



19



OFICINA ESPAÑOLA DE  
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 311 901**

51 Int. Cl.:  
**H04L 12/437** (2006.01)  
**H04L 12/24** (2006.01)  
**H04L 12/46** (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **05011736 .5**  
96 Fecha de presentación : **31.05.2005**  
97 Número de publicación de la solicitud: **1729453**  
97 Fecha de publicación de la solicitud: **06.12.2006**

54 Título: **Procedimiento para conmutación de protección.**

45 Fecha de publicación de la mención BOPI:  
**16.02.2009**

45 Fecha de la publicación del folleto de la patente:  
**16.02.2009**

73 Titular/es:  
**Nokia Siemens Networks GmbH & Co. KG.**  
**St. Martin Strasse 76**  
**81541 München, DE**

72 Inventor/es:  
**Ricardo de Frias Rebelo Nunes, Pedro**

74 Agente: **Zuazo Araluze, Alexander**

ES 2 311 901 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).

# ES 2 311 901 T3

## DESCRIPCIÓN

Procedimiento para conmutación de protección.

5 La invención se refiere a un procedimiento para conmutación de protección en una red de datos según la reivindicación 1.

10 Las redes de datos que incluyen una pluralidad de anillos de datos comparten ciertos tramos de anillo para permitir la conmutación de protección y, por lo tanto, impedir puntos únicos de fallos. Sin embargo, si se elige tecnología Ethernet o una tecnología similar para la transmisión de datos una topología de este tipo crea problemas adicionales, debido a que es necesario impedir la formación de bucles en la red.

15 El principio del mecanismo de protección de anillo Ethernet ERP (*Ethernet Ring Protection*) se describe en la Patente estadounidense 6.430.151. Un gestor de redundancia, que está conectado a los extremos de línea de un anillo que contiene una pluralidad de nodos, comprueba la red transmitiendo y recibiendo paquetes de prueba. Si hay una interrupción en el anillo, el gestor de redundancia conecta los extremos de línea.

20 Este procedimiento se describe en detalle para uno o más anillos que tienen un nodo común, en la patente estadounidense 6.766.482 B1 cedida a Extreme Networks y se conoce como "*Ethernet Automatic Protection Switching*" EAPS.

25 En "*ExtremeWare 7.1.0 User Guide*", Extreme Networks, Santa Clara, Ca (US), páginas 281 a 290 se describen dos anillos de datos con nodos compartidos y un enlace compartido. Un anillo incluye un controlador; el otro anillo incluye un compañero. Si el enlace común falla el controlador es responsable de bloquear para impedir un "super bucle". Antes de que el enlace común vuelva el controlador va desde un estado de bloqueo hasta un estado "previo al reenvío", en el que los puertos están todavía bloqueados temporalmente para impedir un super bucle. Este procedimiento de protección requiere intercambios adicionales de diferentes paquetes de control entre el controlador y el compañero.

30 Es un objetivo de la presente invención proporcionar un procedimiento que lleve a una conmutación de protección más rápida y sencilla.

En la reivindicación 1 se describe un procedimiento que soluciona este problema.

35 La presente invención proporciona un procedimiento más sencillo mediante la asignación de diferentes prioridades a gestores de anillo y mediante un protocolo más sencillo que contiene paquetes de alarma que se envían sólo a los gestores de anillo que tienen mayor prioridad.

40 La presente invención se describe por medio de diferentes ejemplos y dibujos adjuntos. La invención puede ampliarse a una red más compleja y a una red similar a Ethernet. La invención resultará más evidente con referencia a la siguiente descripción detallada junto con los dibujos adjuntos, en los que

la figura 1 muestra una red de dos anillos con dos gestores de anillo,

45 la figura 2 muestra un fallo en un tramo común y la nueva estructura de red tras la conmutación de protección,

la figura 3 muestra la estructura de una red más compleja con una pluralidad de tramos compartidos y múltiples fallos,

50 la figura 4 muestra la estructura de una red más compleja con una pluralidad de tramos compartidos y múltiples fallos, y

la figura 5 muestra la estructura de red tras la conmutación de protección.

55 La figura 1 muestra una red que tiene dos anillos. Un primer anillo ERA con nodos 1, 2, 3 que incluye un gestor RMA de anillo asociado, y un segundo anillo ERB con nodos 2, 3, 4 que incluye un gestor RMB de anillo asociado que tiene una prioridad PR1 mayor que el gestor RMA de anillo con prioridad PR2. Cada puerto de un gestor de anillo o un nodo puede transmitir y recibir datos. Ambos anillos ERA y ERB comparten el tramo SP2,3 entre los "nodos de tramo común" 2 y 3 (un nodo de tramo común es un nodo, que tiene al menos un puerto P33, P23 conectado al el tramo común, o está insertado excepcionalmente entre estos "nodos de extremo" del tramo común). Según los requisitos de 60 Ethernet cada gestor RMA, RMB de anillo bloquea uno de sus puertos, por ejemplo PA2 y PB2, por lo que no hay conexión entre los puertos PA1 y PA2 o PB1 y PB2, que se muestran en diferentes lados de los gestores de anillo en el dibujo, y por lo tanto se evitan bucles (datos).

65 Cada gestor de anillo supervisa su anillo asociado. El gestor RMA de anillo supervisa el anillo ERA enviando "paquetes de prueba" TPA en el primer puerto PA1 de datos y recibiendo estos "paquetes de prueba" en el segundo puerto PA2 a través de una red de área local de control virtual conocida como VCLAN, por ejemplo realizada mediante una longitud de onda o ranura de tiempo diferente en la misma fibra, en la que se transmiten los datos. Una interrupción, por ejemplo entre el nodo 1 y el nodo 2, impediría que el gestor RMA de anillo recibiese sus propios paquetes TPA

## ES 2 311 901 T3

de prueba. El gestor RMA de anillo determinaría “pérdida de paquetes de prueba” LOTP y desbloquearía el segundo puerto PA2. Tras esta conmutación de protección el nodo 1 se conecta a través del gestor RMA de anillo con el nodo 3 y por lo tanto con la red. El anillo ERB se controla de la misma manera enviando paquetes TPB de prueba.

5 Cuando el tramo SP2,3 común entre sus nodos 2 y 3 de tramo común se interrumpe según la figura 2, los nodos 2 y 3 de tramo común lo detectarán (no se recibe señal) y enviarán un “mensaje de fallo” FSP2,3 sólo al gestor RMB de anillo de mayor prioridad PR1, que desbloquea su segundo puerto PB2. Los nodos de tramo común saben a partir de su propia base de datos de gestión o a partir de un sistema de gestión, qué gestor de anillo tiene la prioridad más alta. El desbloqueo del gestor RMB de anillo lleva a la red mostrada en la figura 2, en la que todos los nodos están conectados según esta “conmutación de protección” del gestor RMB de anillo. Se evita un “super bucle”, mostrado como una línea discontinua, porque el segundo puerto PA2 del gestor RMA de anillo permanece bloqueado. El mensaje de fallo también se transmite a través de la red de área local de control virtual.

15 Los paquetes de prueba enviados periódicamente por el gestor RMA de anillo tienen un intervalo de, por ejemplo, 50ms entre dos paquetes de prueba consecutivos y al menos tienen que monitorizarse dos paquetes perdidos antes de que el gestor RMA de anillo determine una señal de alarma. La conmutación de protección, es decir, el desbloqueo de los puertos del gestor RMB de anillo, se produce en un tiempo mucho más corto y los paquetes de prueba del gestor RMA de anillo se reenviarán mediante el gestor RMB de anillo de nuevo al gestor RMA de anillo. Por tanto, el gestor RMA de anillo ve un anillo completo y mantiene su segundo puerto RA2 bloqueado. Es suficiente y en una red más compleja favorable, cuando los paquetes de prueba sólo se transmiten a través de anillos de mayor prioridad.

25 La detección “pérdida de paquetes de prueba” LOTP del gestor RMB de anillo no tiene consecuencias, porque este gestor de anillo ya ha desbloqueado sus puertos. La transmisión de paquetes de prueba podría detenerse, cuando los puertos ya están desbloqueados.

30 Después de la detección de una interrupción del tramo SP2,3 compartido los puertos P23, P33 (al menos un puerto) de los nodos 2 y 3 de tramo común orientados al tramo SP2,3 común se ajustan a un estado “previo al reenvío” PFW tal como se muestra en la figura 3, donde se bloquean estos puertos. Cuando el tramo común se ha recuperado, por ejemplo está reparado, y el gestor RMB de anillo bloquea su segundo puerto PB2, los nodos 2 y 3 de tramo común saldrán de este estado previo al reenvío PFS y desbloquearán sus puertos (por ejemplo controlados por el gestor RMB de anillo), de modo que se restablece la configuración original mostrada en la figura 1.

35 La figura 4 muestra una red más compleja con cuatro anillos y tres tramos SP2,3; SP4,5; SP3,C comunes y cuatro gestores RMA, RMB, RMC, y RMD de anillo asociados a cuatro anillos ERA, ERB, ERC, ERD, cada gestor de anillo tiene una prioridad PR3, PR1, PR2, y PR4 diferente. Esta prioridad se asigna a los anillos asociados. Sólo se muestran algunos nodos 1 a 7. Los gestores de anillo están insertados en los enlaces de los anillos. Los tramos comunes están entre dos nodos de anillos adyacentes, por ejemplo ERA, y ERB, o entre un gestor de anillo, por ejemplo RMC y un nodo 6. Un puerto de todos los gestores de anillo está bloqueado para evitar un bucle. La prioridad del gestor de anillo es mayor en el centro de la red y se vuelve menor en los bordes.

40 Para hacer este ejemplo más complicado todos los tramos SP1, SP2 y SP3 comunes pueden interrumpirse al mismo tiempo tal como se muestra en la figura 5.

45 1. Los nodos 2, 3 (pertenecientes también al anillo ERA de prioridad PR3) y los nodos 4, 5 3 (pertenecientes también al anillo ERC de prioridad PR2) envían sus “mensajes de fallo (interrupción)” FSP2,3 y FSP4,5 al gestor RMB de anillo asociado de mayor prioridad PR1. El gestor RMB de anillo desbloquea su puerto PB2 abierto en el momento (1).

50 2. Aproximadamente al mismo tiempo (2) el gestor RMC de anillo detecta el “enlace caído” del tramo SP3 común y desbloquea su primer puerto PC1 abierto.

55 3. Todos los paquetes de prueba se reenvían a anillos de mayor prioridad. Por tanto, los paquetes de prueba del gestor RMA de anillo respectivamente el anillo ERA se reenvían a los anillos ERB y ERC, y el mensaje de prueba del anillo ERD se reenvía a los anillos ERC, ERB, y ERA. Los paquetes de prueba de ERB están restringidos a su propio bucle ERB. Sólo los paquetes de prueba de los anillos ERA y ERD son necesarios para la función de protección porque los puertos de RMB y RMC ya están desbloqueados. Por lo tanto, la transmisión de los paquetes de prueba de los demás gestores de anillo podría detenerse. En este momento los gestores RMA de anillo del anillo ERA y RMD del anillo ERD están transmitiendo paquetes TPA y TPD de prueba. Los intervalos de prueba para transmitir paquetes de prueba consecutivos de gestores de anillo con menor prioridad se eligen más largos que los intervalos de prueba de paquetes de prueba que se transmiten por gestores de anillo de mayor prioridad. Por lo tanto, el gestor RMA de anillo con prioridad PR3 determina “bucle caído” LOTP antes que el gestor RMD de anillo con prioridad PR4 y desbloquea su segundo puerto PA2 en el momento (3). Los paquetes de prueba de ERD se transmiten a través de RMC, nodos 5 y 4, RMA, nodos 1,2, RMB, nodos 4, 6 y 7 y se reciben en el puerto bloqueado.

65 En una variación del procedimiento los paquetes de prueba pueden enviarse a todos los anillos, pero sólo se transmiten a través de gestores de anillo con mayor prioridad. También puede enviarse el mensaje FSPXX de fallo a todos los gestores de anillo, pero sólo el gestor de anillo asociado del tramo compartido roto con mayor prioridad lo aceptará. Esto es sólo una cuestión de la VCLAN virtual y no influye en la función.

## ES 2 311 901 T3

	1, 2, 3, ...	nodo
	ERA	anillo A
5	RMA	gestor A de anillo del anillo ERA
	SP2,3	tramo compartido entre los nodos 2 y 3
	FSP2,3	mensaje de fallo del tramo SP2,3 compartido
10	TPA	paquete de prueba de RMA
	PFW	estado previo al reenvío
15		
20		
25		
30		
35		
40		
45		
50		
55		
60		
65		

## ES 2 311 901 T3

### REIVINDICACIONES

5 1. Procedimiento para conmutación de protección en una red de datos que incluye al menos dos anillos (ERA, ERB) con un tramo (SP2,3) compartido y una pluralidad de nodos (1-4), teniendo cada anillo (ERA, ERB) un gestor (RMA, RMB) de anillo asociado para comprobar su anillo (ERA, ERB) asociado,

**caracterizado** porque

10 los gestores (RMA, RMB) de anillo tienen diferentes prioridades (PR1, PR2) dedicadas,

15 cada nodo (2,3) de tramo compartido está monitorizando el tramo (SP2,3) compartido y, en caso de un fallo de tramo, envía un mensaje (FSP2,3) de fallo a un gestor (RMB) de anillo de mayor prioridad (PR1) de un anillo (ERB) asociado, y el gestor (ERB) de anillo de mayor prioridad desbloquea su puerto (PB2) mientras que el gestor (RMA) de anillo de menor prioridad (PR1) mantiene su puerto (PA2) bloqueado.

20 2. Procedimiento según la reivindicación 1, **caracterizado** porque, cada gestor (RMA) de anillo envía paquetes (TPA) de prueba a uno de sus puertos (PA1) y monitoriza la recepción de este paquete de prueba en su segundo puerto (PA2) y, si los paquetes (TPA) de prueba no se reciben, desbloquea su puerto (PA2).

25 3. Procedimiento según la reivindicación 2, **caracterizado** porque, según la prioridad de los gestores de anillo (RMA, RMB, ....) los paquetes (TPA, TPB, ....) de prueba se transmiten desde los gestores (RMA, RMB, ....) de anillo con diferentes intervalos de tiempo entre dos paquetes (TPA) de prueba sucesivos.

30 4. Procedimiento según la reivindicación 3, **caracterizado** porque, los intervalos de tiempo entre los mensajes (TPB) de prueba enviados por el gestor (PRB) de anillo con alta prioridad (PR1) son más cortos que los intervalos de tiempo entre mensajes (TPA) de prueba enviados por el gestor (PRB) de anillo con menor prioridad (PR2).

35 5. Procedimiento según la reivindicación 2, **caracterizado** porque, los paquetes (TPA) de prueba de un gestor (RMA) de anillo sólo se transmiten a través de enlaces pertenecientes a un anillo (ERB, ERC) con mayor prioridad.

40 6. Procedimiento según la reivindicación 2, **caracterizado** porque, el puerto (P23, P33) de un nodo (2, 3) de tramo común orientado a un tramo (SP2,3) común se ajusta a un estado (PFW) previo al reenvío hasta que se repara el fallo, y porque el puerto (P23, P33) de un nodo (2, 3) de tramo común orientado a un tramo (SP2,3) común se desbloquea después de que se bloqueen los puertos (PBA, PB2) de los gestores (RMA, RMB) de anillo de los anillos asociados, de tal modo que se evita un bucle de datos.

40

45

50

55

60

65

FIG 1

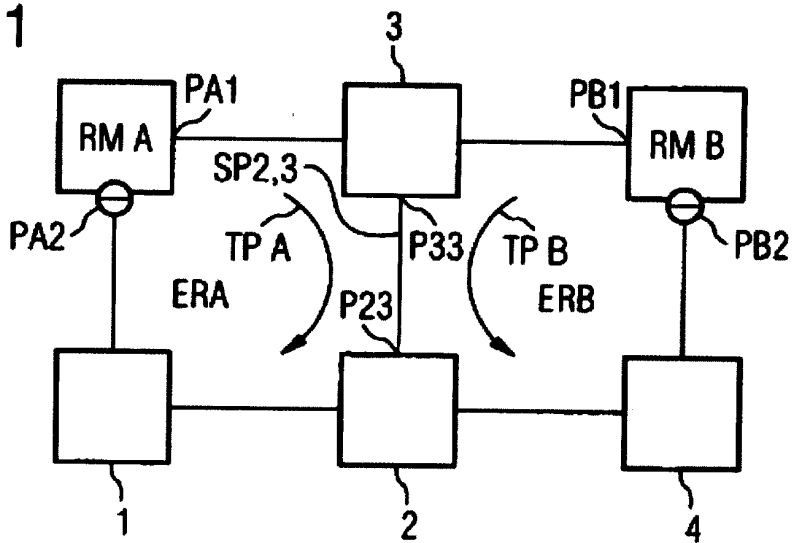


FIG 2

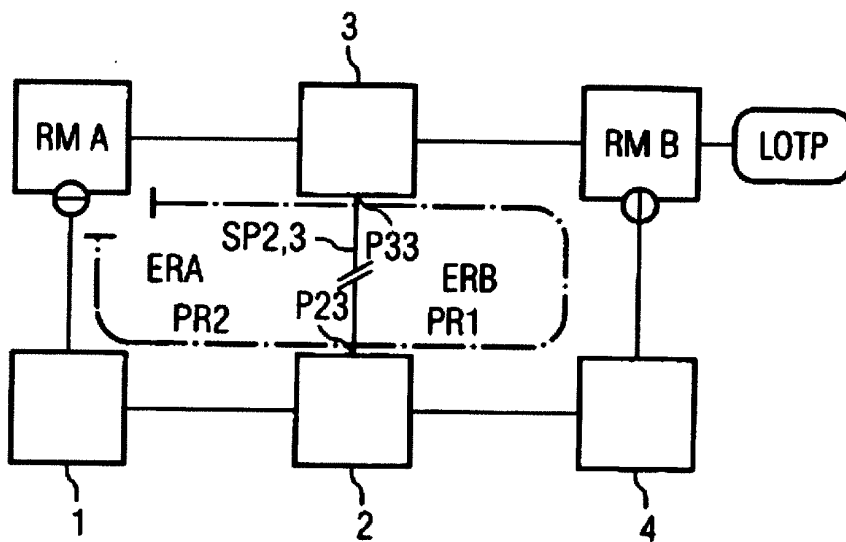


FIG 3

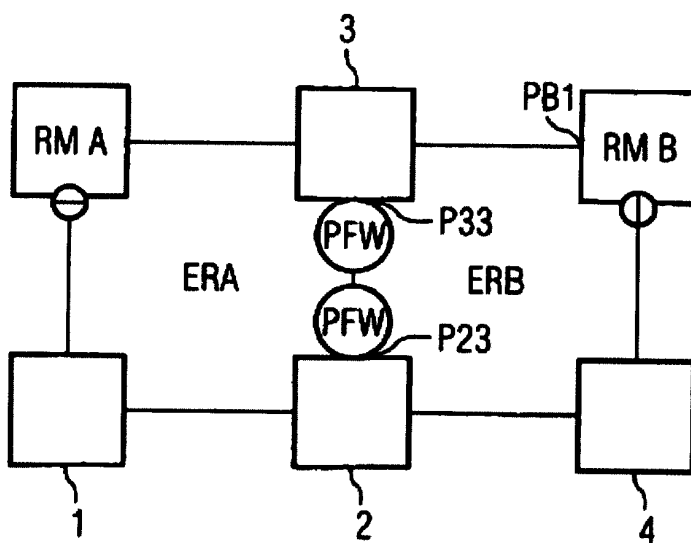


FIG 4

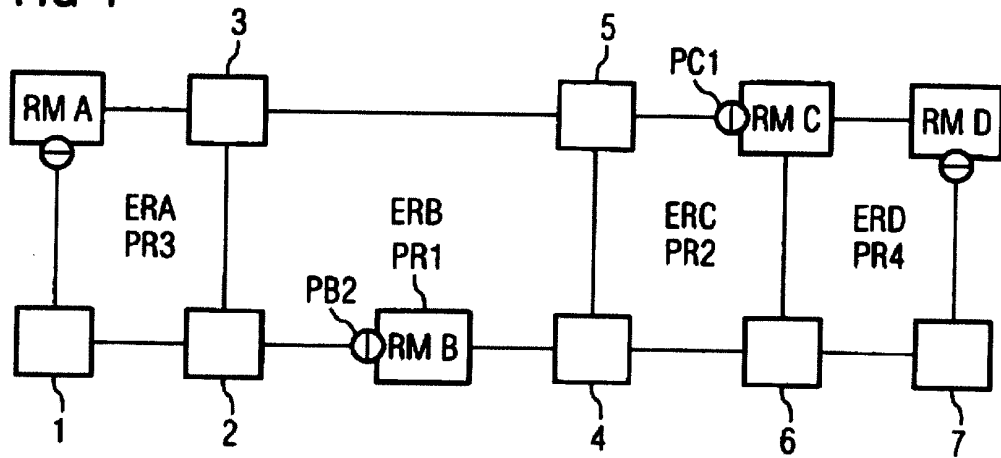


FIG 5

