(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 097**

(51) Int. Cl.:
H04L 12/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07712179 .6**
(96) Fecha de presentación : **08.02.2007**
(97) Número de publicación de la solicitud: **2109958**
(97) Fecha de publicación de la solicitud: **21.10.2009**

(54) Título: **Localización de fallos en arquitecturas basadas en múltiples árboles de expansión.**

(45) Fecha de publicación de la mención BOPI:
18.05.2011

(45) Fecha de la publicación del folleto de la patente:
18.05.2011

(73) Titular/es: **Telefonaktiebolaget LM Ericsson (publ)**
164 83 Stockholm, SE

(72) Inventor/es: **Farkas, János y**
Zhao, Wei

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Campo técnico

La presente invención se refiere a un método para la localización de fallos en redes. Se refiere en particular a un método para localizar fallos en arquitecturas basadas en múltiples árboles de expansión.

Antecedentes

Para que la red de acceso de Ethernet pueda distribuir servicios con calidad de tipo operador, son cada vez más importantes una detección rápida de las averías y un tiempo breve de conmutación por fallo. Después de que se haya detectado una avería y de que los datos se hayan conmutado hacia trayectos alternativos, es necesario que exista un mecanismo para localizar la avería en la red y, a continuación, arreglarla.

El Protocolo Simple de Gestión de Redes (SNMP), RFC1157, proporciona el mecanismo de trampa para que elementos de la red gestionada den la alarma a un sistema de gestión cuando se produce una avería. Las trampas SNMP son eventos predefinidos, entre los cuales, por ejemplo, "enlace averiado" ("*link down*") es uno de los eventos más comunes definidos por la RFC 1157 y soportado por todos los proveedores. Cuando se produce una avería de un enlace, el dispositivo de la red gestionada asociado a este enlace emitirá un evento de notificación hacia el sistema de gestión. Tras recibir el evento, el sistema de gestión puede optar por realizar ciertas acciones sobre la base del evento, por ejemplo, arreglar la avería del enlace, etcétera.

Un planteamiento más nuevo, especificado por la IEEE 802.1ag ("Draft Standard for Local and Metropolitan Area Networks – Virtual Bridged Local Area Networks – Amendment 5: Connectivity Fault Management", IEEE 802.1ag, 2005) intenta afrontar la gestión de averías, incluyendo la localización de las mismas, desde la capa 2. Proporciona tanto una arquitectura como mensajes de trabajo que tienen su correspondencia en la Capa 2 con el Ping y el TraceRoute de IP. La esencia de la arquitectura de 802.1ag se encuentra en los dominios de gestión anidados y en la designación de puntos extremos de mantenimiento y puntos intermedios de mantenimiento. La arquitectura anidada proporciona tanto una visión desde un extremo a otro de la red completa a lo largo del trayecto de aprovisionamiento de servicios como un reproductor responsable detallado de cada asalto de la red. Por tanto, cuando se produce una avería de un enlace, resulta sencillo hace frente a la avería, capa a capa, y llegar al nivel en el que reside la responsabilidad y en el que se deben tomar medidas. Aparte de la propia arquitectura, la 802.1ag define también cuatro mensajes para intercambio de información y localización de averías:

Mensajes de comprobación de continuidad:

Estos son mensajes de "latido" emitidos periódicamente por puntos extremos de mantenimiento. Permiten que los puntos extremos de mantenimiento detecten una pérdida de conectividad de servicio entre ellos mismos. Permiten también que puntos extremos de mantenimiento descubran otros puntos extremos de mantenimiento dentro de un dominio, y permiten que puntos intermedios de mantenimiento descubran puntos extremos de mantenimiento.

Mensajes de rastreo de enlaces:

Los mismos son transmitidos por un punto extremo de mantenimiento al producirse una solicitud, del administrador, de realizar un seguimiento del trayecto (salto a salto) hacia un punto extremo de mantenimiento de destino. Permiten que el nodo de transmisión descubra datos de conectividad vitales sobre el trayecto. El concepto es similar al del Traceroute de IP.

Mensajes de bucle de retorno:

Los mismos son transmitidos por un punto extremo de mantenimiento al producirse una solicitud, del administrador, de verificar la conectividad hacia un punto intermedio de mantenimiento o punto extremo de mantenimiento en particular. El bucle de retorno indica si el punto de mantenimiento objetivo es o no accesible; no permite un descubrimiento del trayecto salto a salto. El concepto es similar al del Eco de ICMP (Ping).

Mensaje de AIS:

Proporcionan una notificación asíncrona a otros elementos de la red informando de que se ha producido un fallo en la red Ethernet metropolitana. La AIS se usa típicamente para suprimir alarmas en elementos de red que no sean aquellos que detectan directamente el fallo.

En redes en las que los nodos están interconectados a través de múltiples trayectos, el Protocolo de Árbol de Expansión (STP) puede evitar la formación de bucles. Esto garantiza que exista únicamente un trayecto activo entre dos dispositivos de red cualesquiera. La totalidad de trayectos activos forma un denominado árbol de expansión. El Protocolo de Múltiples Árboles de Expansión (MSTP) permite establecer una correspondencia de varias VLANs con un número reducido de árboles de expansión. Esto es posible debido a que la mayoría de las redes no requieren más que unas pocas topologías lógicas. Cada árbol puede gestionar múltiples VLANs que tienen la misma topología. Basándose en esto, se han propuesto varias arquitecturas tolerantes a fallos, basadas en múltiples árboles de expansión.

Según describen S. Sharama, K. Gopalan, S. Nanda, y T. Chiueh en "Viking: A multi-spanning-tree Ethernet

architecture for metropolitan area and cluster networks", IEEE INFOCOM 2004, la arquitectura Viking usa múltiples árboles de expansión que se reconfiguran después de un evento de avería. Si ocurre una avería, el Gestor Viking (VM) recibe una notificación por medio de trampas SNMP. El VM notifica entonces a los nodos frontera de la red, de que deben redirigir el tráfico hacia árboles no dañados e inicia el nuevo cálculo y la reconfiguración de los árboles.

Por contraposición, el concepto de una Ethernet flexible de bajo coste se basa en árboles de expansión estáticos que se configuran antes del funcionamiento de la red y no cambian a pesar de la aparición de averías (J. Farkas, C. Antal, G. Toth y L. Westberg, "Distributed Resilient Architecture for Ethernet Networks", *Proceedings of Design of Reliable Communication Networks*, 16 a 19 de octubre de 2005, págs. 512 a 522; J. Farkas, C. Antal, L. Westberg, A. Paradisi, T. R. Tronco y V. G. Oliveira, "Fast Failure Handing in Ethernet Networks", *Proceedings of IEEE International Conference on Communications*, 11 a 15 de junio de 2006; J. Farkas, A. Paradisi, y C. Antal, "Low-cost survivable Ethernet architecture over fiber", *J. Opt. Netw.* 5, págs. 398 a 409, 2006). En esta arquitectura, se implementan una detección de averías y una gestión de fallos de una manera distribuida en los nodos frontera. Esta arquitectura consta de conmutadores de Ethernet convencionales, de serie, de bajo coste, disponibles en el mercado; se excluye cualquier solución que se fundamente en una nueva funcionalidad de los conmutadores de Ethernet, con el fin de mantener la ventaja del precio de los productos de Ethernet actuales. Las funcionalidades adicionales que son necesarias para proporcionar flexibilidad se implementan en forma de un protocolo de software en los nodos frontera de la red Ethernet.

La Fig. 2 muestra un ejemplo correspondiente a dicha arquitectura. Por la red se establecen estáticamente múltiples árboles de expansión predefinidos para que actúen como trayectos o bien principales o bien alternativos que se pueden usar para encaminar tráfico en la red, pudiendo de este modo gestionar posibles averías. Para lograr protección contra cualquier avería individual de un enlace o nodo, la topología de los árboles de expansión debe ser tal que quede por lo menos un árbol funcional completo en caso de avería de cualquier elemento de red individual. Por lo tanto, los árboles de expansión deben ser parcialmente disjuntos, es decir, deben comprender diferentes elementos de red, no pueden ser idénticos. Por ejemplo, se pueden calcular árboles de expansión. Se pueden gestionar múltiples averías con más árboles; es cuestión del diseño de los árboles. Los árboles de expansión se establecen antes de la puesta en marcha de la red, permaneciendo invariables durante el funcionamiento, incluso en presencia de una avería.

En el caso de una avería, cada nodo frontera debe dejar de reenviar tramas a los árboles afectados y debe redirigir el tráfico hacia árboles no dañados. Por lo tanto, es necesario un protocolo para la detección de averías y para notificar a todos los nodos frontera sobre los árboles deteriorados. El tiempo de conmutación por fallo depende principalmente del tiempo transcurrido entre el evento de la avería y su detección por parte de los nodos frontera ya que la conmutación de protección desde un árbol a otro se realiza sin ninguna reconfiguración de los conmutadores de Ethernet.

El Protocolo de Gestión de Averías (FHP) es un protocolo distribuido sencillo y ligero, implementado en los nodos frontera, que se basa en unos pocos mensajes de difusión general para proporcionar una protección rápida contra una avería individual de un enlace o nodo que se produce en la red.

El protocolo define básicamente tres tipos de mensajes de difusión general:

- *En funcionamiento*: mensaje enviado periódicamente por uno o más nodos frontera a los que se hace referencia como *emisor* a través de cada VLAN según un intervalo de tiempo predefinido $T_{Funcionamiento}$;

- *Avería*: mensaje emitido por un nodo frontera denominado *notificador* cuando, en un intervalo de detección predefinido T_{DI}, no llega a través de una VLAN un mensaje En funcionamiento, para informar a la totalidad del resto de nodos frontera sobre una avería en esa VLAN;

- *Reparada*: mensaje emitido por el mismo *notificador* que detectó una avería, cuando llega un mensaje En funcionamiento a través de una VLAN que había fallado previamente, para informar a la totalidad del resto de nodos frontera sobre la reparación de la VLAN que había fallado.

Se distinguen dos tipos de *notificadores* basándose en los ajustes de sus temporizadores: *primarios* y *secundarios*. Hay pocos *notificadores* configurados como *primarios*; al resto que no son ni *emisores* ni *notificadores primarios* se les denomina *notificadores secundarios*. La razón de diferenciar *notificadores primarios* y *secundarios* es reducir el número de mensajes de notificación simultáneos durante un evento de avería, según se detalla posteriormente.

Tal como se muestra en la Fig. 3, los mensajes En funcionamiento son difundidos de forma general periódicamente por el nodo frontera *emisor* a través de cada VLAN en el comienzo del intervalo de tiempo $T_{Funcionamiento}$. El requisito es que los mensajes En funcionamiento sean recibidos en todas las VLANs en cada uno de los otros nodos frontera (*notificadores*) en el intervalo de tiempo predefinido T_{DI}. Debido a que el retardo de transmisión es, en general, diferente para cada *notificador*, y los intervalos de tiempo del protocolo son cortos, la sincronización de los *notificadores* con respecto al *emisor* tiene una importancia clave. Por lo tanto, cada *notificador* pone en marcha un temporizador cuando ha llegado el primer mensaje En funcionamiento con el fin de medir cuándo ha transcurrido el T_{DI}, es decir, el primer mensaje En funcionamiento recibido sincroniza el *notificador* con el *emisor*. De este modo, se ha eliminado el efecto de la diferencia en el retardo de transmisión entre *notificadores* diferentes. Los mensajes En funcionamiento posteriores experimentan un retardo algo diferente ya que se desplazan por un trayecto diferente, lo cual se ha de tener

en cuenta durante la configuración de T_{DI}. La llegada de todos los mensajes En funcionamiento se registra en cada nodo frontera *notificador*. Si hay mensajes En funcionamiento que no han llegado dentro de T_{DI}, entonces las VLANs correspondientes se consideran averiadas. Es decir, la pérdida de un mensaje En funcionamiento individual se interpreta como la avería de una VLAN. No obstante, para evitar falsas alarmas debidas a una pérdida de trama del mensaje En funcionamiento, los *notificadores* se pueden configurar para esperar dos o tres periodos subsiguientes de En funcionamiento, y marcar una VLAN como averiada únicamente si se pierde regularmente un mensaje En funcionamiento en cada periodo.

Todos los nodos frontera, excepto el *emisor*, supervisan la recepción de mensajes En funcionamiento. No obstante, para evitar una carga excesiva del protocolo después de una avería, existen solamente unos pocos nodos frontera *notificadores primarios* cuya función es notificar a otros nodos frontera sobre la avería. El intervalo de detección de los *notificadores primarios* es menor que el de los *notificadores secundarios*, y se puede ajustar dependiendo del tamaño de la red y de otros parámetros. Cuando un nodo frontera *notificador* detecta una avería, difunde de forma general un mensaje *Avería* a través de cada VLAN operativa que se considera no dañada, el cual contiene las IDs de las VLANs averiadas. Puesto que cada nodo frontera recibe los mensajes *Avería*, todos ellos tienen conocimiento de las VLANs averiadas.

Puesto que el número de *notificadores primarios* está limitado de manera intencionada, algunas averías podrían ser no detectadas dependiendo de la topología de la red. Por lo tanto, si un *notificador secundario* detecta una avería basándose en que se echa en falta la llegada de un mensaje *En funcionamiento*, entonces este nodo difunde de forma general el mensaje *Avería* para informar a la totalidad del resto de nodos frontera sobre la avería de la misma manera que se ha descrito anteriormente.

Los planteamientos basados en el SNMP y el CFM tienen sus limitaciones. Por ejemplo, el SNMP depende del funcionamiento correcto del IP, el cual no es siempre válido en un entorno de acceso a Ethernet de la capa 2. Se pueden usar trampas SNMP para la localización de fallos según se propone, por ejemplo, en la arquitectura Viking expuesta anteriormente. No obstante, puede haber nodos de red que no puedan enviar trampas SNMP, por ejemplo, nodos no gestionables, nodos no configurados o configurados de forma defectuosa. En este caso, las trampas SNMP no pueden resolver la localización de fallos. La 802.1ag es una norma relativamente nueva y el mecanismo especificado es complejo, y su eficacia no ha sido demostrada todavía. No obstante, los planteamientos basados tanto en el SNMP como en el CFM tienen un problema en común: carecen del mecanismo adecuado de conmutación por fallo. Ambas soluciones pueden identificar cuándo y en dónde se produce una avería de un enlace, pero ninguna de ellas tiene una solución completa sobre cómo orientar a la red para eludir la avería.

Un documento de Luke Demoracski: “Fault-Tolerant Beacon Vector Routing for Mobile Ad Hoc Networks” *Parallel and Distributed Processing Symposium*, 2005 Proceedings, 19ª IEEE International, Denver, Co, USA, 04 a 08 de abril de 2005, Piscataway, NJ, USA, IEEE, 4 de abril de 2005, presenta un planteamiento nuevo y robusto de Encaminamiento por Vectores de Balizas (BVR) Tolerante a Fallos, con múltiples mejoras novedosas. El algoritmo de tolerancia a fallos NetRec se amplió para aplicarse al BVR. La nueva técnica, ManRec, proporciona tolerancia a los fallos en presencia de múltiples fallos simultáneos, aunque el encaminamiento por vectores de balizas descrito en el documento no es aplicable a las redes que fundamentan la presente invención. El ManRec no usa conocimiento global sobre la topología de la red, es decir, no se definen árboles.

La publicación de patente WO 2006135282 describe una red con varios nodos en los que se configuran redes de área local virtuales, VLANs. Cada VLAN conecta nodos predeterminados. Se envían mensajes de tipo en funcionamiento, de difusión general, a intervalos regulares, para comprobar si las VLANs están en funcionamiento. Los nodos registran si los mensajes de tipo en funcionamiento llegan, y cuando se echa en falta un mensaje esperado, se envía una notificación de difusión general a otros de los nodos. Después de esta notificación, estos nodos sabrán cuáles de las VLANs no son utilizables en ese momento.

La publicación de patente US2004160904 describe un nodo de un sistema de árboles de expansión que funciona en una red que conecta una pluralidad de nodos. Comprende dos unidades de transferencia que determinan un puerto de destino de salida, basándose en la dirección MAC de destino de una trama de entrada, dos gestores de árboles que configuran un árbol de expansión de acuerdo con un protocolo de árboles de expansión, y un puerto virtual de conexión del gestor de árboles y la unidad de transferencia, aunque no da a conocer ninguna información que permita localizar un fallo en la red.

Sumario

Es un objetivo de la presente invención superar por lo menos algunas de las desventajas anteriores y proporcionar un método mejorado de localización de un fallo en una red.

Según un primer aspecto de la presente invención, se proporciona un método de localización de un fallo en una red. La red comprende nodos, enlaces, y nodos frontera configurados en forma de una pluralidad de árboles de expansión, siendo cada árbol un conjunto de nodos y enlaces. Los árboles de expansión son parcialmente disjuntos. El método comprende recibir información sobre la configuración de la pluralidad de topologías de árboles en la red y monitorizar la conectividad de todos los árboles de la red mediante la monitorización de una notificación de pérdida de conectividad. Se recibe una notificación de pérdida de conectividad. Al producirse la detección de una notificación de

una pérdida de conectividad en la red, la localización del fallo se determina como uno de los elementos de red comunes a los árboles que han fallado.

En una primera configuración del aspecto anterior, se pueden determinar y excluir elementos de red que forman parte de árboles que no han fallado.

En otra configuración del aspecto anterior, los elementos de red restantes se pueden comprobar en búsqueda de un fallo.

En otra configuración del aspecto anterior, la etapa de monitorización de la conectividad de la red puede comprender además monitorizar una notificación de pérdida de conectividad en uno o más árboles.

Todavía en otra configuración del aspecto anterior, dicha notificación puede comprender una identificación del árbol que ha fallado.

En una configuración adicional del aspecto anterior, dicha notificación puede comprender además información de trayecto desde un nodo frontera de difusión general a un nodo frontera informador de averías.

En otra configuración del aspecto anterior, se puede aplicar una monitorización de la conectividad de punto-a-punto y dicha notificación puede comprender además información referente a qué conexiones de punto-a-punto han fallado.

Todavía en una configuración adicional del aspecto anterior, mensajes de Rastreo de Enlaces recuperan información del trayecto.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un método de notificación de pérdida de conectividad en una red. La red comprende nodos, enlaces, y nodos frontera dispuestos en forma de una pluralidad de árboles de expansión, de manera que los árboles de expansión son parcialmente disjuntos, comprendiendo además la red medios para gestión de redes. El método comprende además la monitorización de mensajes En funcionamiento difundidos de forma general por otro nodo frontera. Al detectar que se echa en falta un mensaje En funcionamiento, se notifica a la gestión de la red sobre una pérdida de conectividad.

En una primera configuración del aspecto anterior, la etapa de notificación a la gestión de la red puede comprender enviar la identificación del(de los) árbol(es) que ha(n) fallado.

En otra configuración del aspecto anterior, dicha notificación puede comprender además información de trayecto desde el nodo frontera de difusión general hacia el nodo frontera informador de averías.

En una configuración adicional del aspecto anterior, al producirse la detección de una pérdida de conectividad en un árbol, nodos frontera puede redirigir el tráfico hacia árboles no afectados por la pérdida de conectividad.

Según un tercer aspecto de la presente invención, se proporciona una gestión de red adaptada para funcionar de acuerdo con el primer aspecto o cualquiera de sus configuraciones.

En una configuración del tercer aspecto, la gestión de red comprende un servidor.

Según un cuarto aspecto de la presente invención, se proporciona un nodo frontera adaptado para funcionar de acuerdo con el segundo aspecto o cualquiera de sus configuraciones.

La presente invención puede proporcionar una localización eficaz de fallos cuando se usen topologías lógicas de múltiples árboles. Por otra parte, no introduce un gasto adicional en los cometidos de los nodos frontera para la gestión de fallos.

Breve descripción de los dibujos

La Fig. 1 ilustra un ejemplo de una topología física.

La Fig. 2 ilustra un ejemplo de topologías lógicas.

La Fig. 3 muestra un diagrama esquemático de secuencia temporal de los mensajes del protocolo y los cometidos de los nodos.

La Fig. 4 muestra un diagrama de flujo de notificación de un fallo en una red de acuerdo con la presente invención.

La Fig. 5 muestra un diagrama de flujo de localización de un fallo en una red de acuerdo con la presente invención.

Descripción detallada

En los documentos anteriores de J. Farkas, C. Antal, G. Toth, L. Westberg; J. Farkas, C. Antal, L. Westberg, A. Paradisi, T. R. Tronco, V. G. Oliveira; y J. Farkas, A. Paradisi y C. Antal, se describe de forma detallada una arquitectura

de red basada en múltiples árboles de expansión. Por consiguiente, en la red se implementan topologías lógicas de árboles con el fin de proporcionar flexibilidad. Los árboles no son disjuntos de forma completa, sino parcial, con el fin de evitar una complejidad significativa de la gestión provocada por los árboles. El método según la presente invención funciona de forma independiente con respecto al diseño de las topologías de los árboles.

La arquitectura subyacente consta de nodos internos y Nodos Frontera (EN) y los enlaces de interconexión. Los nodos internos pueden ser equipos de serie sin ninguna funcionalidad especial relacionada con la arquitectura. Por el contrario, los nodos frontera implementan el Método de Gestión de Averías (FHM) antes descrito. Según este método, en cada árbol se difunde de forma general un mensaje denominado En funcionamiento, y en los nodos frontera se monitoriza la llegada de estos mensajes. Basándose en mensajes En funcionamiento perdidos, se puede detectar la avería (o pérdida de conectividad) de árboles, y nodos frontera pueden redirigir el tráfico hacia árboles no dañados. La reanudación se puede resolver también basándose en mensajes En funcionamiento, recién aparecidos, sobre árboles que estaban averiados.

También se pueden aplicar otros métodos de monitorización de conectividad, por ejemplo, CFM ó BFD, los cuales son métodos de monitorización de punto-a-punto. Es necesario que se monitoricen todos los árboles entre cada uno de los pares de nodos frontera, y se debe informar al sistema de gestión sobre la avería. Así, se puede aplicar el método de localización de fallos descrito en la presente invención.

Suponiendo que en la red se aplica el método de gestión de fallos antes descrito, se puede determinar la localización del fallo. Puesto que, después del fallo, se difunde de forma general un mensaje Avería que contiene la ID de las topologías (árboles) lógicas averiadas, cada nodo frontera tiene conocimiento de los árboles averiados, lo cual se puede propagar hacia el sistema de gestión que calculó y configuró los árboles. Cada árbol es un conjunto de nodos y enlaces. El elemento averiado está en la intersección de los árboles averiados, el cual puede ser un único nodo o enlace o muy pocos nodos o enlaces. Por consiguiente, la localización del fallo es uno de los elementos de red en la intersección de los árboles averiados.

El conjunto de elementos averiados se puede restringir todavía más ya que el sistema de gestión sabe también que cada nodo y enlace de los árboles operativos que sobrevivieron a la avería están también funcionando. Por lo tanto, se puede obtener un conjunto más pequeño de elementos posiblemente averiados si, de la intersección de los árboles averiados, se eliminan todos aquellos enlaces y nodos que forman parte de cualquiera de los árboles operativos.

Una mejora adicional de la precisión puede ser que, durante la generación de múltiples árboles, en cada nodo frontera, además de la ID del árbol, se almacene también la información de trayecto desde el emisor al nodo frontera. Cuando se produce una avería de enlace o nodo, el nodo frontera envía un mensaje de avería con la información tanto de la ID de árbol como del trayecto. De este modo, el posible fallo se puede circunscribir adicionalmente a un trayecto de un árbol o varios trayectos de múltiples árboles. Los árboles de expansión tolerantes a fallos se calculan fuera de línea y se configuran antes de la puesta en marcha de la red y permanecen estáticos durante el funcionamiento de la misma. La información del trayecto hacia el emisor se puede almacenar en cada nodo frontera durante esta fase de configuración. Otra posibilidad para recuperar información del trayecto puede ser con la ayuda de mensajes de Rastreo de enlaces si se aplica la IEEE 802.1ag en la red.

Tal como se muestra en la Fig. 4, los fallos son gestionados por los nodos frontera según se describe brevemente en la sección previa. En la etapa 410, los nodos frontera están monitorizando para detectar mensajes En funcionamiento perdidos. Los nodos frontera tienen conocimiento de las topologías de árboles averiadas y no dañadas, y pueden dirigir el tráfico hacia árboles disponibles que proporcionen conectividad en la red. Si se almacena la información del trayecto, el nodo frontera tendrá conocimiento también de su trayecto hacia el emisor.

Puesto que los nodos frontera tienen conocimiento de qué topologías lógicas están averiadas, pueden notificar a la gestión de red (NM) las topologías averiadas en la etapa 420. Si se almacena también información de trayecto, entonces los nodos frontera informan también a la NM sobre el(los) trayecto(s) averiado(s) del(de los) árbol(es). La gestión de red tiene conocimiento de todas las topologías lógicas en la red, ya que la red había sido configurada por la gestión de red anteriormente. Por lo tanto, basándose en esta información se pueden determinar elementos de red posiblemente averiados, de la manera siguiente:

Únicamente podrían está averiados aquellos enlaces o nodos que estén incluidos en todas las topologías lógicas averiadas.

En referencia a la Fig. 5, el método de localización de fallos según la presente invención funciona de la siguiente manera:

- En la etapa 510, la gestión de red recibe información sobre la configuración de las topologías de árboles configuradas en la red.
- En la etapa 520, se monitoriza la conectividad en la red.
- En la etapa 530, se informa a la gestión de red sobre los árboles que están averiados en caso de un acontecimiento de avería. Esta información se puede recibir desde nodos frontera. Si también hay disponible información de trayecto, entonces también se puede enviar hacia la Gestión de Red información sobre el(los)

trayecto(s) fallido(s) o averiado(s).

• En la etapa 540, se determinan elemento(s) de red común(es) de todos los árboles dañados.

Adicionalmente, del conjunto de elementos que posiblemente han fallado se pueden excluir aquellos elementos que forman parte de árboles no afectados.

Además, también se puede tener en cuenta la información sobre qué nodo frontera informó de la avería y qué nodo frontera es el que difunde de forma general los mensajes En funcionamiento: elemento(s) de red común(es) en árboles dañados en el trayecto entre nodos de difusión general e informadores de fallos. Si se aplica una monitorización de la conectividad de punto-a-punto, por ejemplo, el CFM, entonces también es una información útil para la localización de fallos que los nodos frontera informen sobre el trayecto entre aquellos pares de nodos frontera que están averiados. Si también hay disponible información de trayecto sobre trayecto(s) averiado(s), entonces la misma también se puede usar para determinar el(los) elemento(s) averiado(s).

• Los elementos de red identificados así como que posiblemente han fallado pueden ser comprobados.

En la siguiente red de ejemplo, cuya topología física se muestra en la Fig. 1, se ilustra una localización de fallos según la presente invención. La red de ejemplo consta de cuatro nodos internos SW1, SW2, SW3 y SW4, cuatro nodos frontera EN1, EN2, EN3 y EN4, y nueve enlaces que interconectan estos nodos.

En referencia a la Fig. 2, se supone una arquitectura de red basada en múltiples árboles de expansión, según se ha descrito detalladamente en los documentos anteriores de J. Farkas, C. Antal, G. Toth, L. Westberg; J. Farkas, C. Antal, L. Westberg, A. Paradisi, T. R. Tronco, V. G. Oliveira; y J. Farkas, A. Paradisi, y C. Antal. Se determinan de forma correspondiente topologías de árboles con el fin de gestionar averías individuales tal como se representa en la Fig. 2, que ilustra un ejemplo de las topologías lógicas que fundamentan la presente invención. Son necesarios tres árboles (T1, T2, y T3) para gestionar todas las posibles averías individuales en esta red ejemplificativa. La red y sus elementos son idénticos a la representación de la Fig. 1.

Si se produce una avería, entonces por lo menos uno de los árboles dejará de funcionar.

Por ejemplo, si uno de los nodos frontera informa a la gestión de red de que el árbol T2 dejó de funcionar (y suponiendo que únicamente este árbol está averiado, es decir, no se recibió ningún informe de avería en otros árboles) entonces la gestión de red concluye que puede que solamente un elemento del árbol T2 tenga un fallo: EN1, SW1, EN2, SW4, EN4, EN3 y los enlaces respectivos entre ellos.

Eliminando además aquellos elementos del árbol T2 que también forman parte de los árboles no afectados T1 y T3, el conjunto de elementos que posiblemente han fallado se puede limitar adicionalmente al enlace entre el nodo SW1 y el nodo SW4 y/o el enlace entre el nodo frontera EN2 y el nodo SW1.

Aplicando los cometidos de los nodos frontera para el Método de Gestión de Fallos (FHM), se puede determinar todavía de forma más precisa la ubicación del fallo. Si el nodo frontera EN1 difunde de forma general los mensajes En funcionamiento y el nodo frontera EN2 informa sobre la avería, entonces, de aquí se deduce que el enlace entre el nodo frontera EN2 y el nodo SW1 dejó de funcionar.

Este fallo se puede localizar también basándose en información de trayecto, si es que esta información se implementa también en la red y se incluye en mensajes de avería. En ese caso, el mensaje de avería se notifica al sistema de gestión junto con la siguiente información de trayecto: EN2-SW1-EN1. El nodo SW1, el nodo frontera EN1 y el enlace entre estos dos nodos forman parte también del árbol T1, y se sabe que el árbol T1 está en funcionamiento. Por lo tanto, de aquí se deduce que o bien EN2 ó bien el enlace entre EN2 y el nodo SW1 está averiado.

Usando el mismo método, se deduce que si el nodo frontera EN3 ó el nodo frontera EN4 informa sobre la avería, entonces el enlace entre el nodo SW1 y el nodo SW4 es el averiado.

Se plantea un caso más complejo si únicamente el árbol T2 sobrevive a una avería, es decir, tanto el árbol T1 como el árbol T3 están averiados. En este caso, pueden estar averiados o bien el nodo SW2 ó el nodo SW3 o bien el enlace entre el nodo frontera EN2 y el nodo SW3, pero no es posible identificar el elemento de red preciso que provoca el fallo.

La situación más difícil se puede plantear cuando el nodo frontera EN2 difunde de forma general los mensajes En funcionamiento. Si cualquier otro nodo frontera difunde de forma general el mensaje En funcionamiento, entonces la ubicación del fallo se puede localizar basándose en qué nodo(s) frontera informó(informaron) sobre la avería. No obstante, si el nodo frontera EN2 difunde de forma general los mensajes En funcionamiento, entonces resulta sencillo averiguar cuándo está averiado el nodo SW2, ya que, en ese caso, el nodo frontera EN1 informa sobre la avería del árbol T3 y el nodo frontera EN3 informa sobre la avería del árbol T1. Por otro lado, no es posible determinar si está averiado el nodo SW3 ó únicamente el enlace entre SW3 y EN2, ya que en este caso la totalidad del resto de nodos frontera informa sobre la avería tanto del árbol T1 como del árbol T3, pero la Gestión de Red puede comprobar si el nodo SW3 está disponible. Es decir, en este caso no se puede hallar el elemento de red exacto, pero se determina la ubicación de la avería.

La totalidad del resto de elementos de red averiados se puede determinar basándose en la información de los árboles averiados y el(los) informador(es) de la(s) avería(s) y el nodo frontera de difusión general en este ejemplo. En redes más grandes, usando este método el conjunto de elementos de red posiblemente averiados se puede limitar a unos pocos.

El método propuesto da un paso más allá basándose en los cometidos de los nodos frontera para el Método de Gestión de Fallos (FHM), y, junto con ello, puede proporcionar una solución completa para una conmutación por fallo y una detección de fallos rápidas. No introduce un gasto adicional en los cometidos de los nodos frontera para el FHM, heredando así todas las ventajas, tales como la cualidad de ser ligero, velocidad, y eficacia.

El método propuesto es sencillo y se puede aplicar eficazmente para la localización de fallos cuando se usen topologías lógicas de múltiples árboles para el reenvío de tráfico y se monitorice la disponibilidad de estas topologías. De este modo, el método propuesto se puede aplicar sencillamente en una arquitectura de bajo coste que proporcione únicamente características básicas. Además, el método propuesto se puede aplicar también en redes que consten de nodos que proporcionen características mejoradas, como la IEEE 802.1ag.

Otra posible ventaja que puede ofrecer la propuesta es que el cálculo realizado por el sistema de gestión con la finalidad de localizar los fallos puede proporcionar indicios estadísticos sobre el uso de los enlaces y posibles cuellos de botella de la red, que pueden resultar muy útiles para la asignación y optimización de recursos de la red.

REIVINDICACIONES

1. Un método de localización de un fallo en una red,

comprendiendo la red nodos (SW1, SW2, SW3, SW4), enlaces, y nodos frontera (EN1, EN2, EN3, EN4) configurados en forma de una pluralidad de árboles de expansión, siendo cada árbol un conjunto de nodos y enlaces, siendo parcialmente disjuntos los árboles de expansión;

comprendiendo el método las etapas de:

- recibir información (510) sobre la configuración de la pluralidad de topologías de árboles en la red;

- monitorizar la conectividad (520) de todos los árboles en la red mediante la monitorización de una notificación de pérdida de conectividad en uno o más árboles; recibir una notificación de pérdida de conectividad

- al producirse la detección de una notificación de pérdida de conectividad en la red, identificar árboles que han fallado (530);

caracterizado porque

el método comprende además la etapa de:

- determinar la ubicación del fallo (540) como uno de los elementos de red comunes a los árboles que han fallado.

2. El método según la reivindicación 1, que comprende además determinar y excluir elementos de red que forman parte de árboles que no han fallado.

3. El método según cualquiera de las reivindicaciones anteriores, que comprende además la etapa de comprobar los elementos de red restantes en busca de un fallo.

4. El método según la reivindicación 1, en el que dicha notificación de pérdida de conectividad comprende una identificación del árbol que ha fallado.

5. El método según la reivindicación 4, en el que dicha notificación de pérdida de conectividad comprende además información del trayecto desde un nodo frontera de difusión general hacia un nodo frontera informador de averías.

6. El método según la reivindicación 4, en el que se aplica una monitorización de conectividad de punto-a-punto y dicha notificación de pérdida de conectividad comprende además información referente a qué conexiones de punto-a-punto han fallado.

7. El método según la reivindicación 5, en el que se recupera información del trayecto mediante mensajes de Rastreo de Enlaces.

8. Una gestión de red adaptada para funcionar según todas las etapas del método de acuerdo con una cualquiera de las reivindicaciones 1 a 7.

9. La gestión de red según la reivindicación 8, en la que la gestión de red comprende un servidor.

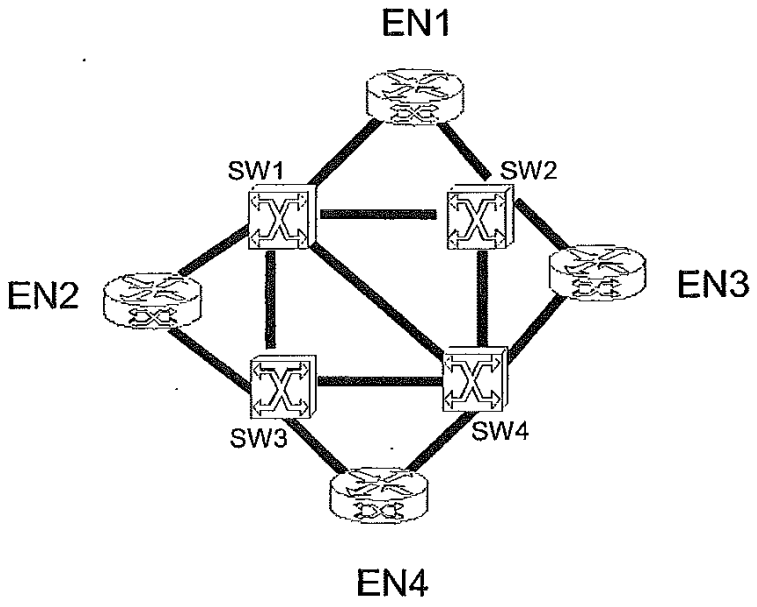
EN1
SW1
SW2
EN2
EN3
SW3
SW4
EN4

Fig. 1

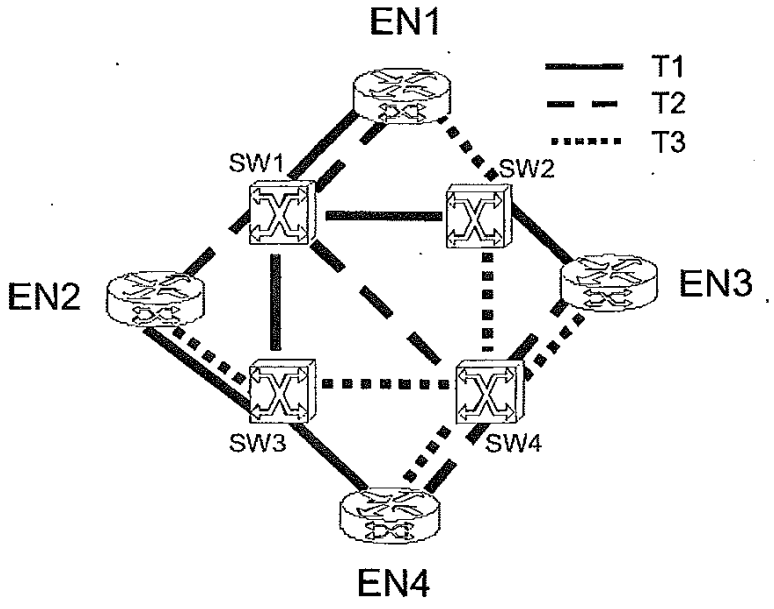
EN1
T1
T2
T3
SW1
SW2
EN2
EN3
SW3
SW4
EN4

Fig. 2

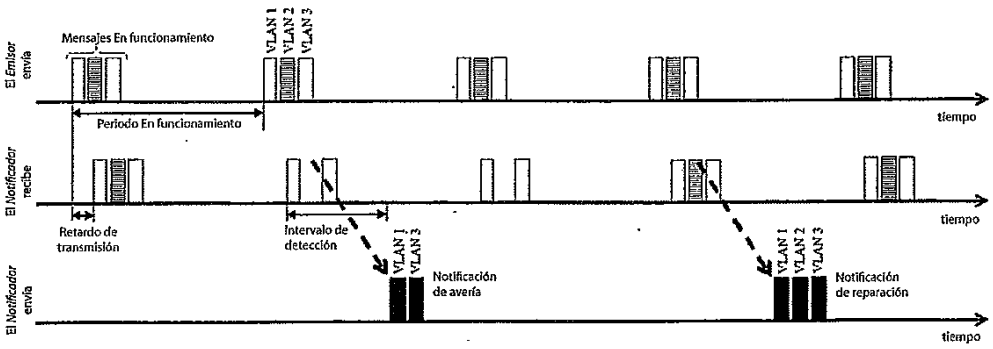
El Emisor envía
Mensajes En funcionamiento
VLAN 1
VLAN 2
VLAN 3
Periodo En funcionamiento
tiempo
El Notificador recibe
Retardo de transmisión
Intervalo de detección
tiempo
El Notificador envía
VLAN 1
VLAN 3
Notificación de avería
VLAN 1
VLAN 2
VLAN 3
Notificación de reparación
tiempo

Fig. 3

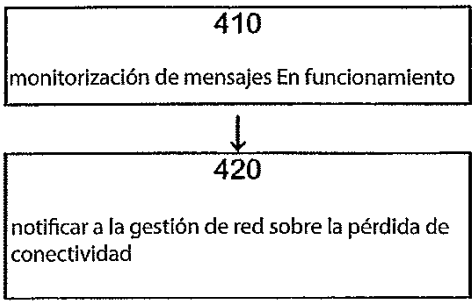
410
monitorización de mensajes En funcionamiento
420
notificar a la gestión de red sobre la pérdida de conectividad

Fig. 4

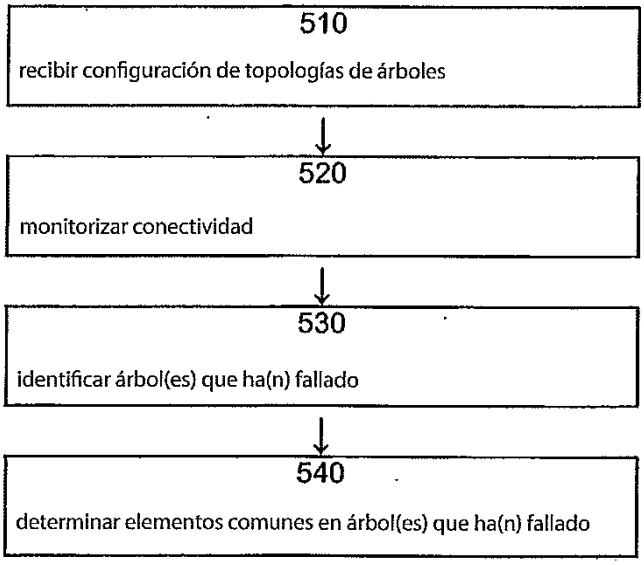
510
recibir configuración de topologías de árboles
520
monitorizar conectividad
530
identificar árbol(es) que ha(n) fallado
540
determinar elementos comunes en árbol(es) que ha(n) fallado

Fig. 5