opuesto de la sesión de Detección de Reenvío Bidireccional; cuando se recibe el primer paquete de Detección de Reenvío Bidireccional desde el lado opuesto por un lado de la sesión de Detección de Reenvío Bidireccional, fijar el valor de la etiqueta que indica si se ha recibido un primer paquete desde el lado opuesto, para indicar que se ha recibido el primer paquete de Detección de Reenvío Bidireccional enviado por el lado opuesto de la sesión de Detección de Reenvío Bidireccional;

enviar (402), por un lado de la sesión de Detección de Reenvío Bidireccional, un paquete de Detección de Reenvío Bidireccional al lado opuesto, y recibir (402) un paquete de Detección de Reenvío Bidireccional desde el lado opuesto; incluyendo: A) el envío, por un lado de la sesión de Detección de Reenvío Bidireccional, un paquete de Detección de Reenvío Bidireccional al lado opuesto periódicamente, de acuerdo con la longitud de tiempo del temporizador de envío de paquetes de Detección de Reenvío Bidireccional, en el parámetro de la sesión de Detección de Reenvío Bidireccional; B) determinar, por dicho lado de la sesión de Detección de Reenvío Bidireccional, si el valor de la etiqueta que indica si se ha recibido un primer paquete desde el lado opuesto, indica que no se ha recibido un primer paquete de Detección de Reenvío Bidireccional enviado por el lado opuesto de la sesión de Detección de Reenvío Bidireccional, y si es afirmativo, el procedimiento vuelve al proceso A; en otro caso, se ejecuta el proceso C; y

iniciar (404) , por un lado de la sesión de Detección de Reenvío Bidireccional, la función de detección de la sesión de Detección de Reenvío Bidireccional al recibir (403) un primer paquete de Detección de Reenvío Bidireccional desde el lado opuesto; incluyendo C) el desencadenamiento de la detección de fallos, de acuerdo con el inicio del temporizador de detección de la sesión de Detección de Reenvío Bidireccional prefijado por la longitud de tiempo del temporizador de detección de la sesión de Detección de Reenvío Bidireccional, y enviar, por un lado de la sesión de Detección de Reenvío Bidireccional, un paquete de Detección de Reenvío Bidireccional al lado opuesto periódicamente, de acuerdo con la longitud de tiempo del temporizador de envío de paquetes de Detección de Reenvío Bidireccional.

2. El método según la reivindicación 1, en el que, después del proceso A y antes del proceso B, el método comprende además: fijar la longitud de tiempo de expiración, y fijar la longitud de tiempo del temporizador de detección de la sesión de Detección de Reenvío Bidireccional, como longitud de tiempo de expiración, e iniciar el temporizador de detección de la sesión de Detección de Reenvío Bidireccional; y

cuando se determina en el proceso B que el valor de la etiqueta que indica si se ha recibido un primer paquete desde el lado opuesto es FALSO, se determina también si expira el temporizador de detección de la sesión de Detección de Reenvío Bidireccional, y si expira el temporizador de detección de la sesión de Detección de Reenvío Bidireccional, un lado de la sesión de Detección de Reenvío Bidireccional informa que ocurre un fallo en el motor de reenvío del lado opuesto, y el proceso termina; si no es así, el procedimiento continúa en el proceso A.

3. El método según la reivindicación 1, en el que después del proceso A y antes del proceso B, el método comprende además: fijar la longitud del tiempo de expiración y un temporizador de expiración, y fijar la longitud del tiempo de temporizador de expiración como longitud de tiempo de expiración e iniciar el temporizador de expiración; y

cuando se determina en el proceso B que el valor de la etiqueta que indica si se ha recibido un primer paquete desde el lado opuesto es FALSO, se determina también si expira el temporizador de expiración, y si el temporizador de expiración expira, un lado de la sesión de Detección de Reenvío Bidireccional informa que ocurre un fallo en el motor de reenvío del lado opuesto, y el proceso termina; si no es así, el procedimiento vuelve al proceso A.

4. El método según cualquiera de las reivindicaciones 1 a 3, en el que el modo de la sesión de los dos lados de la sesión de Detección de Reenvío Bidireccional es un modo asíncrono.

5. El método según la reivindicación 4, en el que los dos lados de la sesión de Detección de Reenvío Bidireccional son sistemas para implementar la función de Detección de Reenvío Bidireccional.

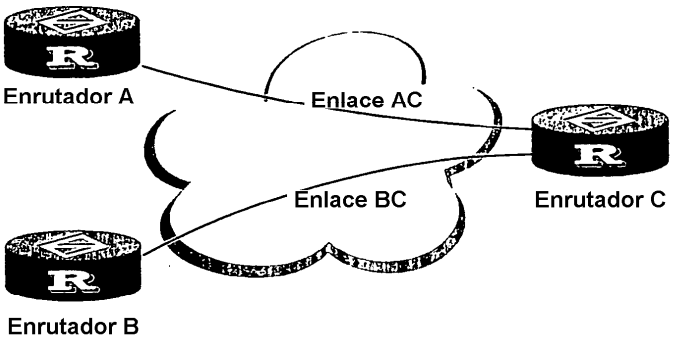
Enrutador A
Enlace AC
Enrutador C
Enlace BC
Enrutador B

Fig.1

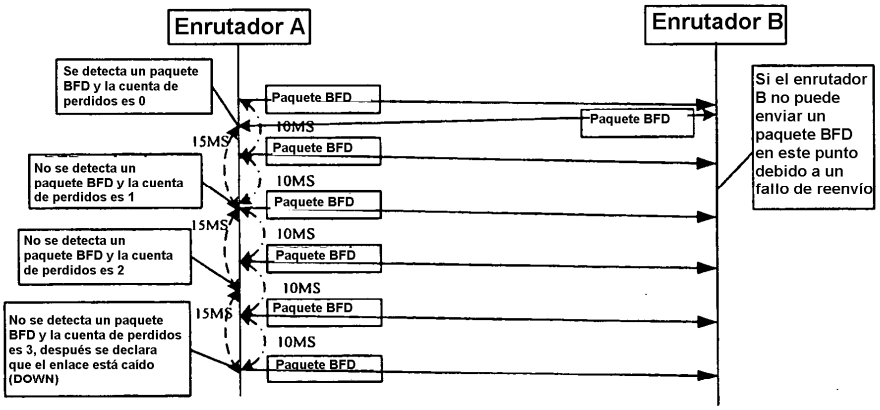
Enrutador A
Enrutador B
Se detecta un paquete BFD y la cuenta de perdidos es 0
Paquete BFD
10MS
15MS
Paquete BFD
Paquete BFD
No se detecta un paquete BFD y la cuenta de perdidos es 1
10MS
15MS
Paquete BFD
No se detecta un paquete BFD y la cuenta de perdidos es 2
10MS
15MS
Paquete BFD
No se detecta un paquete BFD y la cuenta de perdidos es 3, después se declara que el enlace está caído (DOWN)
10MS
Paquete BFD
Si el enrutador B no puede enviar un paquete BFD en este punto debido a un fallo de reenvío

Fig.2

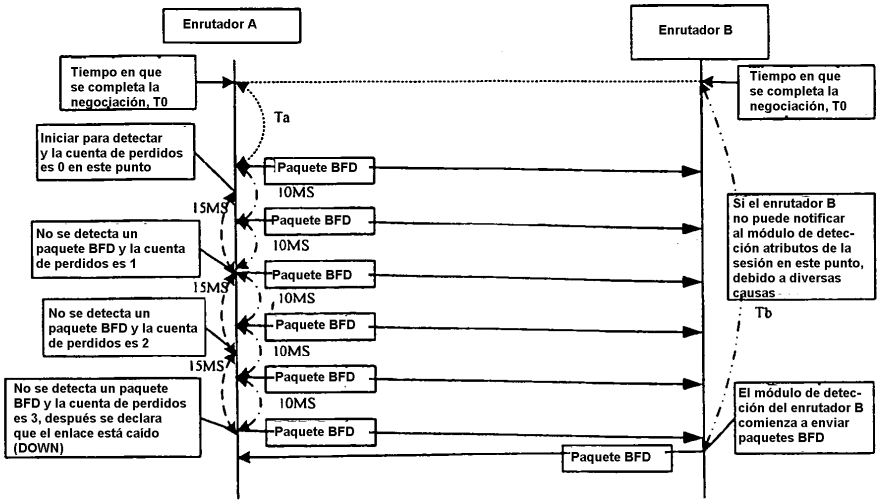
Enrutador A
Enrutador B
Tiempo en que se completa la negocjación, T0
Tiempo en que se completa la negociación, T0
Ta
Iniciar para detectar y la cuenta de perdidos es 0 en este punto
Paquete BFD
10MS
15MS
Paquete BFD
10MS
No se detecta un paquete BFD y la cuenta de perdidos es 1
Si el enrutador B no puede notificar al módulo de detección atributos de la sesión en este punto, debido a diversas causas
Paquete BFD
15MS
10MS
Tb
No se detecta un paquete BFD y la cuenta de perdidos es 2
Paquete BFD
10MS
15MS
El módulo de detección del enrutador B comienza a enviar paquetes BFD
No se detecta un paquete BFD y la cuenta de perdidos es 3, después se declara que el enlace está caído (DOWN)
Paquete BFD
10MS
Paquete BFD
Paquete BFD

Fig.3

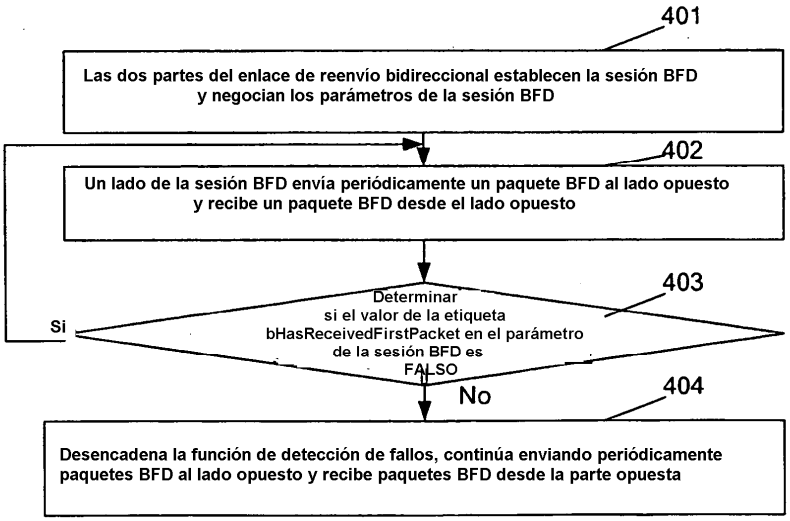
401
Las dos partes del enlace de reenvío bidireccional establecen la sesión BFD y negocian los parámetros de la sesión BFD
402
Un lado de la sesión BFD envía periódicamente un paquete BFD al lado opuesto y recibe un paquete BFD desde el lado opuesto
403
Determinar si el valor de la etiqueta bHasReceivedFirstPacket en el parámetro de la sesión BFD es FALSO
Si
No
404
Desencadena la función de detección de fallos, continúa enviando periódicamente paquetes BFD al lado opuesto y recibe paquetes BFD desde la parte opuesta

Fig.4

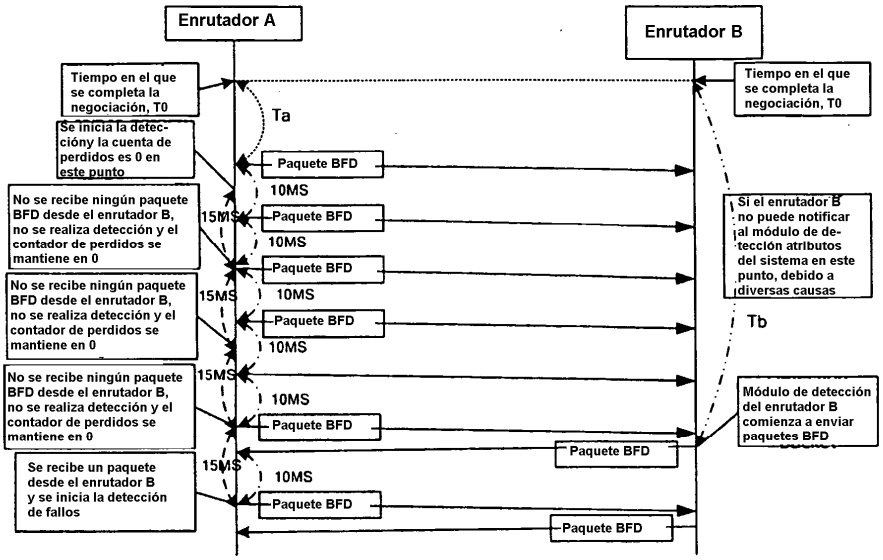
Enrutador A
Enrutador B
Tiempo en el que se completa la negociación, T0
Tiempo en el que se completa la negociación, T0
Ta
Se inicia la detec-ciónyla cuenta de perdidos es 0 en este punto
Paquete BFD
10MS
No se recibe ningún paquete BFD desde el enrutador B, no se realiza detección y el contador de perdidos se mantiene en 0
15MS
Paquete BFD
10MS
Si el enrutador B no puede notificar al módulo de de-tección atributos del sistema en este punto, debido a diversas causas
No se recibe ningún paquete BFD desde el enrutador B, no se realiza detección y el contador de perdidos se mantiene en 0
15MS
Paquete BFD
10MS
Tb
No se recibe ningún paquete BFD desde el enrutador B, no se realiza detección y el contador de perdidos se mantiene en 0
15MS
10MS
Módulo de detección del enrutador B comienza a enviar paquetes BFD
Paquete BFD
Paquete BFD
Se recibe un paquete desde el enrutador B y se inicia la detección de fallos
15MS
10MS
Paquete BFD
Paquete BFD

Fig.5