

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 380 387**

51 Int. Cl.:
H04L 12/26 (2006.01)
H04L 12/28 (2006.01)
H04L 12/437 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

- 96 Número de solicitud europea: **07817055 .2**
96 Fecha de presentación: **10.10.2007**
97 Número de publicación de la solicitud: **2086175**
97 Fecha de publicación de la solicitud: **05.08.2009**

54 Título: **Método y aparato para proteger un anillo ethernet**

30 Prioridad:
23.01.2007 CN 200710073029

45 Fecha de publicación de la mención BOPI:
11.05.2012

45 Fecha de la publicación del folleto de la patente:
11.05.2012

73 Titular/es:
**HUAWEI TECHNOLOGIES CO., LTD.
HUAWEI ADMINISTRATION BUILDING BANTIAN
LONGGANG DISTRICT
SHENZHEN, GUANGDONG PROVINCE 518129,
CN**

72 Inventor/es:
LONG, Hao

74 Agente/Representante:
Lehmann Novo, Isabel

ES 2 380 387 T3

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

DESCRIPCIÓN

Método y aparato para proteger un anillo ethernet.

CAMPO DE LA INVENCION

5 La presente invención se refiere a tecnologías de Ethernet y en particular, a un método y aparato para Protección de Anillo Ethernet (ERP).

ANTECEDENTES DE LA INVENCION

10 Con el rápido desarrollo de Ethernet de clase portadora, la protección ERP se convierte en un método de protección de servicio Ethernet que atrae una amplia atención en el sector. Sobre la base de una topología de anillo lógico o físico, la protección ERP utiliza el bucle cerrado y las características de Ethernet para poner en práctica la conmutación de servicios con protección rápida de punto a punto, punto a multipunto y multipunto a multipunto. La protección ERP se caracteriza por la alta tasa de utilización del ancho de banda, la alta velocidad de la conmutación de protección, bajo coste de construcción de la red y soporte de conmutación de servicios punto a multipunto y multipunto a multipunto.

15 La red de anillo Ethernet adopta una topología de anillo en la capa física. Con el fin de impedir el bucle infinito de un paquete en el anillo de Ethernet, se establece un puerto bloqueado en la capa de enlace. Cuando el paquete de servicio pasa a través del puerto bloqueado, el puerto bloqueado descarta el paquete. En general, la misma topología física puede corresponder a múltiples instancias de anillo y cada instancia de anillo tiene un puerto bloqueado correspondiente. Una instancia de anillo puede corresponder a una Red de Área Local Virtual (VLAN) de control y una o un grupo de redes VLAN(s) de servicio. Conviene señalar que la red VLAN de control se suele utilizar para transmitir los mensajes de control de instancias de anillo y el puerto bloqueado no bloquea el paquete y el tráfico en la red VLAN de control.

20 El proceso de la detección y recuperación de fallos de ERP se describe a continuación haciendo referencia a los dibujos adjuntos.

25 La Figura 1 representa una red de anillo Ethernet en la técnica anterior. Según se representa en la Figura 1, los puentes 1 a 6 sirven como nodos para formar un anillo de Ethernet. El puerto 10 del puente 1 es un puerto bloqueado. En condiciones normales, cuando un paquete de servicio pasa a través del puerto bloqueado, el paquete de servicio se descarta por el puerto bloqueado. El proceso de detección y de recuperación de fallos de la red de anillo Ethernet se detalla a continuación:

1. Detección de fallos

30 La detección de fallos de la red de anillo Ethernet se pone en práctica mediante la detección del intervalo del anillo. Más concretamente, los paquetes de Control de Continuidad (CC) se envían periódicamente para comprobar si el enlace entre puentes adyacentes es normal y para detectar los fallos con rapidez. Si un nodo falla en la recepción del paquete CC desde el nodo adyacente dentro de un periodo preestablecido, el enlace entre el nodo y el nodo adyacente se determina como defectuoso.

2. Protección de servicio en el caso de fallos

35 Después de que un nodo detecte un fallo del enlace entre el nodo y su nodo adyacente, el nodo bloquea los puertos en ambos extremos del enlace defectuoso y envía un mensaje de control a otros nodos en el anillo. Después de recibir el mensaje de control, otros nodos desbloquean el puerto normalmente bloqueado, borran la tabla de reenvíos y reinician su auto-aprendizaje.

3. Recuperación de fallos

40 Cuando un nodo detecta que se recupera un fallo, el nodo desbloquea el puerto que está bloqueado debido al fallo del enlace y envía un mensaje de recuperación de fallos a otros nodos en el anillo. Después de recibir el mensaje de recuperación de fallos, otros nodos bloquean de nuevo el puerto normalmente desbloqueado, borran operativamente la tabla de reenvíos y reinician el auto-aprendizaje. La red de anillo Ethernet recupera el estado de trabajo normal.

45 El proceso de ERP, antes descrito en la técnica anterior, da a conocer que todos los nodos en el anillo borran la tabla de reenvíos y reinician su auto-aprendizaje una vez que falla cualquier enlace. De hecho, el auto-aprendizaje no es necesario en las circunstancias siguientes.

50 La Figura 2 representa una topología de una red de anillo Ethernet en la que falla el enlace en donde se encuentra el puerto normalmente bloqueado 10. Según se representa en la Figura 2, cuando se producen los fallos y la recuperación de fallos en el enlace entre el puente 1 y el puente 2, el enlace defectuoso es el enlace en donde se encuentra el puerto normalmente bloqueado. Después de que falle el enlace, los puertos en ambos extremos del enlace están bloqueados. La topología de la red es la misma que la que ocurre antes del fallo. En este caso, los nodos en la red de anillo Ethernet no necesitan el auto-aprendizaje porque las entradas de la tabla de reenvíos, después del auto-aprendizaje, son compatibles con las existentes antes de dicho auto-aprendizaje.

Después de que se borre operativamente la tabla de reenvíos de los nodos en la red de anillo de Ethernet, resulta imposible crear de nuevo una tabla de reenvíos a no ser que se realice un auto-aprendizaje. En el proceso de crear una tabla de reenvíos, existe un tráfico de radiodifusión masivo en la red de anillo Ethernet, lo que aumenta la carga de la red y se ocupan demasiados recursos de ancho de banda. Por lo tanto, es preciso reducir el borrado innecesario de la tabla de reenvíos y el auto-aprendizaje causado por la ocurrencia de fallos y la recuperación de fallos.

El documento EP 1727313 A1 da a conocer mecanismos de conmutación de protección conocidos para las redes en anillo sobre la base de un gestor de redundancias, que están en la práctica limitadas en rendimiento debido a una velocidad limitada para la supresión de entradas desde las bases de datos de reenvíos de los nodos de la red y debido a una velocidad limitada para conocer una nueva topología para la base de datos de reenvíos. Se presenta un método para conmutación de protección automática de Ethernet, mediante el cual se suprime un número reducido de entradas en las bases de datos de reenvíos.

REFERENCIA CRUZADA A SOLICITUDES RELACIONADAS

Esta solicitud reivindica la prioridad para la Publicación Internacional nº WO2008 / 089633A1, presentada el 10 de octubre de 2007, que reivindica el beneficio de prioridad de la Publicación de Patente China nº CN101232428A, presentada el 23 de enero de 2007.

SUMARIO DE LA INVENCION

Un método y aparato de ERP se dan a conocer en una forma de realización de la presente invención para suprimir un borrado operativo innecesario de la tabla de reenvíos y el auto-aprendizaje y para reducir el tráfico de radiodifusión causado por la ocurrencia de fallos y la recuperación de fallos.

Un método de ERP dado a conocer en una forma de realización de la presente invención comprende:

la determinación de si el enlace defectuoso es un enlace en donde se encuentra un puerto normalmente bloqueado cuando un enlace en una red de anillo de Ethernet es defectuoso y

el envío de un mensaje de control que transmite la primera información de indicación, si el enlace defectuoso es el enlace en donde se encuentra el puerto normalmente bloqueado; evitar el borrado, por un nodo del anillo, de una tabla de reenvíos después de recibir el mensaje de control que transmite la primera información de indicación.

Un aparato de ERP dado a conocer en una forma de realización de la presente invención comprende:

un módulo de detección de estado del enlace, adaptado para: detectar un estado del enlace por intermedio de una notificación recibida y para enviar información de fallo del enlace o información de recuperación del fallo del enlace a un módulo de evaluación, después de detectar un fallo de enlace o una recuperación de fallo de enlace;

un módulo de almacenamiento de información, adaptado para almacenar información sobre un puerto normalmente bloqueado en una red de anillo Ethernet;

un módulo de evaluación, adaptado para: evaluar, según la información sobre el puerto normalmente bloqueado almacenada en el módulo de almacenamiento de información, si el enlace defectuoso o el enlace de recuperación de fallo es un enlace en donde se encuentra el puerto normalmente bloqueado y para dar instrucciones a un módulo generador de mensajes de control para enviar un mensaje de control a otros nodos, si el enlace defectuoso o el enlace de recuperación de fallos no es un enlace en donde se encuentra el puerto normalmente bloqueado y

un módulo generador de mensajes de control, adaptado para generar y enviar un mensaje de control a otros nodos adyacentes, en donde el mensaje de control notifica a los demás nodos si borrar, o no, la tabla de reenvíos;

un módulo de adición de identificador, adaptado para añadir, en función de un resultado de evaluación del módulo de evaluación, información de indicación en el mensaje de control generado por el módulo generador de mensajes de control, en donde la información de indicación indica si borrar, o no, la tabla de reenvíos.

Se puede deducir de la solución técnica según la presente invención, lo que sigue: en las formas de realización de la presente invención, evaluando si el enlace defectuoso o el enlace de recuperación de fallos es, o no, un enlace en donde se encuentra el puerto normalmente bloqueado, se toma una decisión sobre si dar instrucciones, o no, a otros nodos en la red de anillo Ethernet para el borrado operativo de la tabla de reenvíos. Por lo tanto, la dificultad para los nodos en la red de anillo para borrar operativamente la tabla de reenvíos y reiniciar el auto-aprendizaje después de que se evite que cualquier enlace se haga defectuoso o que se recupere cualquier fallo de enlace en la técnica anterior, el tráfico de radiodifusión generado por el borrado operativo innecesario de la tabla de reenvíos y el auto-aprendizaje se reduce de forma efectiva y se mejora la tasa de utilización de ancho de banda en la red de anillo Ethernet.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 representa una red de anillo Ethernet en la técnica anterior;

La Figura 2 representa una topología de una red de anillo Ethernet en la que el enlace en donde se encuentra el puerto normalmente bloqueado falla según se ilustra en la Figura 1;

La Figura 3 representa una topología de una red de anillo Ethernet según una forma de realización de la presente invención;

- 5 La Figura 4 es un diagrama de flujo de un método de ERP dado a conocer en la primera forma de realización de la presente invención;

La Figura 5 representa un formato de trama de un paquete de CC, según una segunda forma de realización de la presente invención;

La Figura 6 representa el formato de un campo de indicador en el paquete de CC ilustrado en la Figura 5;

- 10 La Figura 7 es un diagrama de flujo de otro modo de ERP dado a conocer en una forma de realización de la presente invención;

La Figura 8 representa un formato de trama de un paquete de AIS según una tercera forma de realización de la presente invención;

La Figura 9 representa el formato de un campo de identificador en el paquete de AIS ilustrado en la Figura 7;

- 15 La Figura 10 representa una estructura de un aparato de ERP dado a conocer en una cuarta forma de realización de la presente invención;

La Figura 11 representa una estructura de un aparato de ERP dado a conocer en una quinta forma de realización de la presente invención y

- 20 La Figura 12 representa una estructura de un aparato de ERP dado a conocer en una sexta forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LA INVENCION

Con el fin de hacer más evidentes la solución técnica, los objetivos y ventajas de la presente invención, se describe, a continuación, en detalle haciendo referencia a los dibujos adjuntos y formas de realización preferidas.

Forma de realización 1

- 25 La Figura 3 representa una topología de una red de anillo Ethernet en una forma de realización de la presente invención. Según se representa en la Figura 3, los puentes 1 a 6 son nodos en un anillo Ethernet, la referencia 301 corresponde a un puerto normalmente bloqueado, las referencias 302, 303 y 304 se refieren a puertos normales en el anillo y las referencias 305 y 306 corresponden a enlaces entre nodos. Todos los nodos en la red de anillo Ethernet han preconfigurado la información que indica que 301 es un puerto normalmente bloqueado y los otros puertos son puertos ordinarios en el anillo. Conviene señalar que la Figura 3 solamente representa una estructura de topología de red en una forma de realización de la presente invención y no está prevista para limitar la modalidad de la red aplicable a la solución técnica según la presente invención.

La Figura 4 es un diagrama de flujo de un método de ERP dado a conocer en la primera forma de realización de la presente invención. Según se representa en la Figura 4, el método comprende lo siguiente:

- 35 Etapa S401: Se realiza una evaluación sobre si el nodo, en la red de anillo Ethernet, recibe la notificación desde el nodo adyacente dentro de un periodo preestablecido. Si el nodo en la red de anillo Ethernet recibe la notificación desde el nodo adyacente dentro del periodo preestablecido, el proceso prosigue con la etapa S402; en caso contrario, se repite esta etapa.

- 40 En esta etapa, la notificación puede ser un paquete CC y el paquete CC se puede utilizar para detectar fallos entre los nodos en la red de anillo Ethernet.

Cada nodo envía paquetes CC periódicamente a sus nodos adyacentes. Si un nodo deja de recibir el paquete CC desde el nodo adyacente dentro de un periodo preestablecido, el enlace entre el nodo y el nodo adyacente se determina como defectuoso. El proceso de utilizar el paquete CC para detectar el fallo del enlace es el mismo que el de la técnica anterior y por ello, no se detalla a continuación.

- 45 Etapa S402: Se realiza una evaluación sobre si el enlace defectuoso es, o no, un enlace en donde se encuentra el puerto normalmente bloqueado. Si el enlace defectuoso es un enlace en donde se encuentra el puerto normalmente bloqueado, el proceso prosigue con la etapa S403; en caso contrario, el proceso prosigue con la etapa S404.

En esta etapa, todos los nodos en la red de anillo tienen información configurada sobre el puerto normalmente bloqueado. Si el puerto del enlace defectuoso es compatible con el puerto normalmente bloqueado que ha sido

preconfigurado, se determina que el enlace defectuoso es el enlace en donde se encuentran los puertos normalmente bloqueados.

Etapa S403: El nodo que detecta el fallo del enlace evita (es decir, suprime) el envío de un mensaje de control a otros nodos en la red de anillo Ethernet.

- 5 En esta etapa, debido a que el enlace defectuoso es el enlace en donde se encuentran los puertos normalmente bloqueados, la topología de la red, después de la ocurrencia del fallo, es la misma que la que existía antes de que se produjera el fallo. Por lo tanto, el nodo que detecta el fallo no necesita enviar ningún mensaje de control a otros nodos y los otros nodos no regeneran la tabla de reenvíos ni reinician el auto-aprendizaje.

- 10 Etapa S404: El nodo que detecta el fallo del enlace envía un mensaje de control a otros nodos en la red de anillo Ethernet, notificando a otros nodos la regeneración de la tabla de reenvíos.

El mensaje de control puede ser un paquete de Señal de Indicación de Alarma (AIS) en el mecanismo de Operación, Administración y Mantenimiento (OAM) de Ethernet o un paquete de Conmutación de Protección Automática (APS) en el mecanismo de conmutación de protección de Ethernet y se transmite por intermedio de una red VLAN de control. En esta forma de realización, el paquete de AIS se toma como ejemplo.

- 15 En esta etapa, puesto que el enlace defectuoso no es el enlace en donde se encuentran los puertos normalmente bloqueados, el puerto normalmente bloqueado se desbloquea después de la ocurrencia del fallo, los puertos en ambos extremos del enlace defectuoso quedan bloqueados y la topología de la red cambia después de la ocurrencia del fallo. Por lo tanto, el nodo que detecta el fallo necesita enviar un paquete de AIS a otros nodos, notificando a dichos otros nodos la regeneración de la tabla de reenvíos y la reiniciación del auto-aprendizaje para crear una nueva tabla de reenvíos.

- 20 En esta forma de realización, cuando el nodo en la red de anillo detecta la recuperación del fallo, el método comprende, además:

- la evaluación de si el enlace recuperado es el enlace en donde se encuentran los puertos bloqueados: si el enlace recuperado es el enlace en donde se encuentran los puertos bloqueados, la supresión del envío de un mensaje de recuperación de fallos a otros nodos en la red de anillo; en caso contrario, el envío de un mensaje de recuperación del fallo a otros nodos.

- Después de recibir el mensaje de recuperación del fallo, otros nodos en la red de anillo efectúan el borrado operativo de la tabla de reenvíos local y reinician el auto-aprendizaje. Mientras tanto, los puertos en ambos extremos del enlace recuperado son de nuevo desbloqueados, los puertos normalmente bloqueados se bloquean de nuevo y la red de anillo Ethernet recupera el estado normal.

Forma de realización 2

- La segunda forma de realización difiere de la primera forma de realización en cuanto que: Un nodo en la red de anillo Ethernet no preestablece la información sobre si el puerto al mismo nivel del enlace es un puerto normalmente bloqueado; en su lugar, un mensaje enviado desde un puerto al puerto del mismo nivel del enlace indica si el puerto es, o no, un puerto bloqueado. En esta forma de realización, el nodo realiza la evaluación, en función de la información de identificador del puerto normalmente bloqueado soportado en el paquete CC, si el puerto al mismo nivel del enlace es un puerto normalmente bloqueado y en tal caso, la determinación de si el enlace del puerto es un enlace en donde se encuentra el puerto normalmente bloqueado.

- El procedimiento operativo, en esta forma de realización, es el mismo que el procedimiento operativo representado en la Figura 4 con la excepción de que: en la etapa S401, el paquete CC soporta información de identificador que indica si el puerto es, o no, un puerto normalmente bloqueado.

- La Figura 5 representa un formato de trama de un paquete CC. Según se representa en la Figura 5, el paquete CC soporta un campo de indicadores. El formato estándar del campo de indicadores se representa en la Figura 6. El campo de indicadores contiene varios bits reservados y es adecuado para utilizar uno de los bits para indicar si el puerto que envía el paquete CC es, o no, un puerto normalmente bloqueado. Por ejemplo, el séptimo bit reservado del campo de indicadores se utiliza para indicar si el puerto que envía el paquete CC es, o no, un puerto normalmente bloqueado. Si el valor del séptimo bit reservado es 1, indica que el puerto es un puerto normalmente bloqueado; si el valor es 0, indica que el puerto es un puerto normal.

- Por ejemplo, cuando el nodo 1, en la Figura 3, envía un paquete CC desde un puerto normalmente bloqueado al nodo 2, el séptimo bit reservado del campo de indicadores, en el paquete CC, se establece en 1, lo que indica que el puerto 301, que envía el paquete CC, es un puerto normalmente bloqueado. Cuando el nodo 1 envía un paquete CC desde un puerto normalmente bloqueado al nodo 6, el séptimo bit (bit 7) del campo de indicadores, en el paquete CC, se establece en 0, lo que indica que el puerto que envía el paquete CC es un puerto normal.

En consecuencia, en la etapa S402, cuando ocurren fallos, el nodo en la red de anillo Ethernet evalúa, en función de la información de identificador en la notificación recibida, si el enlace defectuoso es, o no, el enlace en donde se encuentra el puerto normalmente bloqueado.

5 Por ejemplo, después de recibir un paquete CC enviado por el puerto 301 del nodo 1 desde el puerto 302, el nodo 2 en la Figura 3 comprueba si el valor del bit 7 del campo de indicadores en el paquete CC es 1 y, si el valor del bit 7 del campo de indicadores en el paquete CC es 1, registra el enlace del puerto 301 como el enlace en donde se encuentra el puerto normalmente bloqueado. Después de detectar que el enlace de un puerto está defectuoso, el nodo evalúa, en función de la información anteriormente registrada, si el enlace defectuoso es, o no, el enlace en donde se encuentra el puerto normalmente bloqueado.

10 Además, esta forma de realización se refiere también al procedimiento de procesamiento correspondiente en el caso de recuperación de fallos. Dicho procedimiento de procesamiento es el mismo que el procedimiento de procesamiento en la forma de realización 1 y por ello no se repite en esta descripción.

Forma de realización 3

15 En la primera y segunda formas de realización, cuando ocurren fallos o se recuperan fallos en el enlace en donde se encuentra el puerto normalmente bloqueado los nodos en la red de anillo Ethernet no necesitan borrar operativamente la tabla de reenvíos o reiniciar el auto-aprendizaje. Por lo tanto, no es necesario enviar un mensaje de control que notifique a los otros nodos el borrado operativo de la tabla de reenvíos. En el caso, sin embargo, de que otros nodos no tengan conocimiento del fallo del enlace en donde se encuentra el puerto normalmente bloqueado. En esta forma de realización, cuando el enlace en donde se encuentra el puerto normalmente bloqueado está defectuoso, los nodos en la red en anillo no necesitan borrar operativamente la tabla de reenvíos ni reiniciar el auto-aprendizaje, pero reciben un mensaje de control para tener conocimiento del fallo del enlace en la red en anillo.

20 Según se representa en la Figura 7, el procedimiento operativo en esta forma de realización es el mismo que el procedimiento operativo ilustrado en la Figura 4 con la excepción de que: después de que un nodo detecte un fallo de enlace en un puerto, el mensaje de control enviado a otros nodos soporta un indicador sobre si borrar la tabla de reenvíos o no hacerlo. El indicador se define en función de la información anteriormente registrada. Si el puerto defectuoso es un puerto del enlace en donde se encuentra el puerto normalmente bloqueado, el indicador no indica ningún borrado de la tabla de reenvíos (la primera información de indicación). Si el puerto defectuoso no es un puerto del enlace en donde se encuentra el puerto normalmente bloqueado, el indicador sirve para indicar el borrado operativo de la tabla de reenvíos (la segunda información de indicación).

30 El mensaje de control puede ser un paquete de AIS en el mecanismo OAM de Ethernet o un paquete de APS en el mecanismo de conmutación de protección de Ethernet y se transmite por intermedio de una red VLAN de control. En esta forma de realización, el paquete de AIS se toma a modo de ejemplo.

35 La Figura 8 representa un formato de trama estándar de un paquete AIS aplicado en la red de anillo Ethernet. Según se representa en la Figura 8, el paquete AIS incluye un campo de indicadores. Según se indica en la Figura 9, el bit 8 y el bit 7 se pueden utilizar para indicar el tipo de indicación (IT): los valores de IT son "fallo" y "recuperación". El valor "fallo" indica que el tipo de la información de alarma es una ocurrencia de fallo y el valor "recuperación" indica que el tipo de la información de alarma es la recuperación de fallos. Además, el bit 6 se puede utilizar como una indicación de regeneración secuencial en tiempo real, Flush (FI). Si el valor de FI es 1, ello indica que es necesario borrar operativamente la tabla de reenvíos; si el valor de FI es 0, indica que es innecesario borrar operativamente la tabla de reenvíos.

40 Por ejemplo, el nodo en la red de anillo Ethernet, que se representa en la Figura 3, preestablece la información que indica que el puerto 301 es un puerto normalmente bloqueado o conoce dicha información en función de la información de identificador transmitida en el paquete CC anteriormente enviado y registra la información. Cuando el nodo 2 en la Figura 3 detecta que el enlace en donde se encuentra el puerto 301 está defectuoso, el nodo 2 conoce que el enlace defectuoso es el enlace en donde se encuentra el puerto normalmente bloqueado. Por lo tanto, cuando se envía la información de alarma, el nodo 2 establece el IT en "fallo" y establece en FI en 0.

Después de recibir el paquete de alarma, otros nodos comprueban el FI y si el valor de FI es 1, proceden a borrar operativamente la tabla de reenvíos para facilitar, más tarde, la reiniciación del auto-aprendizaje o si el valor de FI es 0, evitar el borrado de la tabla de reenvíos.

50 En esta forma de realización, cuando el nodo en la red en anillo detecta la recuperación de fallos, el método comprende, además, lo siguiente:

55 si el enlace de recuperación de fallos es el enlace en donde se encuentra el puerto normalmente bloqueado, el nodo que detecta la recuperación de fallos envía información de alarma a otros nodos en la red en anillo, en donde la información de alarma es un mensaje de recuperación de fallos. En esta forma de realización, el IT = recuperación del campo de identificadores, en el paquete AIS, se puede utilizar para indicar el paquete AIS como mensaje de recuperación de fallos y el FI se pone a 0;

si el enlace de recuperación de fallos no es el enlace en donde se encuentra el puerto normalmente bloqueado, el nodo que detecta la recuperación de fallos envía la información de alarma a otros nodos en la red en anillo, en donde la información de alarma es un mensaje de recuperación de fallos. En esta forma de realización, el IT = recuperación, en el paquete AIS, se puede utilizar para indicar el paquete AIS como mensaje de recuperación de fallos y el FI se pone a 1;

- 5 después de recibir el mensaje de recuperación de fallos, otros nodos en la red en anillo deciden si proceder a borrar, o no, la tabla de reenvíos local y reiniciar el auto-aprendizaje en función del FI en el mensaje de recuperación de fallos. Mientras tanto, los puertos en ambos extremos del enlace de recuperación de fallos son de nuevo desbloqueados, el puerto normalmente bloqueado se bloquea de nuevo y la red de anillo Ethernet recupera el estado normal.

- 10 Basado en el mismo concepto de diseño que el método de ERP anterior, se da a conocer aquí un aparato de ERP. Puesto que el aparato y el método están basados en el mismo concepto de diseño de la invención, las formas de realización del aparato presentan numerosas características técnicas idénticas o equivalentes y dichas características técnicas se describen solamente sin complicación innecesaria.

Forma de realización 4

- 15 La Figura 10 representa una estructura de un aparato de ERP dado a conocer en la cuarta forma de realización de la presente invención. El aparato está situado en el nodo de la red en anillo. Según se representa en la Figura 10, el aparato comprende:

- 20 un módulo de detección de estado del enlace 101, adaptado para: recibir una notificación (por ejemplo, un paquete CC mencionado aquí en la forma de realización del método) de los nodos adyacentes, para evaluar el estado del enlace en función de la notificación y para enviar información de fallo de enlace o información de recuperación de fallos de enlace a un módulo de evaluación 102 después de detectar un fallo de enlace o una recuperación de fallos del enlace en el enlace entre un nodo local y un nodo adyacente;

- 25 un módulo de evaluación 102, adaptado para: evaluar, en función de la información a cerca del puerto normalmente bloqueado memorizada en un módulo de almacenamiento de información 103, si el enlace defectuoso o el enlace de recuperación de fallos es un enlace en donde se encuentra el puerto normalmente bloqueado y para dar instrucciones a un módulo generador de mensajes de control 104 para enviar un mensaje de control a otros nodos si el enlace defectuoso o el enlace de recuperación de fallos no es un enlace en donde se encuentra el puerto normalmente bloqueado y en donde el mensaje de control se utiliza para notificar a otros nodos si borrar operativamente, o no, la tabla de reenvíos;

- 30 un módulo de almacenamiento de información 103, adaptado para almacenar información sobre el puerto normalmente bloqueado en una red de anillo Ethernet y

un módulo generador de mensajes de control 104, adaptado para generar y enviar un mensaje de control a otros nodos adyacentes, en donde el mensaje de control puede ser un paquete AIS o un paquete APS.

- 35 El proceso de utilizar el aparato, en esta forma de realización, para realizar la protección ERP es el mismo que el proceso descrito en la forma de realización del método anterior de la presente invención y por ello, no se repite en esta descripción.

Forma de realización 5

La Figura 11 representa una estructura de un aparato de ERP dado a conocer en la quinta forma de realización de la presente invención. Según se representa en la Figura 11, esta forma de realización difiere de la cuarta forma de realización en que: el aparato dado a conocer en esta forma de realización comprende, además:

- 40 un módulo de extracción de información de identificador 105, adaptado para: extraer información de identificador a partir de la notificación recibida por el módulo de detección de estado del enlace 101, en donde la información de identificador indica si el puerto, que envía el mensaje de control, es un puerto normalmente bloqueado y para enviar la información de identificador a un módulo de evaluación 102 y

- 45 el módulo de evaluación 102, adaptado para: evaluar, en función de la información de identificador memorizada en el módulo de almacenamiento de información 103 y la información de identificador extraída por el módulo de extracción de información de identificador 105, si el enlace defectuoso o el enlace de recuperación de fallos es un enlace en donde se encuentra el puerto normalmente bloqueado y para dar instrucciones a un módulo generador de mensajes de control 104 para enviar un mensaje de control a otros nodos, si el enlace defectuoso o el enlace de recuperación de fallos no es un enlace en donde se encuentra el puerto normalmente bloqueado.

50 **Forma de realización 6**

La Figura 12 representa una estructura de un aparato de ERP dado a conocer en la sexta forma de realización de la presente invención. Según se representa en la Figura 12, esta forma de realización difiere de la quinta forma de realización en que: esta forma de realización comprende un módulo de adición de identificadores 106 adaptado para conocer, desde el módulo de evaluación 102, si el enlace defectuoso o el enlace de recuperación de fallos es el enlace

en donde se encuentra el puerto normalmente bloqueado y para añadir, en función del resultado de la evaluación del módulo de evaluación 102, un identificador en el mensaje de control generado por el módulo generador de mensajes de control 104, en donde el identificador indica si borrar operativamente, o no, la tabla de reenvíos.

5 Más concretamente, si el enlace defectuoso o el enlace de recuperación de fallos es el enlace en donde se encuentra el puerto normalmente bloqueado, el módulo de adición de identificadores 106 añade un identificador de no borrar operativamente la tabla de reenvíos (la primera información de indicación) en el mensaje de control. Si el enlace defectuoso o el enlace de recuperación de fallos no es el enlace en donde se encuentra el puerto normalmente bloqueado, el módulo de adición de identificadores 106 añade un identificador de borrado operativo de la tabla de reenvíos (la segunda información de indicación) al mensaje de control.

10 Por intermedio del método y aparato dados a conocer en las formas de realización de la presente invención, evaluando si el enlace defectuoso o el enlace de recuperación de fallos es un enlace donde se encuentra el puerto normalmente bloqueado, se toma una decisión sobre si dar instrucciones a otros nodos en la red de anillo Ethernet para borrar operativamente la tabla de reenvíos o no hacerlo. Por lo tanto, la dificultad para los nodos en la red en anillo para borrar operativamente la tabla de reenvíos y reiniciar el auto-aprendizaje después de que ocurra cualquier fallo de enlace o se recupere cualquier fallo de enlace en la técnica anterior queda así evitada. El tráfico de radiodifusión generado por un borrado innecesario de la tabla de reenvíos y el auto-aprendizaje se reduce de forma efectiva y la tasa de utilización del ancho de banda en la red de anillo Ethernet se mejora considerablemente.

20 Aunque la invención ha sido descrita a través de varias formas de realización ejemplo, la invención no está limitada a dichas formas de realización. Es evidente para los expertos en esta materia que se pueden hacer varias modificaciones y variaciones a la invención sin desviarse, por ello, del alcance de protección de la invención. La invención está destinada a cubrir las modificaciones y variaciones a condición de que caigan dentro del alcance de protección definido por las siguientes reivindicaciones o sus equivalentes.

REIVINDICACIONES

1. Un método de Protección de Anillo Ethernet, ERP, que comprende:
cuando un enlace en una red Ethernet en anillo está defectuoso, la evaluación de saber si el enlace defectuoso es un enlace en donde se encuentra un puerto normalmente bloqueado (702);
- 5 el envío de un mensaje de control que transmite la primera información de indicación de si el enlace defectuoso es el enlace en donde se encuentra el puerto normalmente bloqueado (703) y
evitar, por un nodo del anillo, el borrado de una tabla de reenvíos después de recibir el mensaje de control que transmite la primera información de indicación.
2. El método según la reivindicación 1 que comprende, además:
- 10 el envío del mensaje de control que transmite la segunda información de indicación si el enlace defectuoso no es el enlace en donde se encuentra el puerto normalmente bloqueado y
el borrado, por el nodo del anillo, de la tabla de reenvíos después de recibir el mensaje de control que transmite la segunda información de indicación.
- 15 3. El método según la reivindicación 1 o 2, en donde la evaluación de si el enlace defectuoso es el enlace en donde se encuentra el puerto normalmente bloqueado, comprende:
la evaluación, por demanda de información sobre el puerto normalmente bloqueado preestablecido en un nodo local, de si el enlace defectuoso es el enlace en donde se encuentra el puerto normalmente bloqueado.
4. El método según la reivindicación 1 o 2, en donde la evaluación de si el enlace defectuoso es el enlace en donde se encuentra el puerto normalmente bloqueado, comprende:
- 20 la evaluación, en función de la información del identificador transmitida en una notificación recibida, de si el enlace defectuoso es el enlace en donde se encuentra el puerto normalmente bloqueado y en donde, la información de identificador indica si un puerto que envía la notificación es el puerto normalmente bloqueado.
5. El método según la reivindicación 1 o 2 que comprende, además:
cuando la recuperación del fallo se produce en el enlace, evaluar si el enlace recuperado de los fallos es el enlace en donde se encuentra el puerto normalmente bloqueado;
- 25 el envío del mensaje de control que transmite la primera información de indicación si el enlace recuperado de los fallos es el enlace en donde se encuentra el puerto normalmente bloqueado.
6. El método según la reivindicación 5 que comprende, además:
el envío, por un nodo que detecta la recuperación de fallos, del mensaje de control que transmite la segunda información de indicación a otros nodos, en un anillo, si el enlace recuperado de los fallos no es el enlace en donde se encuentra el puerto normalmente bloqueado.
- 30 7. Un aparato de protección de anillo Ethernet, ERP, que comprende:
un módulo de almacenamiento de información (103), adaptado para almacenar información sobre un puerto normalmente bloqueado en una red de anillo Ethernet;
- 35 un módulo generador de mensajes de control (104), adaptado para generar y enviar un mensaje de control a otros nodos adyacentes, en donde el mensaje de control notifica a otros nodos si es necesario borrar una tabla de reenvíos;
un módulo de detección de estado del enlace (101), adaptado para: detectar un estado del enlace por intermedio de una notificación recibida y para enviar la información de fallo del enlace a un módulo de evaluación (102) después de detectar un fallo en el enlace;
- 40 el módulo de evaluación (102), adaptado para: evaluar, en función de la información sobre el puerto normalmente bloqueado memorizada en el módulo de almacenamiento de información, si un enlace defectuoso es un enlace en donde se encuentra el puerto normalmente bloqueado y para dar instrucciones al módulo generador de mensajes de control para enviar el mensaje de control a los demás nodos si el enlace defectuoso es el enlace en donde se encuentra el puerto normalmente bloqueado y
- 45 un módulo de edición de identificador (106), adaptado para añadir, en función de un resultado de evaluación del módulo de evaluación, la primera información de indicación en el mensaje de control generado por el módulo generador de mensajes de control, en donde la primera información de indicación indica a los demás nodos no borrar la tabla de reenvíos.

8. El aparato según la reivindicación 7 que comprende, además:

5 un módulo de extracción de información de identificador (105) adaptado para: extraer información de identificador desde la notificación recibida por el módulo de detección de estado del enlace, en donde la información de identificador indica si un puerto que envía el mensaje de control es, o no, el puerto normalmente bloqueado y para enviar la información de identificador al módulo de almacenamiento de información para su almacenamiento.

9. Un aparato de Protección de Anillo Ethernet, ERP, que comprende:

10 un módulo de almacenamiento de información (103), adaptado para almacenar información respecto a un puerto normalmente bloqueado en una red de anillo Ethernet;

un módulo generador de mensajes de control (104), adaptado para generar y enviar un mensaje de control a otros nodos adyacentes, en donde el mensaje de control notifica a otros nodos si borrar, o no, una tabla de reenvíos;

un módulo de detección de estado del enlace (101), adaptado para: detectar un estado del enlace por intermedio de una notificación recibida y para enviar una información de recuperación de fallo del enlace a un módulo de evaluación (102) después de detectar una recuperación de fallo del enlace;

15 el módulo de evaluación (102), adaptado para: evaluar, en función de la información sobre el puerto normalmente bloqueado memorizada en el módulo de almacenamiento de información, si un enlace recuperado de fallos es un enlace en donde se encuentra el puerto normalmente bloqueado y para dar instrucciones al módulo generador de mensajes de control para enviar el mensaje de control a los demás nodos si el enlace recuperado de los fallos es el enlace en donde se encuentra el puerto normalmente bloqueado y

20 un módulo de adición de identificador (106) adaptado para añadir, en función de un resultado de evaluación del módulo de evaluación, la primera información de indicación en el mensaje de control generado por el módulo generador de mensajes de control, en donde la primera información de indicación indica a los demás nodos no borrar la tabla de reenvíos.

10. El aparato según la reivindicación 9 que comprende, además:

25 un módulo de extracción de información de identificador (105) adaptado para: extraer información de identificador desde la notificación recibida por el módulo de detección de estado del enlace, en donde la información de identificador indica si un puerto que envía el mensaje de control es, o no, el puerto normalmente bloqueado y para enviar la información de identificador al módulo de almacenamiento de información para su almacenamiento.

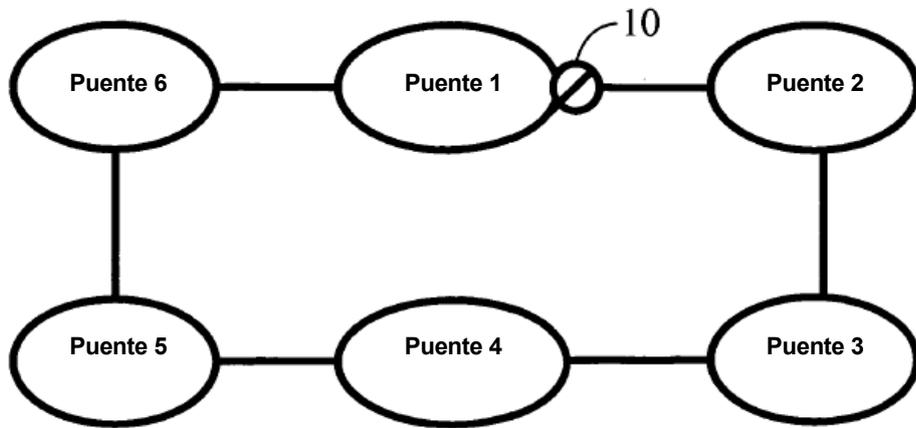


Figura 1

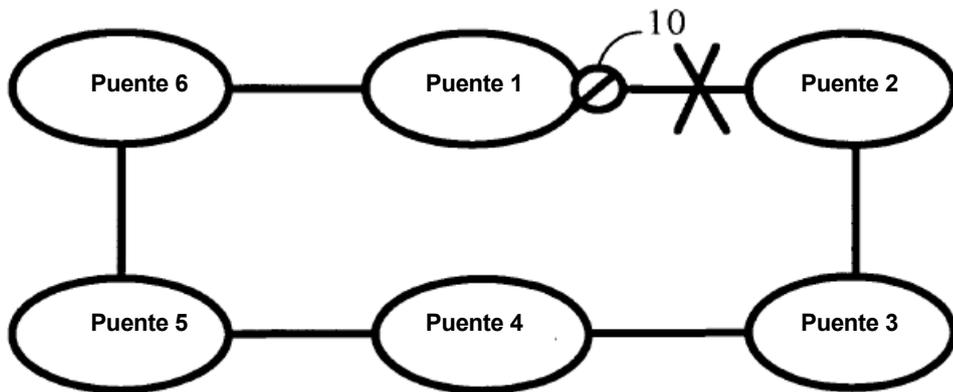


Figura 2

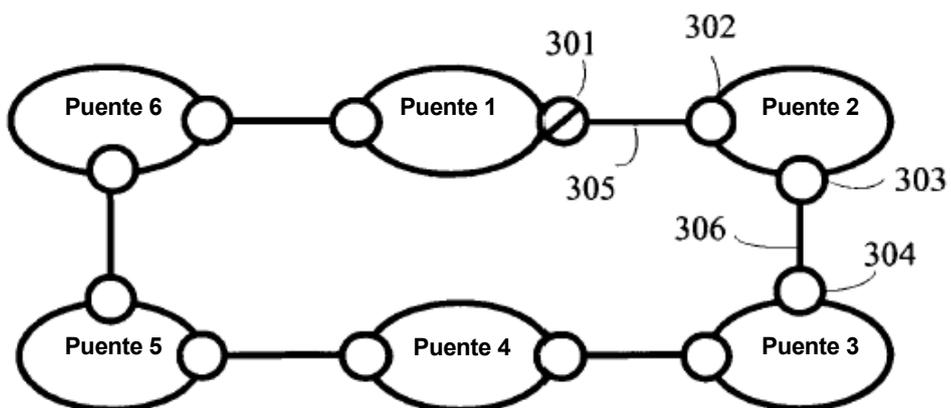


Figura 3

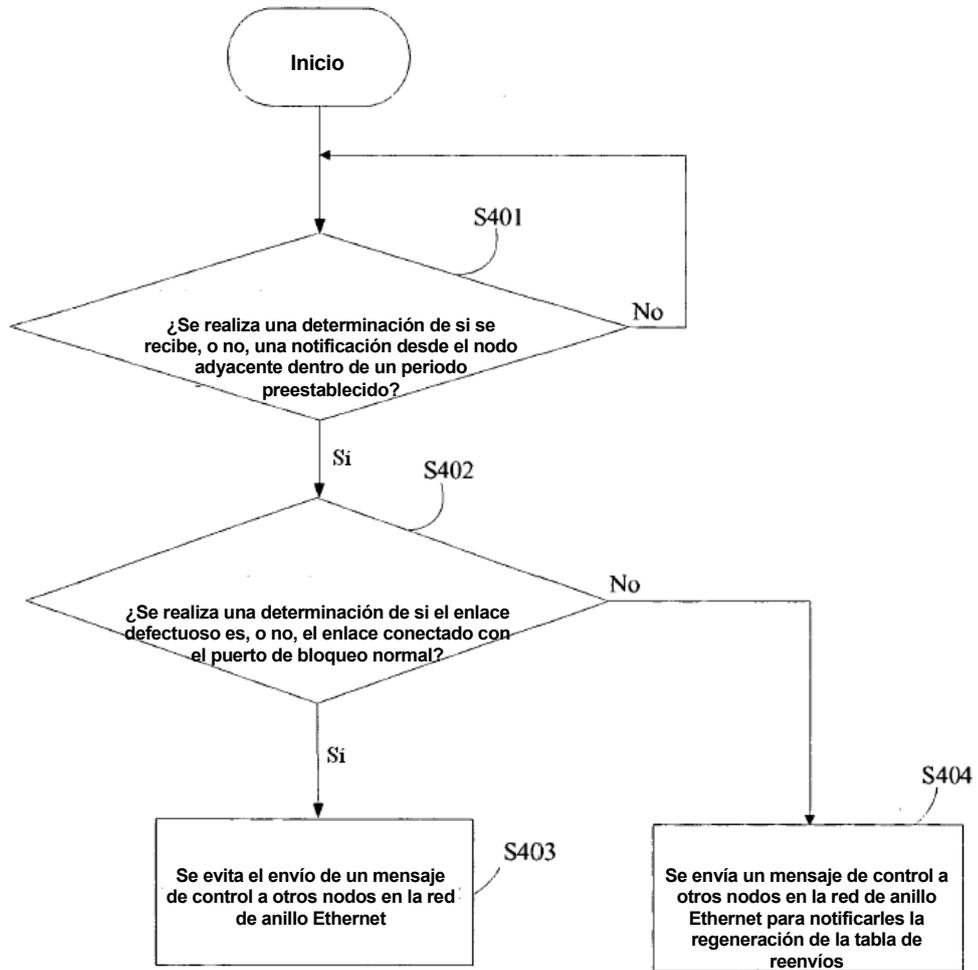


Figura 4

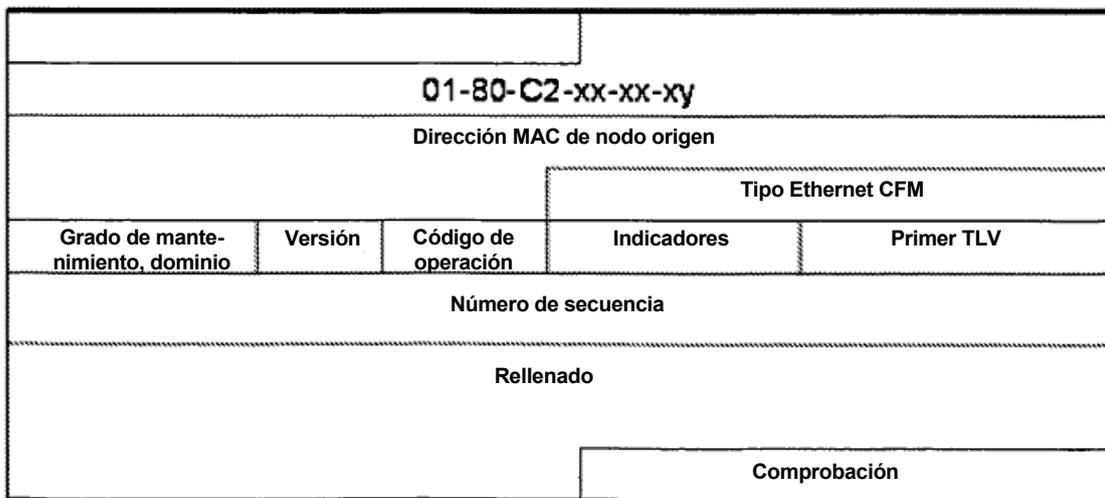


Figura 5

MSB							LSB
8	7	6	5	4	3	2	1
RDI	Reservado (0)				Periodo		

Figura 6

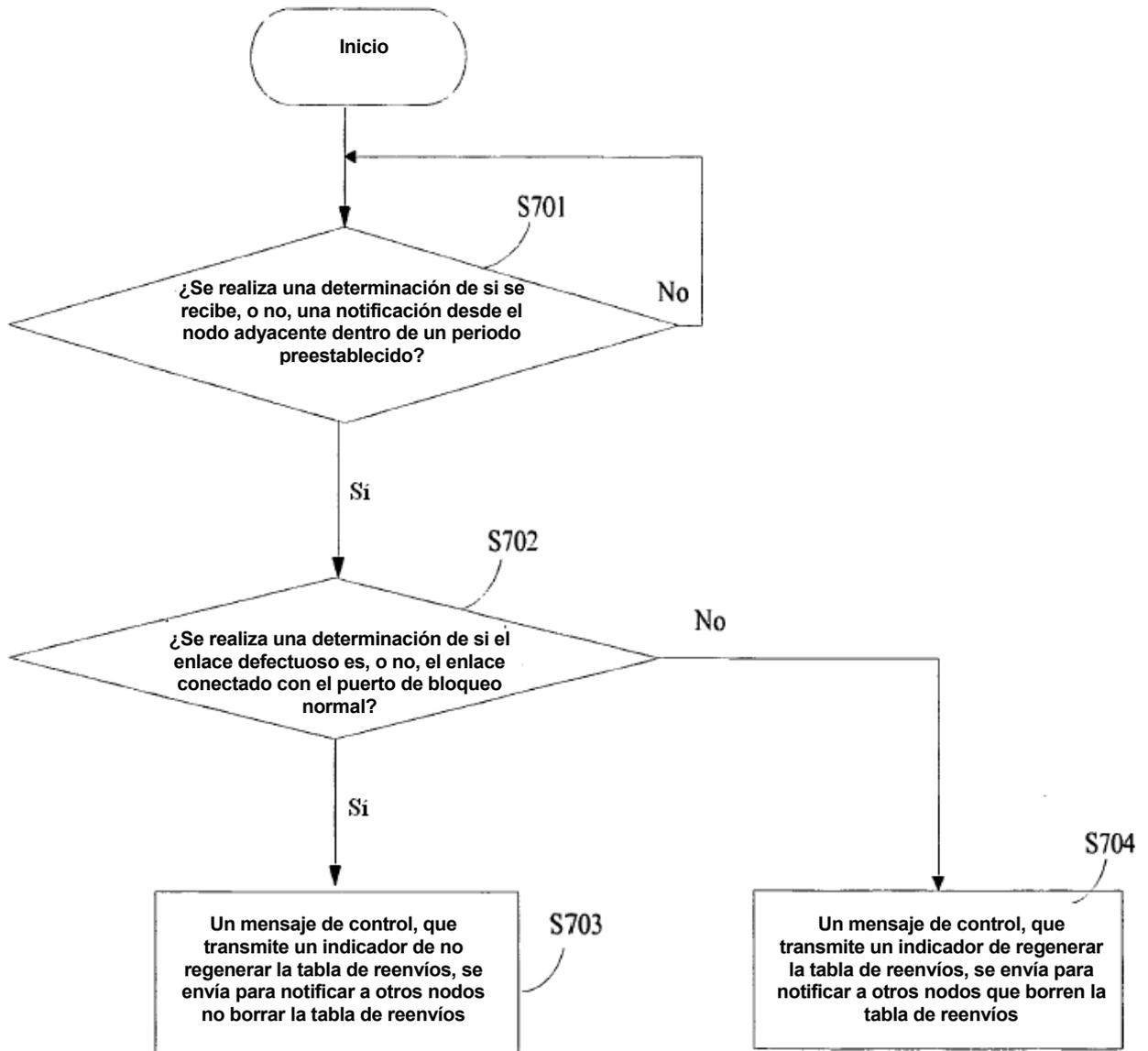


Figura 7

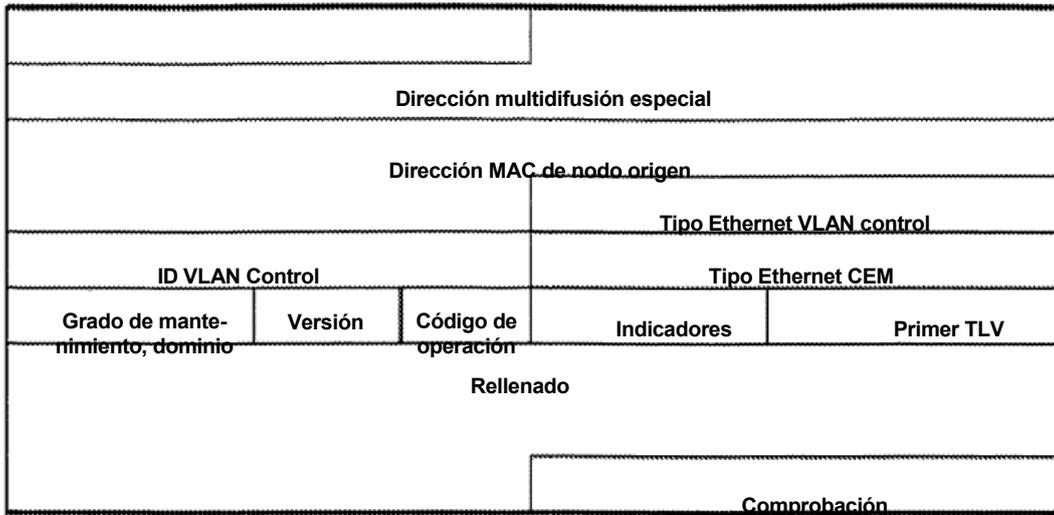


Figura 8

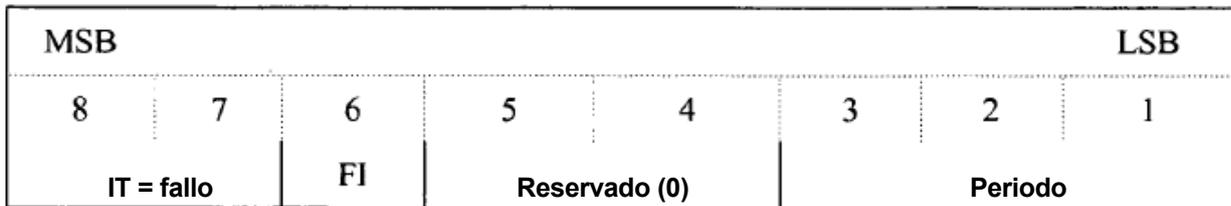


Figura 9

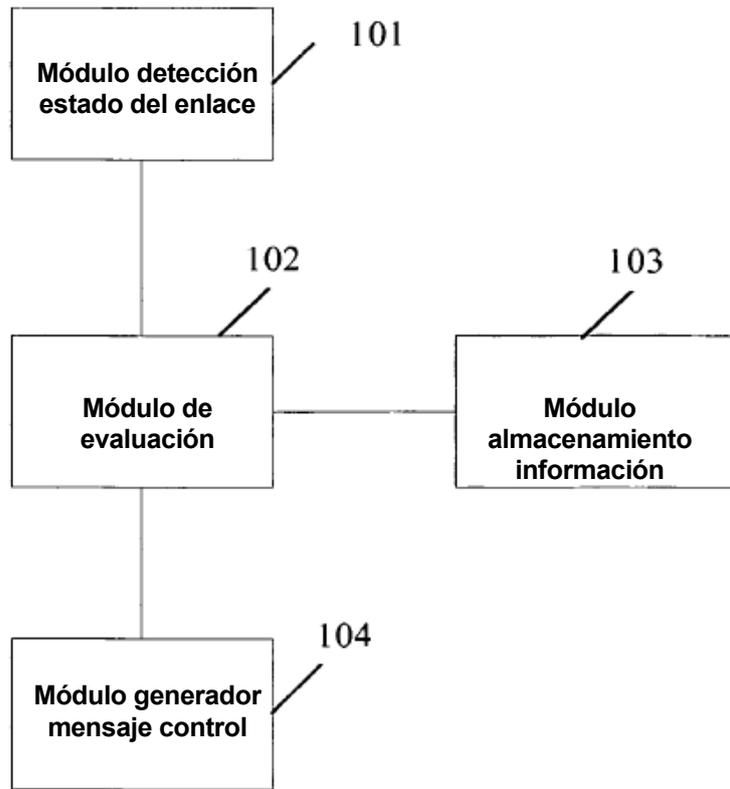


Figura 10

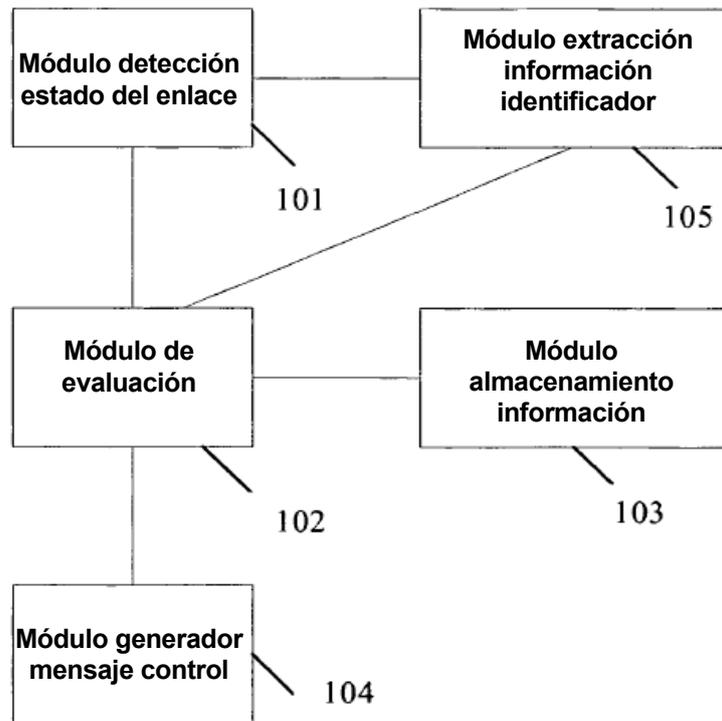


Figura 11

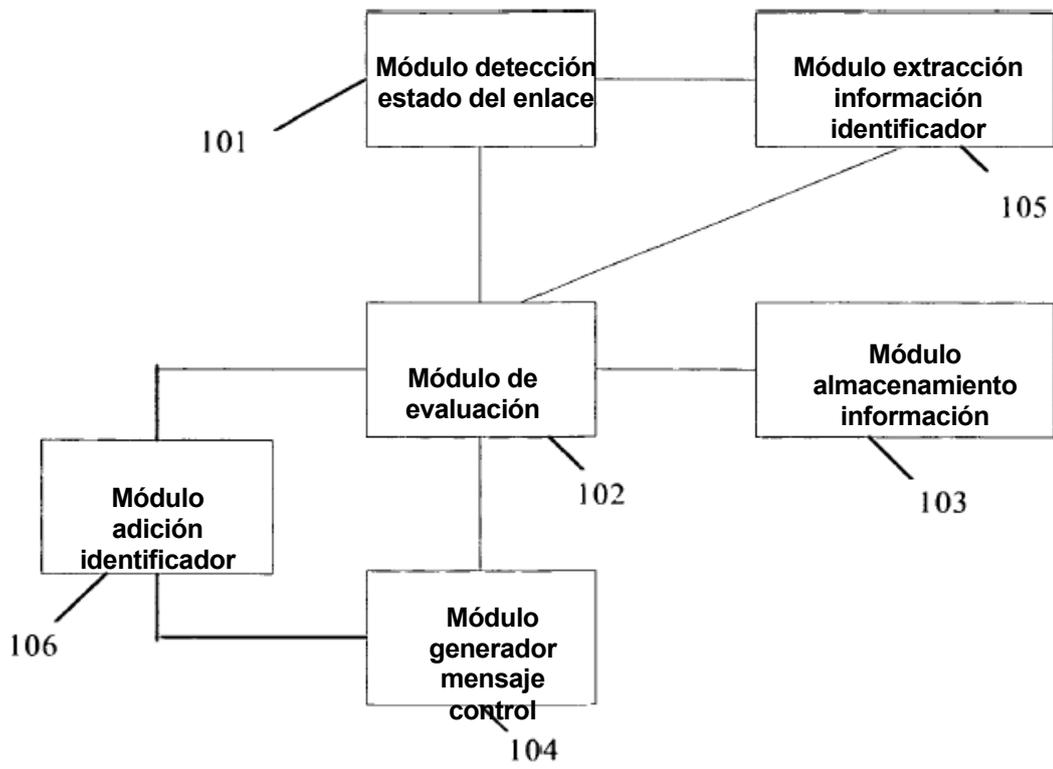


Figura 12