(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 266 445**

(51) Int. Cl.:
H04L 12/42 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **02701519 .7**
(86) Fecha de presentación : **03.03.2002**
(87) Número de publicación de la solicitud: **1378096**
(87) Fecha de publicación de la solicitud: **07.01.2004**

(54) Título: **Protección selectiva para topologías de anillo.**

(30) Prioridad: **02.04.2001 US 281232 P**
03.10.2001 US 969839

(45) Fecha de publicación de la mención BOPI:
01.03.2007

(45) Fecha de la publicación del folleto de la patente:
01.03.2007

(73) Titular/es: **Corrigent Systems Ltd.**
126b Yigal Alon Street
Tel Aviv 67443, IL

(72) Inventor/es: **Bruckman, Leon**

(74) Agente: **Curell Suñol, Marcelino**

DESCRIPCIÓN

Protección selectiva para topologías de anillo.

Campo de la invención

La presente invención se refiere en general a sistemas y protocolos de comunicación de redes y específicamente a métodos de protección contra fallos en redes de conmutación de paquetes.

Antecedentes de la invención

Las topologías de anillo de redes están ganando popularidad, particularmente en las redes de protocolo de Internet (IP). Estas redes permiten a las empresas de explotación de telefonía ofrecer anchos de banda grandes a los usuarios de manera rentable, dado que cada nodo en la red necesita únicamente dos interfaces, en lugar de tener que mantener una interfaz independiente para cada uno de los nodos en una red poligonal. Las redes en anillo se prestan asimismo a reencaminarse rápidamente en el caso de fallos en la red, dado que dos rutas alternativas, en el sentido horario y en el sentido antihorario, están generalmente disponibles para conectar dos nodos cualesquiera en el anillo.

Un inconveniente de las configuraciones de anillo tradicionales, como SONET/SDH, es que una de las direcciones se designa como el anillo activo, mientras que la otra dirección permanece en espera para la protección contra fallos cuando sea necesario. En otras palabras, en cualquier momento dado, todos los nodos en el anillo transmiten y reciben datos solamente en la dirección activa. Por tanto, generalmente la mitad del ancho de banda disponible en estos anillos se reserva para la protección contra fallos y no se explota en condiciones de funcionamiento normales.

Algunos protocolos bidireccionales desarrollados recientemente proporcionan una utilización de ancho de banda más eficaz permitiendo datos que han de transferirse entre un par de nodos cualesquiera en cualquier dirección alrededor del anillo, mientras que se mantiene la protección rápida contra los fallos. Se hace referencia a las dos direcciones de tráfico opuestas comúnmente como un anillo interior y un anillo exterior. Se apreciará, sin embargo, que en el contexto de la presente solicitud de patente y en las reivindicaciones, los términos "interior" y "exterior" así como "sentido horario" y "sentido antihorario" se emplean arbitrariamente para distinguir entre las dos direcciones opuestas del flujo de paquetes en una red en anillo. Estos términos se seleccionan únicamente con fines explicativos y no necesariamente están relacionados con las características físicas de la red.

El protocolo bidireccional principal para anillos de paquete de alta velocidad es el protocolo RPR (anillos de recuperación de paquetes) que está en el proceso de definirse como estándar IEEE 802.17. El encaminamiento de capas de red mediante RPR se describe, por ejemplo, por Jogalekar *et al*. en "IP over Resilient Packet Rings" (Internet Draft-draft-joglekar-iporpr-00) y por Herrera *et al*. en "A framework for IP over Packet Transport Rings" (Internet Draftdraft-ietf-ipoptr-framework-00). Una solución propuesta para el control de acceso al medio (MAC, Media Access Control, capa 2 de protocolo) en redes en anillo bidireccional es el protocolo SRP (protocolo de reutilización espacial) que se describe por Tsiang *et al*. en Request for Comments (RFC) 2892 of the Internet Engineering Task Force (IETF). Están disponibles en www.ietf.org.

Al usar protocolos como estos, cada nodo en red en anillo puede comunicarse directamente con todos los otros nodos a través del anillo interior o el exterior, utilizando las direcciones del control del acceso al medio (MAC) apropiado de los nodos. Cada paquete enviado a través de uno de los anillos lleva un encabezamiento indicando su nodo de destino. El nodo de destino reconoce su dirección en el encabezamiento y extrae el paquete del anillo. Todos los otros nodos hacen pasar el paquete avanzando de manera transparente alrededor del anillo.

Cuando se produce un fallo en un enlace en una red en anillo bidireccional, los paquetes destinados a atravesar el enlace averiado en uno de los anillos deben reencaminarse rápidamente para alcanzar su destino mediante el otro anillo. Este reencaminamiento se conoce en la técnica como "protección". Para este fin se emplean dos esquemas: la envoltura y direccionamiento. La envoltura, que es el método utilizado en anillos SRP, se logra conectando en bucle la corriente de datos en los nodos que están adyacentes al enlace averiado. Por tanto, los paquetes que alcanzan el enlace averiado en el anillo interior se conectan en bucle para desplazarse a su destino mediante el anillo exterior, y viceversa. De esta manera, la protección se realiza simplemente mediante los nodos que son adyacentes al enlace averiado. En la protección basada en el direccionamiento, por otro lado, se informa a cada uno de los nodos sobre el enlace averiado. Entonces cada nodo direcciona todo su tráfico de manera correspondiente sobre el anillo que alcanza el destino deseado sin pasar por el enlace averiado.

El documento WO-00/74318-A1 da a conocer un método para la protección de rutas que conmutan en redes de anillos provistas de un mecanismo de envoltura. La envoltura es ventajosa en cuanto a su velocidad y simplicidad, dado que solamente los nodos que detectan el fallo necesitan realizar la función de protección. Incluso no es necesario informar a los otros nodos de que se ha producido un fallo. Una desventaja de la envoltura es que los paquetes protegidos deben desplazarse mucho más lejos para alcanzar sus destinos. La disponibilidad de los recursos de red se reduce asimismo dado que los paquetes protegidos se desplazan a través de todos los segmentos de la red al menos una vez, y a menudo dos veces. Además, cuando se repara el fallo y se finaliza la envoltura, algunos paquetes tienden a alcanzar sus destinos de manera desordenada dado que no pueden desplazarse de nuevo por su trayecto original que es mucho más corto que el trayecto de envoltura utilizado por los paquetes anteriores. Como resultado, el proceso de envoltura es problemático como mecanismo de protección para tráfico en tiempo real tal como voz o vídeo que es sensible a la fluctuación y al desorden en los paquetes.

El tráfico en tiempo real por tanto se maneja mejor mediante el direccionamiento, a pesar del aumento en la complejidad de este método. Dado que el direccionamiento requiere que todos los nodos estén informados e implementen la protección contra fallos, su comienzo es intrínsecamente más lento que la envoltura. Los nodos deben enlazarse mediante un protocolo de protección adecuado para que puedan informarse unos a otros de las condiciones de fallo. Un paquete de notificación de fallo enviado por otro nodo mediante el protocolo debe atravesar entonces todo el anillo para actualizar todos los demás nodos. Los paquetes que se transmiten entre el tiempo en el que se produce

el fallo y el inicio del direccionamiento por lo general se pierden. En algunas aplicaciones de datos la pérdida de incluso un paquete puede llevar a que se rechace una trama entera o un bloque de datos. Por tanto, las pérdidas de paquetes debido a la protección deberían mantenerse a un mínimo.

Por tanto, es evidente que mientras que la envoltura es generalmente el mejor esquema de protección para aplicaciones de datos en bloque, el direccionamiento es mejor para el tráfico en tiempo real. Dado que las redes de paquetes modernas soportan normalmente ambos tipos de tráfico, ni la envoltura, ni el direccionamiento, proporcionan una solución óptima. En el SRP, tal como se describe en el RFC 2892 (sección 3.4) mencionado anteriormente, los dos esquemas se combinan utilizando en primer lugar la envoltura y después el direccionamiento del tráfico después de un fallo. Sin embargo en este caso, el tráfico en tiempo real se trastorna dos veces: en primer lugar cuando se produce el fallo y comienza la envoltura, y después cuando tiene lugar el direccionamiento dado que el trayecto dirigido es más corto que el trayecto de envoltura. Por tanto, todavía existe la necesidad de una solución para la protección que satisfaga las necesidades de los datos en bloque y del tráfico en tiempo real.

Sumario de la invención

Un objetivo de la presente invención consiste en proporcionar métodos de protección mejorados así como dispositivos que implementan tales métodos para usar en redes de anillo.

Otro objetivo de algunos aspectos de la presente invención consiste en proporcionar métodos de protección que puedan optimizarse para diferentes tipos de tráfico simultáneamente.

En formas de realización preferidas de la presente invención, se dispone una red en anillo bidireccional de manera que al producirse un fallo en uno de los enlaces de la red, se envuelven determinadas clases de paquetes mientras que otras no. Preferentemente, se envuelven los servicios de datos que no son sensibles a retardos y que pueden tratar el desorden de los paquetes para minimizar el número de paquetes perdidos debido al fallo, mientras que los servicios en tiempo real, que son sensibles a la fluctuación y al desorden no se envuelven. Más preferentemente, el direccionamiento se aplica a los servicios en tiempo real, mientras que los servicios de datos que son sensibles al retardo se envuelven. Alternativamente, tras el periodo de envoltura inicial, durante el cual se establece el direccionamiento, los servicios de datos también pueden direccionarse. Además, alternativamente, pueden envolverse determinados servicios y, de manera opcional, direccionarse después, mientras que otros servicios simplemente se rechazan para garantizar que, en condiciones de fallo, hay suficiente ancho de banda disponible en la red para el tráfico protegido de alta prioridad.

En algunas formas de realización preferidas de la presente invención, esta envoltura selectiva se implementa añadiendo un indicador a cada paquete, que indica si el paquete ha de envolverse o no. Después de que un nodo ha detectado un fallo en un enlace adyacente, comprueba el indicador en cada paquete que recibe para decidir si lo envuelve o no, pasa o rechaza el paquete. El nodo de envío determina si una determinada clase de paquetes debería tener fijado el indicador de envoltura o volver a fijarlo en función del tipo de servicio implicado (por ejemplo, datos o tiempo real). De manera alternativa o adicional, fijar el indicador puede depender de la identidad del usuario que envía el paquete o de otros factores configurados por un operario del sistema. Alternativamente además, en otras formas de realización no se usa el indicador de envoltura y en su lugar, los nodos deciden qué paquetes envolver basándose en otra información transportada en los paquetes, tal como la dirección de origen o destino o el tipo de protocolo.

El objetivo de la presente invención proporciona una solución flexible, simple al problema de la protección de redes de anillo de tráfico mixto. Tal como se mencionó anteriormente, ni la envoltura ni el direccionamiento, ni la envoltura seguida del direccionamiento previstos en el SRP, proporcionan una solución óptima para todos los tipos de tráfico en redes de este tipo.

Por tanto se proporciona, según la presente invención, un método para la protección contra fallos en una red en anillo bidireccional en la que el tráfico de paquetes se transmite simultáneamente tanto en el sentido horario, como en el sentido antihorario alrededor de la red, caracterizado porque comprende:

transmitir unos primer y segundo flujos de paquetes alrededor de la red en anillo bidireccional mientras que define el primer flujo como un flujo de envoltura, y el segundo flujo como un flujo de no envoltura; y

al detectar un nodo en la red que un segmento de la red próxima al nodo se ha averiado, envolver los paquetes en el primer flujo en el nodo entre los sentidos horario y antihorario para evitar el segmento averiado, mientras que los paquetes en el segundo flujo no se envuelven.

Los paquetes en el segundo flujo que alcanzan el nodo pueden pasar o rechazarse.

El método puede incluir además direccionar los paquetes en el segundo flujo en uno de los sentidos horario y antihorario para alcanzar un destino del segundo flujo mientras que se evita el segmento averiado. Preferentemente, el direccionamiento de paquetes en el segundo flujo comprende enviar un mensaje de indicación de fallo desde el nodo que detecta los segmentos averiados a un nodo de origen del segundo flujo, e iniciar el direccionamiento de los paquetes en el segundo flujo respondiendo al mensaje. Más preferentemente, el método comprende, cuando se inicia el direccionamiento de los paquetes en el segundo flujo, direccionar también los paquetes en el primer flujo e interrumpir la envoltura de los paquetes.

Además, adicionalmente, el método puede incluir enviar un mensaje de indicación de fallo desde el nodo que detecta los segmentos averiados a otros nodos en la red y, después de que los otros nodos hayan recibido el mensaje, direccionar los paquetes en el primer flujo en uno de los sentidos horario y antihorario para alcanzar un destino del primer flujo mientras evita el segmento averiado, e interrumpir la envoltura de los paquetes. Normalmente los paquetes en el segundo flujo se rechazan mientras continúa el fallo.

Preferentemente, la transmisión de flujos primero y segundo incluye fijar un indicador de envoltura en los paquetes en el primer flujo, mientras que se vuelve a fijar el indicador de envoltura en los paquetes en el segundo flujo, y la envoltura de los paquetes incluye determinar los paquetes que han de envolverse en respuesta al indicador de envoltura.

En una forma de realización preferida, la transmi-

sión del segundo flujo incluye proporcionar un servicio en tiempo real, mientras que la transmisión del primer flujo incluye proporcionar un servicio de transmisión de datos que es sustancialmente más tolerante a las variaciones de retardo y al desorden en la entrega de paquetes que el servicio en tiempo real. Normalmente, el servicio en tiempo real incluye al menos un servicio de voz en paquetes y un servicio de vídeo en paquetes.

También se proporciona, según la presente invención, un aparato de comunicación que incluye:

un medio de comunicación, y

una pluralidad de nodos de comunicación acoplados entre sí mediante el medio de comunicación para formar una red en anillo en la que se configuran los nodos para transmitir el tráfico a los otros nodos tanto en el sentido horario como en el sentido antihorario, caracterizado porque el tráfico incluye un primer flujo de paquetes definidos como un flujo de envoltura y un segundo flujo de paquetes definido como flujo de no envoltura,

los nodos están adaptados de tal manera que al detectar un nodo dado entre los nodos en la red que un segmento de la red próxima al nodo dado se ha averiado, los paquetes en el primer flujo se envuelven en el nodo dado entre los sentidos horario y antihorario para evitar el segmento averiado, mientras que los paquetes en el segundo flujo no se envuelven.

Se proporciona además, según una forma de realización preferida de la presente invención, un dispositivo de comunicación, para funcionar como un nodo en una red en anillo por la cual se transmite el tráfico en los sentidos horario y antihorario, caracterizado porque comprende:

un bloque de procesamiento de tráfico, adaptado para preparar paquetes de datos de salida para transmitirlos por la red en anillo, de tal manera que los paquetes pertenecen o bien a un primer flujo de paquetes definido como un flujo de envoltura, o bien a un segundo flujo de paquetes definido como un flujo de no envoltura, y

un bloque de control de acceso a los medios (MAC) de interconexión al bloque de procesamiento de tráfico y adaptado para acoplarse a la red para transmitir los paquetes de datos de salida y recibir los paquetes entrantes por la red en anillo tanto en el sentido horario como en el antihorario, y adaptado además para detectar un fallo de un segmento de la red próximo al dispositivo, y en respuesta al fallo, para envolver los paquetes que pertenecen al primer flujo entre los sentidos horario y antihorario para evitar el segmento averiado, sin envolver los paquetes en el segundo flujo.

La presente invención se pondrá más claramente de manifiesto a partir de la descripción detallada siguiente de las formas de realización preferidas de la misma, haciendo referencia a los dibujos, en los que:

Breve descripción de los dibujos

La figura 1 es un diagrama de bloques que muestra esquemáticamente una red en anillo bidireccional según una forma de realización preferida de la presente invención;

la figura 2 es un diagrama de bloques que muestra esquemáticamente detalles de un nodo en la red de la figura 1, según una forma de realización preferida de la presente invención,

las figuras 3A y 3B son diagramas de bloques que muestran esquemáticamente mecanismos de protección implementados en la red de la figura 1 en respuesta a un fallo en un enlace, según una forma de realización preferida de la presente invención, y

las figuras 4 y 5 son diagramas de flujo que muestran esquemáticamente métodos de protección contra fallos en una red en anillo según una forma de realización preferida de la presente invención.

Descripción detallada de las formas de realización preferidas

La figura 1 es un diagrama de bloques que muestra esquemáticamente una red en anillo de paquetes 20 según una forma de realización preferida de la presente invención. La red 20 comprende nodos 22, marcados de N1 a N6, que están conectados entre sí mediante medios de comunicación bidireccionales, tal como cables conductores o fibras ópticas. Los nodos normalmente comprenden equipos de conmutación y funcionan como puntos de acceso o portales a otras redes (puntos de agregación). Los medios de comunicación en la red 22 están configurados para definir un anillo exterior 24 por el que los paquetes se transportan entre los nodos en un sentido horario, y un anillo interior 26, por el que los paquetes se transportan en un sentido antihorario. Sin embargo, tal como se mencionó anteriormente, las designaciones de “interior”, “exterior”, “sentido horario” y “sentido antihorario” son arbitrarias y se utilizan en la presente memoria simplemente por conveniencia y claridad en la explicación. Además la designación y el número de nodos en la red 20 se seleccionan en la presente memoria a título de ejemplo, y la red puede, mediante el mismo testigo (token), comprender un número mayor o menor de nodos.

La figura 2 es un diagrama de bloques que muestra esquemáticamente detalles de uno de los nodos 22 en la red 20 según una forma de realización preferida de la presente invención. El nodo 22 comprende un bloque de control de acceso al medio (MAC) 33 conectado para transmitir y recibir datos a través de los anillos 24 y 26. El bloque 33 es responsable de la gestión de los anillos y realiza las funciones de capa del MAC de capturar paquetes que se dirigen al nodo 22 en cualquier anillo, mientras que pasa el resto del tráfico a través del siguiente nodo a lo largo del anillo. Preferentemente, el bloque 33 funciona según el protocolo RPR descrito en los antecedentes de la invención o con otro protocolo bidireccional similar. El protocolo de anillo básico se extiende por un protocolo de protección que proporciona la envoltura selectiva según una forma de realización preferida de la presente invención, tal como se describirá en detalle más adelante.

Cuando el bloque del MAC 33 captura un paquete dirigido a su propio nodo 22 entrega el paquete a un bloque de procesamiento de tráfico 34 del nodo. El bloque 34 es responsable de las funciones de capa de red, tal como procesamiento IP, y opcionalmente otras funciones de nivel superior, tales como la calidad de servicio (QoS) y la seguridad en la red. En un nodo que sirve como punto de acceso, por ejemplo, el bloque 34 es normalmente responsable de entregar paquetes a los usuarios que están conectados a la red 20 a través del nodo y de recibir paquetes desde los usuarios para la transmisión por la red 20.

Según el protocolo de protección aplicado en la red 20, los paquetes que se desplazan por la red contienen un indicador de envoltura, preferentemente en forma de un único bit en una ubicación específica en

o cerca del comienzo de cada paquete. El bloque de procesamiento de tráfico 34 fija o vuelve a fijar preferentemente el indicador de envoltura en cada paquete que transmite a la red. Normalmente, fijar el indicador de envoltura depende del tipo de servicio al que pertenece el paquete. Adicional o alternativamente fijar el indicador puede depender de la identidad de un usuario que envía los paquetes (y en particular del nivel de QoS que el usuario ha contratado), o de otros criterios establecidos por el usuario o gestor de una red 20.

Volviendo ahora al ejemplo representado en la figura 1, dos flujos 28 y 30 de paquetes se dirigen desde el nodo de origen N1 a través de los nodos intermedios N6 y N5 al nodo de destino N4 a través del anillo interior 26. A título de ejemplo, se supone que el flujo 28 pertenece a un servicio de datos, que transfiere bloques de datos según un protocolo que es relativamente insensible a fluctuaciones y al desorden de paquetes, tal como una aplicación de correo electrónico u otra aplicación de transferencia de datos que funciona a través del TCP/IP. El flujo 30, por otro lado, se supone que pertenece a un servicio en tiempo real, tal como voz a través del IP (VoIP) o servicio de vídeo bajo demanda (streaming) que puede tolerar paquetes perdidos ocasionales pero que es sensible a la fluctuación y al desorden. El indicador de envoltura se fija en los paquetes de flujo 28 pero se vuelve a fijar en los paquetes de flujo 30. Ambos flujos se interrumpen mediante un fallo 32 de un enlace entre los nodos N5 y N6.

Las figuras 3A y 3B muestran esquemáticamente cómo la red 20 gestiona el fallo 32 para los dos tipos diferentes de servicio ilustrados por los flujos 28 y 30, según una forma de realización preferida de la presente invención. Aunque por motivos de claridad, las figuras 3A y 3B son independientes, en la práctica, el mecanismo de protección ilustrado en las dos figuras puede funcionar simultáneamente. En la figura 3A se observa que el flujo 28 está envuelto en el anillo exterior 24 en los nodos N6 y N5, definiendo por tanto un trayecto de flujo de envoltura 36. Mientras tanto, el flujo 30 se direcciona mediante el anillo N1 en el anillo exterior 24, definiendo por tanto un trayecto de flujo de direccionamiento 38. Dado que el flujo 30 está indicado como un flujo de no envoltura, cualquier paquete en el flujo 30 que alcance el nodo N6 antes que el N1 comienza a direccionar los paquetes en el anillo exterior que se rechaza normalmente. Por tanto, de manera adicional o alternativa puede haber flujos (no representados) en la red 20 que ni se envuelven ni se direccionan. Los paquetes en estos flujos se rechazan simplemente si alcanzan los nodos N5 y N6 mientras que el fallo 32 continúa. Como otra alternativa, el flujo 28 puede envolverse temporalmente en el trayecto 36, normalmente hasta que se haya informado a todos los nodos en la red 20 sobre el fallo 32 y estén listos para iniciar el direccionamiento. En este momento, el trayecto de flujo 36 se suspende, y en su lugar, el flujo 28 se direcciona a lo largo del trayecto de flujo 38.

Se hará ahora referencia a las figuras 4 y 5 que son diagramas de flujo que ilustran esquemáticamente métodos para la protección contra fallos en la red 20 según una forma de realización preferida de la presente invención. El método se describe, mediante un ejemplo, haciendo referencia a los flujos 28 y 30. Se supone que los paquetes en el flujo 28 están indicados para la envoltura, mientras que los del flujo 30 no están indicados y así que se direccionan. La figura 4 describe el comportamiento de un nodo adyacente al enlace en el que se produce el fallo 32, tal como el nodo N6, mientras que la figura 5 se refiere a un nodo que origina un flujo de paquetes, tal como el nodo N1. La extensión del método a otras configuraciones de nodo y a esquemas de protección alternativos, tal como los mencionados anteriormente, es sencilla.

El método de la figura 4 se inicia cuando el nodo N6 detecta un fallo 32 de un enlace, en una etapa de detección de fallos 40. Inmediatamente al detectar el fallo, el N6 transmite un paquete de indicación de fallo alrededor del anillo 24, en una etapa de notificación 42 para informar a los otros nodos del fallo. (Normalmente, el nodo N5 también detecta el fallo, y por consiguiente, transmite un paquete de indicación de fallo alrededor del anillo 26). Posteriormente, el nodo N6 recibe paquetes en el anillo 26, en una etapa de recepción de paquetes 44, y determina cómo tratar cada paquete individualmente. El nodo comprueba el encabezamiento del paquete para determinar si el indicador de envoltura está fijado o se ha vuelto a fijar, en una etapa de comprobación de indicador 46. Si el indicador está fijado, el nodo N6 envuelve el paquete desde el anillo 26 en el anillo 24, en una etapa de envoltura 48. En el caso del flujo 28, el paquete se envuelve en el trayecto 36. Cuando el paquete alcanza el nodo N5, el indicador de envoltura se comprueba de nuevo, y por consiguiente el paquete se envuelve de vuelta en el anillo 26 en el que alcanza finalmente el nodo de destino N4.

Después de transmitir el paquete de indicación de fallo en la etapa 42, pero antes de que el nodo N1 esté listo para direccionar el flujo 30 en el trayecto 38, el nodo N6 puede todavía recibir paquetes que pertenecen al flujo 30. Dado que el indicador de envoltura de estos paquetes no está fijado, el nodo N6 simplemente pasa los paquetes sin envolverlos, en una etapa de no envoltura 50. Como resultado, estos paquetes se rechazan.

Tal como se muestra en la figura 5, el nodo N1 prepara paquetes en los flujos 28 y 30 para la transmisión, en una etapa de preparación de paquetes 60. Cuando no se produce un fallo en la red, los paquetes están destinados para la transmisión en una ruta a través de los nodos N6 y N5. Antes de transmitir los paquetes, N1 comprueba para determinar si se sabe si se han producido fallos en los enlaces que tiene que atravesar cada flujo, en una etapa de comprobación de fallos 62. Mientras ninguno de los otros nodos haya informado de tal fallo, y N1 no haya detectado un fallo por sí mismo, los paquetes se transmiten a lo largo de la ruta normal, sin direccionarse, en una etapa de transmisión normal 64. Si ha ocurrido el fallo 32, pero la indicación de fallo de N6 no ha llegado todavía al N1, los paquetes se transmitirán todavía en la ruta normal. En este caso, los paquetes en el flujo 28 se envuelven mediante N6, tal como se mencionó anteriormente, pero los paquetes en el flujo 30 se pasan a través de N6 en la etapa 50 y por tanto se rechazarán.

Una vez que N1 recibe la indicación de fallo, comienza direccionando los paquetes en el flujo 30 al flujo 38, en una etapa de direccionamiento 66. De manera similar, el nodo N6 y los otros nodos en la red 20 inician en este punto el direccionamiento de los flujos de paquetes que originan a los destinos apropiados. Preferentemente, para ahorrar recursos de red, N1 y los otros nodos direccionan asimismo los flu-

jos envueltos, tal como el flujo 28. Alternativamente, durante el fallo, solamente algunos flujos se direccionan, mientras que otros se envuelven o se atrasan o se rechazan para conservar recursos de red.

Aunque las formas de realización preferidas se describen en la presente memoria haciendo referencia a determinados tipos específicos de redes y protocolos, y particularmente a redes de paquetes basadas en el protocolo RPR, los principios de la presente invención pueden aplicarse de manera similar en redes en anillo bidireccionales y protocolos de otros tipos. De esta manera se apreciará que las formas de realización preferidas descritas anteriormente se citan a título de ejemplo, y que la presente invención no está limitada a lo que se ha mostrado y descrito en particular en la presente memoria anteriormente. El alcance de la presente invención comprende las combinaciones y combinaciones secundarias de las diversas características descritas anteriormente en la presente memoria, así como las variaciones y modificaciones de la misma que resultarán evidentes para el experto en la materia a partir de la descripción y que no se han dado a conocer en la técnica anterior.

REIVINDICACIONES

1. Método de protección contra fallos en una red en anillo bidireccional (20), en la que el tráfico de paquetes se transmite simultáneamente tanto en el sentido horario, como en el sentido antihorario alrededor de la red, **caracterizado** porque comprende las etapas siguientes:

transmitir unos primer y segundo flujos de paquetes (28, 30) alrededor de la red en anillo bidireccional (20) mientras que define el primer flujo (28) como un flujo de envoltura (48), y el segundo flujo (30) como un flujo de no envoltura (50); y

al detectar por un nodo (22) en la red que un segmento de la red próxima al nodo (22) se ha averiado, envolver los paquetes (48) en el primer flujo (28) en el nodo (22) entre los sentidos horario y antihorario para evitar el segmento averiado, mientras que los paquetes en el segundo flujo (30) no se envuelven (50).

2. Método según la reivindicación 1, en el que los paquetes en el segundo flujo (30) que alcanzan el nodo (22) se rechazan.

3. Método según la reivindicación 1, y que comprende direccionar los paquetes (66) en el segundo flujo (30) en uno de los sentidos horario y antihorario para alcanzar un destino del segundo flujo (30) mientras que se evita el segmento averiado.

4. Método según la reivindicación 3, en el que el direccionamiento de paquetes en el segundo flujo (30) comprende enviar un mensaje de indicación de fallo (62) desde el nodo (22) que detecta los segmentos averiados a un nodo de origen (22) del segundo flujo (30), e iniciar el direccionamiento de los paquetes (66) en el segundo flujo (30) en respuesta al mensaje.

5. Método según la reivindicación 4, y que comprende, cuando se inicia el direccionamiento de los paquetes (66) en el segundo flujo (30), direccionar asimismo los paquetes (66) en el primer flujo (28) e interrumpir la envoltura de los paquetes.

6. Método según cualquiera de las reivindicaciones 1 a 5, y que comprende enviar un mensaje de indicación de fallo (62) desde el nodo (22) que detecta los segmentos averiados a otros nodos (22) en la red (20) y, después de que los otros nodos (22) hayan recibido el mensaje, direccionar los paquetes (66) en el primer flujo (28) en uno de los sentidos horario y antihorario para alcanzar un destino del primer flujo (28) mientras evita el segmento averiado, e interrumpir la envoltura de los paquetes.

7. Método según la reivindicación 6, en el que los paquetes en el segundo flujo (30) se rechazan mientras continúa el fallo.

8. Método según cualquiera de las reivindicaciones 1 a 5, en el que la transmisión de los primer y segundo flujos (28, 30) comprende fijar un indicador de envoltura (46) en los paquetes en el primer flujo (28), mientras que se vuelve a fijar el indicador de envoltura (46) en los paquetes en el segundo flujo (30), y en el que la envoltura de los paquetes comprende determinar los paquetes que han de envolverse en respuesta al indicador de envoltura.

9. Método según cualquiera de las reivindicaciones 1 a 5, en el que la transmisión del segundo flujo (30) comprende proporcionar un servicio en tiempo real, mientras que la transmisión del primer flujo (28) comprende proporcionar un servicio de transmisión de datos que es sustancialmente más tolerante a las variaciones de retardo y al desorden en la entrega de paquetes que el servicio en tiempo real.

10. Método según la reivindicación 9, en el que el servicio en tiempo real comprende al menos un servicio de voz en paquetes y un servicio de vídeo en paquetes.

11. Sistema de comunicación, que comprende:

un medio de comunicación, y

una pluralidad de nodos de comunicación (22) acoplados entre sí mediante el medio de comunicación para formar una red en anillo (20), sobre la que se configuran los nodos (22) para transmitir el tráfico a los otros nodos tanto en el sentido horario como en el sentido antihorario, **caracterizado** porque el tráfico comprende un primer flujo (28) de paquetes definidos como un flujo de envoltura y un segundo flujo (30) de paquetes definido como flujo de no envoltura,

estando los nodos (22) adaptados, al detectar por un nodo dado de entre los nodos en la red que un segmento de la red próxima al nodo dado se ha averiado, para envolver los paquetes en el primer flujo (28) en el nodo dado entre los sentidos horario y antihorario para evitar el segmento averiado, y para no envolver los paquetes en el segundo flujo.

12. Sistema según la reivindicación 11, en el que el nodo dado está adaptado para rechazar los paquetes en el segundo flujo (30) que alcanzan el nodo dado.

13. Sistema según la reivindicación 11, en el que los nodos están además adaptados para direccionar los paquetes en el segundo flujo (30) en uno de los sentidos horario y antihorario para alcanzar el destino del segundo flujo mientras se evita el segmento averiado.

14. Sistema según la reivindicación 13, en el que el nodo dado está adaptado para enviar un mensaje de indicación de fallo (62) a un nodo de origen del segundo flujo (30) de entre los nodos en la red, que está adaptado para iniciar el direccionamiento (66) de los paquetes en el segundo flujo (30) en respuesta al mensaje.

15. Sistema según la reivindicación 14, en el que los nodos están además adaptados, cuando se inicia el direccionamiento de los paquetes en el segundo flujo (30), para direccionar asimismo (66) los paquetes en el primer flujo, con lo que el nodo dado está adaptado para interrumpir la envoltura de los paquetes.

16. Sistema según cualquiera de las reivindicaciones 11 a 15, en el que el nodo dado (22) está adaptado para enviar un mensaje de indicación de fallo (62) a los otros nodos (22) en la red (20), y en el que los nodos están adaptados, tras recibir el mensaje, para direccionar (66) los paquetes en el primer flujo (28) en uno de los sentidos horario y antihorario para alcanzar un destino del primer flujo (28) mientras se evita el segmento averiado, con lo que el nodo dado está adaptado para interrumpir la envoltura de los paquetes.

17. Sistema según la reivindicación 16, en el que el nodo dado está adaptado para rechazar los paquetes en el segundo flujo (30) que alcanza el nodo dado mientras continúa el fallo.

18. Sistema según cualquiera de las reivindicaciones 11 a 15, en el que los nodos que transmiten los primer (28) y segundo (30) flujos están adaptados para fijar un indicador de envoltura (46) en los paquetes en el primer flujo (28), mientras que vuelven a fijar el indicador de envoltura en los paquetes en el segundo flujo (30), en el que el nodo dado está adaptado para identificar los paquetes que han de envolverse (48) en respuesta al indicador de envoltura.

19. Sistema según cualquiera de las reivindicaciones 11 a 15, en el que el segundo flujo (30) pertenece a un servicio en tiempo real, mientras que el primer flujo (28) comprende un servicio de transmisión de datos que es sustancialmente más tolerante a las variaciones de retardo y al desorden en la entrega de paquetes que el servicio en tiempo real.

20. Sistema según la reivindicación 19, en el que el servicio en tiempo real comprende al menos un servicio de voz en paquetes y un servicio de vídeo en paquetes.

21. Dispositivo de comunicación, para funcionar como un nodo en una red en anillo sobre la cual se transmite el tráfico en los sentidos horario y antihorario, **caracterizado** porque comprende:

un bloque de procesamiento de tráfico (34), adaptado para preparar los paquetes de datos de salida para transmitirlos por la red en anillo (20), de manera que los paquetes pertenecen o bien a un primer flujo (28) de los paquetes definido como un flujo de envoltura, o bien a un segundo flujo (30) de los paquetes definido como un flujo de no envoltura, y

un bloque de control de acceso a medios (MAC) (33), en interconexión al bloque de procesamiento de tráfico (34) y adaptado para acoplarse a la red (20) para transmitir los paquetes de datos de salida y recibir los paquetes entrantes por la red en anillo (20) tanto en el sentido horario como en el antihorario, y adaptado además para detectar un fallo de un segmento de la red próximo al dispositivo, y en respuesta al fallo, para envolver los paquetes que pertenecen al primer flujo (28) entre los sentidos horario y antihorario con el fin de evitar el segmento averiado, sin envolver los paquetes en el segundo flujo (30).

22. Dispositivo según la reivindicación 21, en el que bloque del MAC está adaptado para rechazar los paquetes en el segundo flujo que alcanzan el bloque del MAC (33) después de que se produzca el fallo.

23. Dispositivo según la reivindicación 21, en el que el bloque del MAC (33) está además adaptado para direccionar los paquetes en el segundo flujo (30) en uno de los sentidos horario y antihorario para alcanzar un destino del segundo flujo (30) mientras se evita el segmento averiado.

24. Dispositivo según la reivindicación 23, en el que el bloque del MAC (33) está adaptado para enviar un mensaje de indicación de fallo (62) por la red a un nodo de origen del segundo flujo (30), para hacer que el nodo de origen inicie el direccionamiento de los paquetes en el segundo flujo (30) en respuesta al mensaje.

25. Dispositivo según la reivindicación 24, en el que el bloque de MAC (33) está además adaptado, cuando se inicia el direccionamiento (66) de los paquetes en el segundo flujo (30), para direccionar también los paquetes en el primer flujo (28), e interrumpir inmediatamente la envoltura de los paquetes.

26. Dispositivo según cualquiera de las reivindicaciones 21 a 25, en el que el bloque del MAC (33) está adaptado para enviar un mensaje de indicación de fallo (62) a los otros nodos en la red, que están adaptados, tras recibir el mensaje, para direccionar los paquetes en el primer flujo (28) en uno de los sentidos horario y antihorario para alcanzar un destino del primer flujo (28) mientras se evita el segmento averiado, con lo que el bloque del MAC (33) está adaptado para interrumpir la envoltura de los paquetes.

27. Dispositivo, según la reivindicación 26, en el que el bloque de MAC (33) está adaptado para rechazar los paquetes en el segundo flujo (30) que alcanzan el bloque del MAC (33) mientras continúa el fallo.

28. Dispositivo según cualquiera de las reivindicaciones 21 a 25, en el que el bloque del MAC (33) está adaptado para fijar un indicador de envoltura (46) en los paquetes en el primer flujo (28), y para volver a fijar el indicador de envoltura en los paquetes en el segundo flujo (30), y en el que el bloque del MAC (33) está adaptado para identificar los paquetes que han de envolverse en respuesta al indicador de envoltura.

29. Dispositivo según cualquiera de las reivindicaciones 21 a 25, en el que el segundo flujo (30) pertenece a un servicio en tiempo real, mientras que el primer flujo (28) comprende un servicio de transmisión de datos que es sustancialmente más tolerante a la variación de retardo y al desorden en la entrega de paquetes que el servicio en tiempo real.

30. Dispositivo según la reivindicación 29, en el que el servicio en tiempo real comprende al menos un servicio de voz en paquetes y un servicio de vídeo en paquetes.

FIG. 1

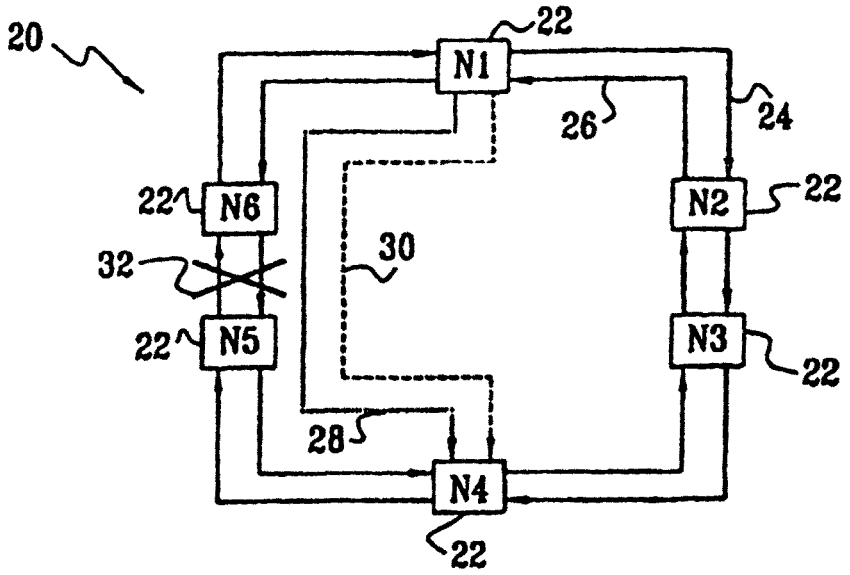
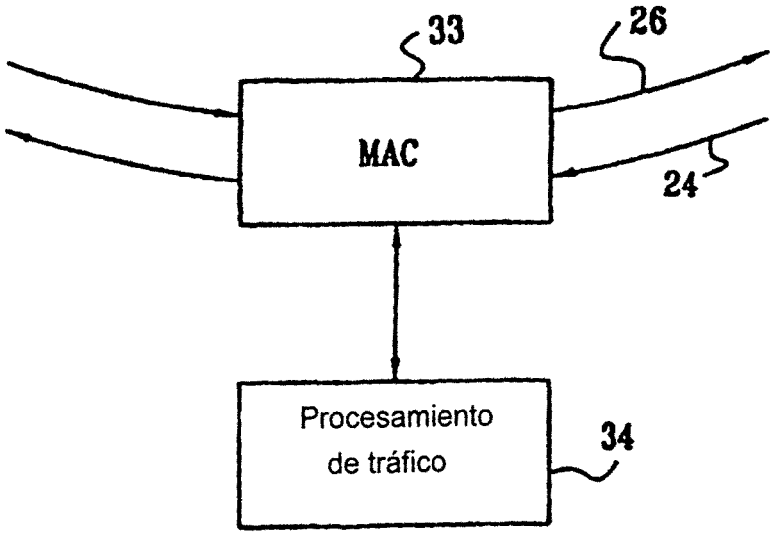

20
22
N1
26
24
22
N6
N2
22
32
30
22
N5
N3
22
28
N4
22

FIG. 2


22


33
26
MAC
24
Procesamiento
de tráfico
34

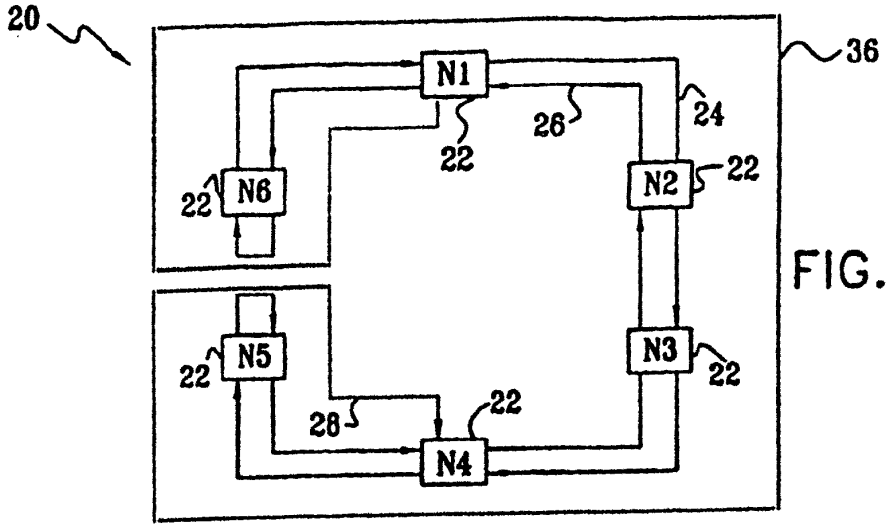

20
36
N1
22
26
24
22
N6
22
N2
22
N5
22
N3
22
28
22
N4

FIG. 3A

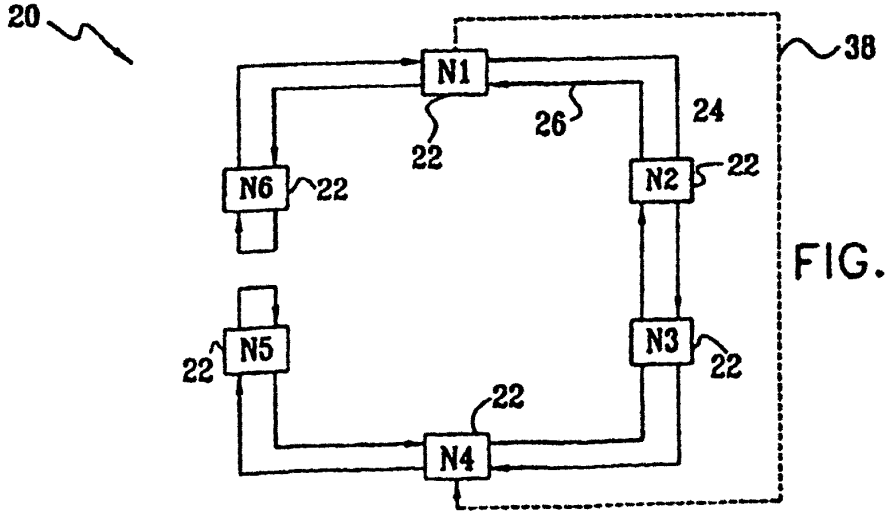

20
38
N1
22
26
24
N6
22
N2
22
22
N5
22
N3
22
22
N4

FIG. 3B

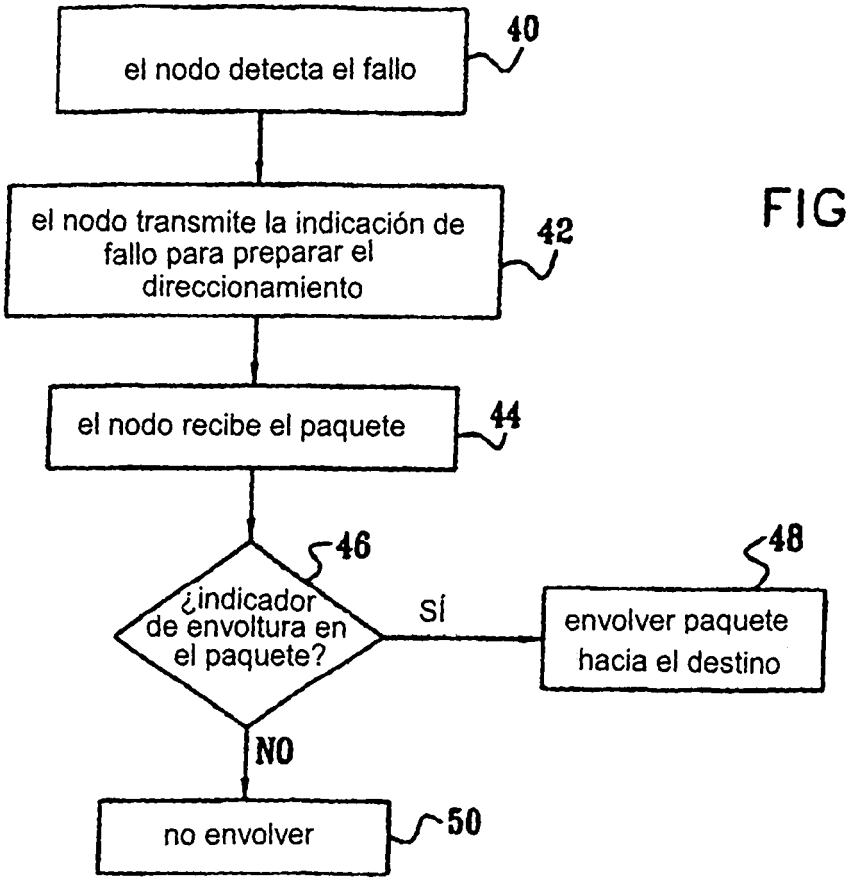

el nodo detecta el fallo
40
el nodo transmite la indicación de fallo para preparar el direccionamiento
42
el nodo recibe el paquete
44
46
¿indicador de envoltura en el paquete?
SÍ
48
envolver paquete hacia el destino
NO
no envolver
50

FIG. 4

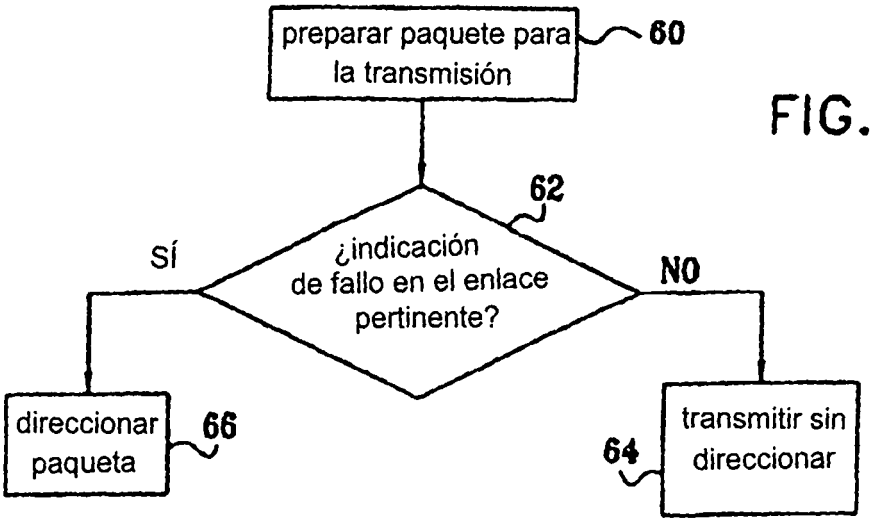

preparar paquete para la transmisión
60
62
¿indicación de fallo en el enlace pertinente?
SÍ
NO
direccionar paqueta
66
transmitir sin direccionar
64

FIG. 5