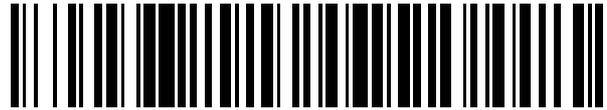


19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 455 190**

51 Int. Cl.:

H04L 12/24 (2006.01)

H04L 12/437 (2006.01)

H04L 12/26 (2006.01)

H04L 12/42 (2006.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **19.12.2007 E 07855718 (8)**

97 Fecha y número de publicación de la concesión europea: **19.02.2014 EP 2207307**

54 Título: **Método para el procesamiento del fallo operativo del puerto esclavo del nodo maestro en un sistema de red Ethernet en anillo**

30 Prioridad:

12.10.2007 CN 200710182245

45 Fecha de publicación y mención en BOPI de la traducción de la patente:

14.04.2014

73 Titular/es:

**ZTE CORPORATION (100.0%)
ZTE PLAZA, KEJI ROAD SOUTH, HI-TECH
INDUSTRIAL PARK, NANSHAN DISTRICT
SHENZHEN, GUANGDONG 518057, CN**

72 Inventor/es:

WU, SHAOYONG

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 455 190 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 para el procesamiento del fallo operativo del puerto esclavo del nodo maestro en un sistema de red Ethernet en anillo

5 CAMPO TÉCNICO

10 La presente invención se refiere a un campo técnico de protección automática de red Ethernet en anillo y más en particular, a un método de procesamiento de fallos para un puerto esclavo de un nodo maestro en un sistema Ethernet en anillo.

ANTECEDENTES DE LA INVENCION

15 Un sistema de protección de red Ethernet en anillo en RFC3619 está configurado en un anillo mediante la conexión de una pluralidad de nodos uno respecto a otro. Una pluralidad de dominios, esto es, dominios de protección de red Ethernet en anillo, pueden definirse en el anillo. Un dominio comprende un nodo maestro y varios nodos de tránsito y un grupo de redes de área local virtuales de servicio (VLANs) que se protegen y utilizan para reenviar datos de usuarios, en donde dos puertos del nodo maestro en el anillo se definen como puerto maestro y puerto esclavo respectivamente y las redes VLANs de servicio, que están protegidas, se definen como redes VLAN de servicio protegidas. Cuando los enlaces en el anillo funcionan adecuadamente, el nodo maestro bloquea la función de reenvío de la red VLAN de servicio protegida del puerto esclavo, de modo que ningún circuito en anillo se forme en la red y se evita la denominada "tormenta de difusión" introducida por el circuito en anillo en la red; cuando falla un enlace, el nodo maestro libera la función de reenvío de la red VLAN de servicio protegida del puerto esclavo de modo que los datos del usuario pueden pasar a través del puerto esclavo del nodo maestro y se asegura la conectividad del servicio. En alguna técnica de protección de red Ethernet en anillo, un nodo maestro es también referido como propietario de enlace de protección de anillo, un enlace que conecta directamente el puerto esclavo del nodo maestro que se refiere como Enlace de Protección de Anillo.

30 La Figura 1 es un diagrama topológico del sistema de protección automática de la red Ethernet en anillo en un estado operativo normal. El sistema está constituido por los nodos S1, S2, S3 y S4 y un dominio de protección de la red Ethernet en anillo está configurado en un anillo constituido por los cuatro nodos. En este dominio, el nodo maestro es S2 y los otros nodos S1, S3 y S4 son nodos de tránsito. Dos puertos del nodo maestro S2, en el anillo, son el puerto maestro y el puerto esclavo, respectivamente, en donde el puerto 2 es el puerto maestro (P) y el puerto 1 es el puerto esclavo (S). Además, una red VLAN de servicio protegida, en donde cada puerto en el anillo está configurado, se define en el dominio. Cuando los enlaces en el anillo funcionan adecuadamente, el nodo maestro S2 bloquea la función de reenvío de datos de la red VLAN de servicio protegida del puerto esclavo 1 para evitar un circuito en anillo existente en la red y que ocurra la denominada "tormenta de difusión"; cuando falla un enlace en el anillo, el nodo maestro S2 libera la función de reenvío de datos de la red VLAN de servicio protegida del puerto esclavo 1, de modo que los datos de la red VLAN de servicio sean accesibles de nuevo, según se indica en la Figura 2.

45 Cada nodo detecta si existe un fallo en un enlace adyacente a dicho nodo en el anillo y envía un mensaje de alarma de fallo del enlace para notificar al nodo maestro que existe un fallo en los enlaces cuando se detecta un fallo operativo. Después de recibir el mensaje de alarma de fallo del enlace, el nodo maestro libera la función de reenvío de datos de la red VLAN de servicio protegida del puerto esclavo, de modo que los datos en la red VLAN de servicio sean accesibles de nuevo. Cuando falla un enlace correspondiente al puerto esclavo del nodo maestro (esto es, el enlace que conecta directamente el puerto esclavo), un nodo en un extremo opuesto en relación con el puerto esclavo del nodo maestro lo notifica al nodo maestro enviando un mensaje de alarma de fallo del enlace después de que el nodo detecte dicho fallo de enlace y a continuación, el nodo maestro realiza una transferencia del fallo del enlace y libera la función de reenvío de datos de la red VLAN de servicio protegida del puerto esclavo, según se ilustra en la Figura 3. Puesto que el enlace que conecta el puerto esclavo del nodo maestro está en un estado de fallo operativo y no se pueden reenviar los datos y el puerto esclavo se establece en un estado liberado, de este modo existe un fallo del estado operativo del puerto.

55 El fallo del estado operativo del puerto, anteriormente citado, puede dar lugar a los problemas siguientes:

60 en primer lugar, la información falsa de los usuarios cuando los usuarios la requieren, puesto que el puerto está en un estado operativo liberado, lo que significa que se pueden transmitir los datos; sin embargo, los datos no se pueden transmitir en el estado liberado actual;

65 en segundo lugar, si el enlace es unidireccional, un extremo opuesto del puerto esclavo del nodo maestro no puede detectar el fallo operativo del puerto, mientras que el puerto esclavo del nodo maestro puede detectar el fallo del enlace, en este caso, si el puerto esclavo del nodo maestro está en un estado operativo liberado y el extremo opuesto del puerto esclavo del nodo maestro está también en un estado liberado, con lo que ningún puerto en el anillo está bloqueado cuando se recupere el enlace, lo que dará lugar a un bucle instantáneo y a la 'tormenta de difusión' antes citada.

Existe un problema similar en otros métodos de protección de red Ethernet en anillo, tales como un método dado a conocer en la patente EP1727313.

5 La solicitud de patente china CN 1812361A da a conocer un método de procesamiento de fallos para un puerto esclavo de un nodo maestro en una red Ethernet en anillo en donde cuando el nodo maestro detecta el fallo del enlace directo de su puerto esclavo, el puerto esclavo no se restablece para el reenvío.

SUMARIO DE LA INVENCION

10 La presente invención da a conocer un método de procesamiento de fallos para un puerto esclavo de un nodo maestro en un sistema Ethernet en anillo con el fin de evitar un fallo del estado operativo del puerto cuando falla un enlace que conecta directamente el puerto esclavo del nodo maestro en el dominio del sistema Ethernet en anillo.

15 Para resolver el problema técnico anterior, la presente invención da a conocer un método de procesamiento de fallos operativos para un puerto esclavo de un nodo maestro en un sistema Ethernet en anillo, que comprende las etapas siguientes:

(1) la detección, por el nodo maestro, de un estado de un enlace que conecta directamente el puerto esclavo y

20 (2) el establecimiento del puerto esclavo en un estado bloqueado si falla el enlace que conecta directamente el puerto esclavo del nodo maestro haciendo caso omiso de si el sistema Ethernet en anillo está en un estado operativo normal o en un estado de fallo operativo antes de que se detecte el fallo del enlace que conecta directamente el puerto esclavo y el mantenimiento del puerto esclavo en el estado bloqueado durante el fallo operativo del enlace.

25 Además, en la etapa (1), el nodo maestro detecta el estado del enlace que conecta directamente el puerto esclavo detectando una señal óptica.

30 Además, si ninguna señal óptica transmitida por el enlace que conecta directamente el puerto esclavo se detecta por el nodo maestro, se determina que el enlace que conecta directamente el puerto esclavo está en condición de fallo operativo.

35 Además, en la etapa (1), se transmite un paquete entre el nodo maestro y un nodo en un extremo opuesto del enlace que conecta directamente el puerto esclavo para detectar el estado operativo del enlace que conecta directamente el puerto esclavo.

40 Además, si no se recibe ningún paquete de detección desde el nodo en el extremo opuesto por el nodo maestro, en un periodo de tiempo, se determina que el enlace que conecta directamente el puerto esclavo está en condición de fallo operativo.

45 Además, en la etapa (2), cuando el puerto esclavo está en estado bloqueado, se rechazarían los datos si los datos se reciben en el puerto bloqueado desde una red de área local virtual protegida y los datos de la red de área local virtual protegida no serían enviados ni reenviados a un puerto de un nodo en un extremo opuesto.

50 Según el método de procesamiento de fallos operativos para un puerto esclavo de un nodo maestro en un sistema Ethernet en anillo, cuando falla un enlace que conecta directamente el puerto esclavo del nodo maestro, el puerto esclavo se establece en un estado bloqueado y el puerto esclavo se mantiene en el estado bloqueado durante el fallo operativo del enlace correspondiente al puerto esclavo del nodo maestro, con el fin de garantizar que el puerto esclavo del nodo maestro esté en un estado operativo correcto.

BREVE DESCRIPCION DE LOS DIBUJOS

55 La Figura 1 es el diagrama topológico de un sistema de protección de Ethernet en anillo cuando funcionan adecuadamente los enlaces en el anillo;

La Figura 2 es el diagrama topológico de un sistema de protección de Ethernet en anillo cuando falla un enlace en el anillo;

60 La Figura 3 es el diagrama topológico de un sistema de protección de Ethernet en anillo cuando falla un enlace que conecta el puerto esclavo del nodo maestro;

La Figura 4 es el diagrama de flujo de un método de procesamiento de fallos operativos para un puerto esclavo de un nodo maestro en un sistema de Ethernet en anillo según la presente invención;

65 La Figura 5 es una ilustración de una forma de realización de la presente invención cuando falla un enlace que conecta un puerto esclavo de un nodo maestro;

La Figura 6 es una ilustración de una forma de realización de la presente invención cuando falla una pluralidad de enlaces en el anillo.

FORMAS DE REALIZACIÓN PREFERIDAS DE LA PRESENTE INVENCION

5 La idea de la presente invención es que un nodo maestro en un sistema Ethernet en anillo bloquearía un puerto esclavo cuando detecta que falla un enlace de conexión directa del puerto esclavo sea cual fuere un estado del sistema Ethernet en anillo en condición normal o en condición de fallo operativo antes de que se detecte un fallo del puerto esclavo y mantener el puerto esclavo en el estado bloqueado durante el fallo operativo del enlace.

10 La presente invención se describirá, en detalle, haciendo referencia a los dibujos adjuntos y una forma de realización descrita a continuación.

15 Según se ilustra en la Figura 4, un método de procesamiento de fallos para un puerto esclavo de un nodo maestro en un sistema Ethernet en anillo, según la presente invención, comprende las etapas siguientes de:

Etapas 401, la detección, por el nodo maestro del estado del enlace que conecta directamente el puerto esclavo;

20 Existe una pluralidad de mecanismos de detección, actualmente, que se pueden utilizar para detectar un estado operativo de un enlace. A modo de ejemplo, se pueden utilizar fibras para detectar señales ópticas y si no se detecta ninguna señal óptica, el enlace se considera como estando en condición de fallo operativo; como alternativa, se realiza la detección transmitiendo un paquete entre el nodo maestro y el nodo en el extremo opuesto y si no se recibe ningún paquete de detección desde el nodo en el extremo opuesto en un periodo de tiempo, se considera que el enlace está en condición de fallo operativo.

25 Etapa 402, si falla el enlace que conecta directamente el puerto esclavo del nodo maestro, el establecimiento del puerto esclavo en un estado bloqueado, esto es, bloqueando la función de reenvío de la red VLAN de servicio protegida del puerto esclavo sea cual fuere un estado del sistema Ethernet en anillo en condición normal o en condición de fallo operativo antes de que se detecte un fallo del puerto esclavo y manteniendo el puerto esclavo en el estado bloqueado durante el fallo del enlace que conecta directamente el puerto esclavo del nodo maestro.

30 Cuando el puerto esclavo está en el estado bloqueado, se rechazarían los datos si se reciben los datos en el puerto bloqueado desde la red VLAN protegida y los datos de la red VLAN protegida no se enviarían ni reenviarían al puerto del nodo en el extremo opuesto. Por supuesto, todavía se permite transmitir las tramas del protocolo del sistema Ethernet en anillo.

35 Las Figuras 5 y 6 ilustran una forma de realización de la presente invención en un sistema de protección de Ethernet en anillo:

40 existen 3 nodos transmisores y 1 nodo maestro en el anillo y falla un enlace que conecta un puerto esclavo del nodo maestro, de modo que el puerto esclavo del nodo maestro se establece en un estado bloqueado, según se ilustra en la Figura 5. Falla otro enlace y se envía un mensaje de alarma de fallo operativo del enlace al nodo maestro y el puerto esclavo se mantiene todavía en el estado bloqueado, puesto que falla el enlace que conecta el puerto esclavo del nodo maestro, según se indica en la Figura 6.

45 Según el método de procesamiento de fallos operativos para un puerto esclavo de un nodo maestro en un sistema de Ethernet en anillo en conformidad con la presente invención, el puerto esclavo del nodo maestro se mantiene en el estado bloqueado durante el fallo operativo del enlace correspondiente al puerto esclavo, con el fin de evitar el fallo del estado operativo del puerto cuando falla el puerto esclavo del nodo maestro en el dominio de Ethernet en anillo, con lo que se evita la información falsa del usuario cuando la requiere y se evita la posibilidad de la denominada 'tormenta de difusión'. La presente invención se puede aplicar en una pluralidad de tecnologías de protección de Ethernet en anillo.

50 La descripción anterior es simplemente una forma de realización preferida y no pretende limitar el alcance de la presente invención. Un experto en esta técnica considerará que la presente invención puede tener diversas modificaciones y variantes, que caerán todas ellas dentro del alcance de protección de la presente invención según se determina por las reivindicaciones.

Aplicabilidad industrial

60 Según el método de procesamiento de fallos operativos para un puerto esclavo de un nodo maestro en un sistema Ethernet en anillo, en conformidad con la presente invención, cuando falla el enlace que conecta el puerto esclavo del nodo maestro, el puerto esclavo se establece y mantiene en el estado bloqueado durante el fallo operativo del enlace correspondiente al puerto esclavo con el fin de evitar el fallo del estado operativo del puerto cuando falla el puerto esclavo del nodo maestro en el dominio Ethernet en anillo, con lo que se evita la información falsa del usuario cuando la requiere y para evitar la posibilidad de la denominada 'tormenta de difusión'. La presente invención se

puede aplicar en una pluralidad de tecnologías de protección de Ethernet en anillo.

REIVINDICACIONES

- 5 **1.** Un método de procesamiento de fallos operativos para un puerto esclavo de un nodo maestro en un sistema de Ethernet en anillo, que comprende las etapas siguientes:
- 1) el nodo maestro detecta un estado de un enlace que conecta directamente el puerto esclavo y
- 10 2) establecimiento del puerto esclavo en un estado bloqueado si falla el enlace que conecta directamente el puerto esclavo del nodo maestro,
- 15 caracterizado por cuanto que
- la etapa de establecimiento se realiza haciendo caso omiso de si el sistema Ethernet en anillo está en un estado normal o en un estado de fallo antes de que se haya detectado el fallo del enlace que conecta directamente el puerto esclavo y
- 20 por cuanto que el método comprende, además, el mantenimiento del puerto esclavo en el estado bloqueado durante el fallo del enlace.
- 2.** El método según la reivindicación 1, en donde en la etapa 1), el nodo maestro que detecta el estado del enlace que conecta directamente el puerto esclavo se realiza detectando una señal óptica.
- 3.** El método según la reivindicación 2, en donde si no se detecta ninguna señal óptica transmitida por el enlace, que conecta directamente el puerto esclavo, por el nodo maestro, se determina que el enlace que conecta directamente el puerto esclavo está en condición de fallo operativo.
- 25 **4.** El método según la reivindicación 1, en donde en la etapa 1), la detección del estado del enlace que conecta directamente el puerto esclavo se efectúa mediante la transmisión de un paquete entre el nodo maestro y un nodo en una extremidad opuesta del enlace que conecta directamente el puerto esclavo.
- 30 **5.** El método según la reivindicación 4, en donde si no se recibe un paquete de detección desde el nodo en la extremidad opuesta por el nodo maestro durante un determinado periodo de tiempo, se determina que el enlace que conecta directamente el puerto esclavo está en condición de fallo operativo.
- 35 **6.** El método según la reivindicación 1, en donde en la etapa 2), cuando el puerto esclavo está en el estado bloqueado, se rechazarían los datos si fueran recibidos en el puerto bloqueado procedente de una red de área local virtual protegida y los datos de la red de área local virtual protegida no serían enviados ni reenviados a un puerto de un nodo en una extremidad opuesta.

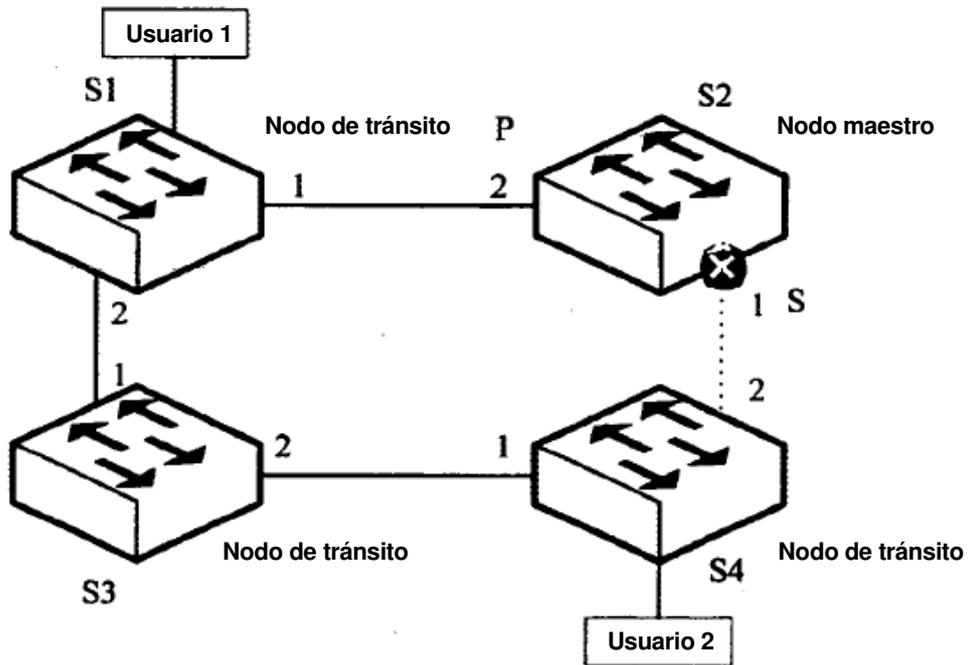


FIG. 1

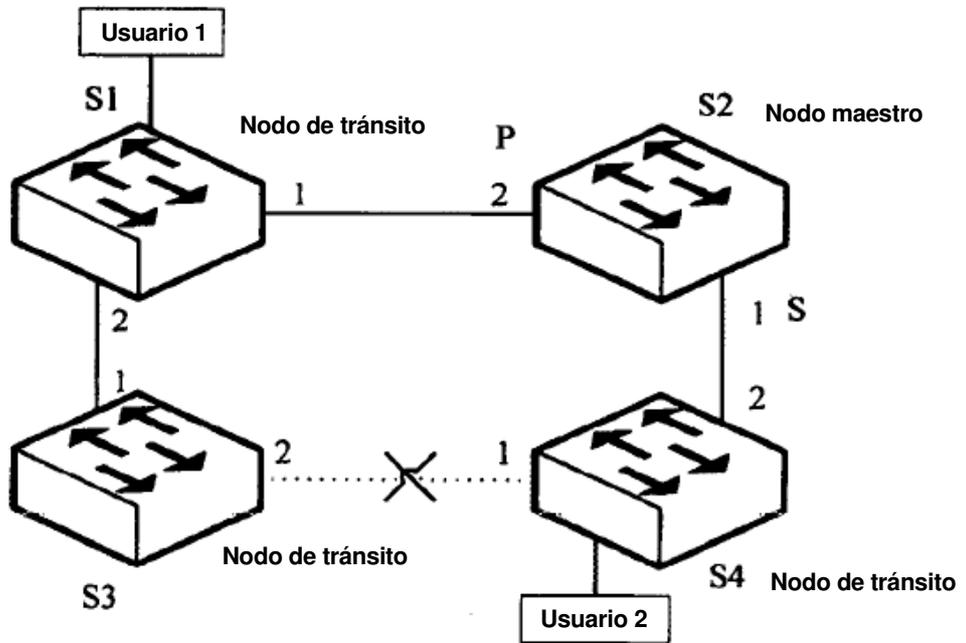


FIG. 2

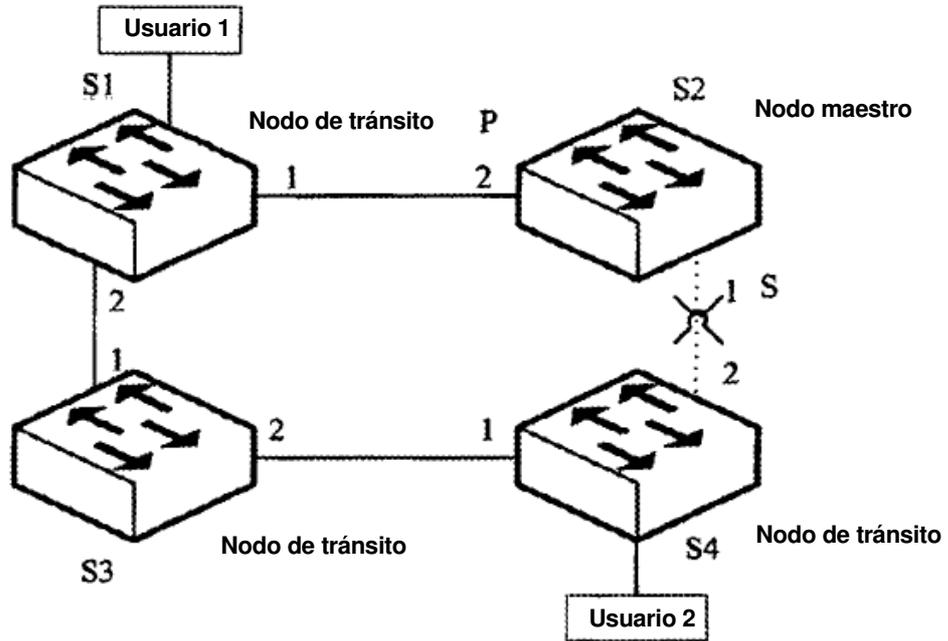


FIG. 3

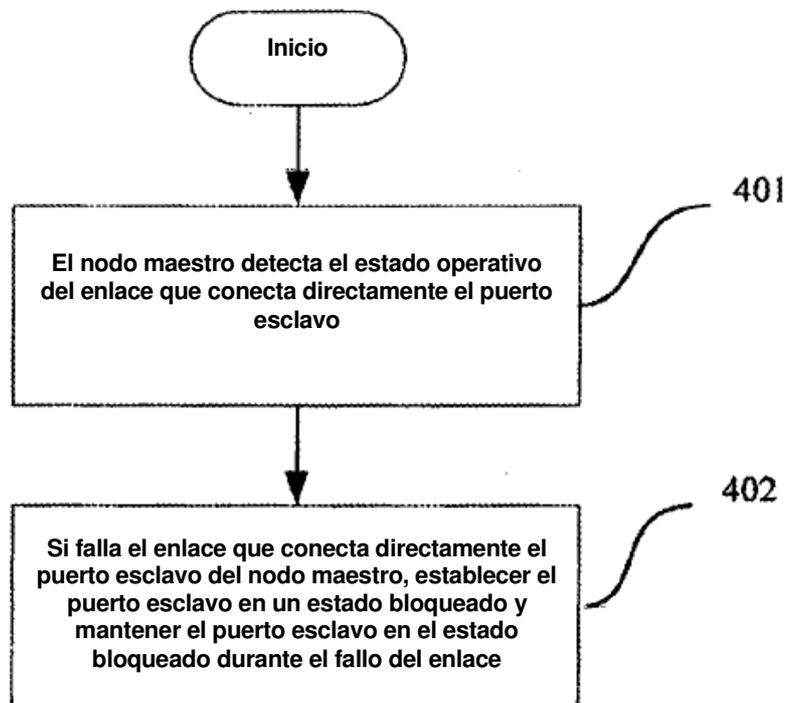


FIG. 4

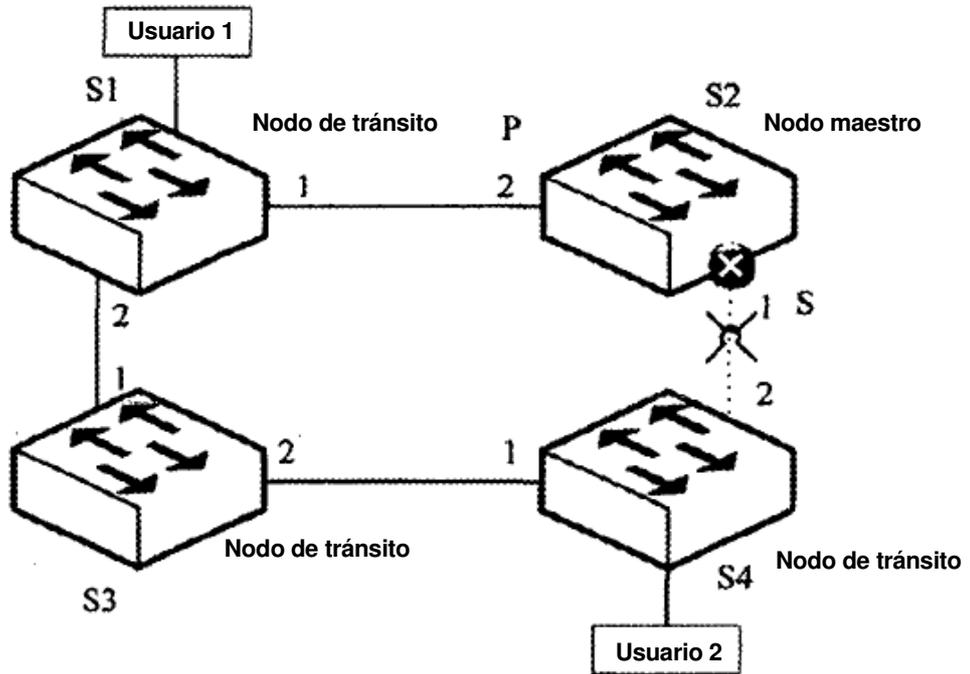


FIG. 5

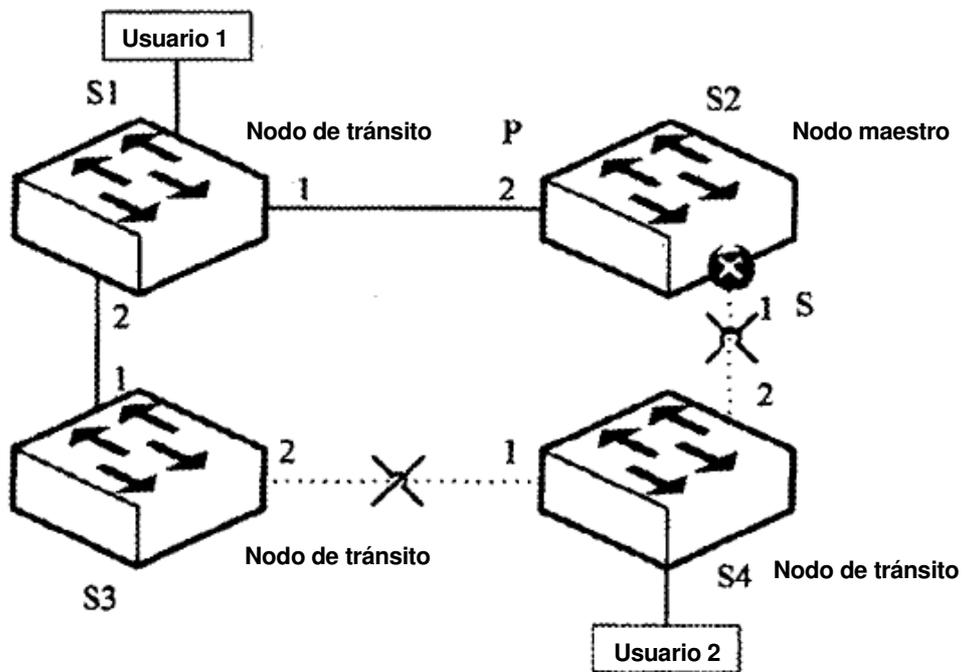


FIG. 6