



19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA

11 Número de publicación: **2 365 864**

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

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Número de solicitud europea: **06722220 .8**

96 Fecha de presentación : **31.03.2006**

97 Número de publicación de la solicitud: **1868322**

97 Fecha de publicación de la solicitud: **19.12.2007**

54 Título: **Un método para implementar protección de redes combinando la doble adscripción de elementos de red y la protección de redes en anillo.**

30 Prioridad: **04.04.2005 CN 2005 1 0063129**

45 Fecha de publicación de la mención BOPI:
11.10.2011

45 Fecha de la publicación del folleto de la patente:
11.10.2011

73 Titular/es: **HUAWEI TECHNOLOGIES Co., Ltd.**
Huawei Administration Building
Bantian Longgang District
Shenzhen, Guangdong Province 518129, CN

72 Inventor/es: **Li, Xixiang**

74 Agente: **Lehmann Novo, María Isabel**

ES 2 365 864 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

Un método para implementar protección de redes combinando la doble adscripción de elementos de red y la protección de redes en anillo.

Campo de la invención

- 5 La presente invención se refiere a tecnologías de protección para redes de comunicación y, en particular, a un método para proteger una red mediante una combinación de doble adscripción de elementos de red y protección de redes en anillo.

Antecedentes de la invención

- 10 Con el rápido desarrollo de la industria de las comunicaciones las redes ópticas de transporte están experimentando también profundas revoluciones. La vigorosa emergencia de servicios de datos hace que se aplique ampliamente la tecnología de MPLS (Multi-Protocol Label Switching – conmutación de etiquetas multiprotocolo) y, a nivel de red, ha habido métodos de protección de redes de transporte de datos y de doble adscripción de elementos de red.

- 15 La interconexión de redes de transporte de datos adopta a menudo el método de doble adscripción de elementos de red. Como se muestra en la figura 1, se establece una ruta para transportar un servicio entre, respectivamente, un elemento de red P y unos elementos de red A y B. Se transporta el servicio a través de la ruta de servicio (ruta de trabajo) entre el elemento de red P y el elemento de red A. Si falla el elemento de red A, se puede transportar el servicio a través de la ruta entre el elemento de red P y el elemento de red B. Normalmente, solo se utiliza la ruta entre el elemento de red P y el elemento de red A para transportar el servicio, y la ruta entre el elemento de red P y el elemento de red B puede considerarse como una ruta de protección.

- 20 La interconexión en red con doble adscripción puede proteger un servicio en funcionamiento contra influenciación del mismo debido al fallo de uno u otro de los elementos de red A, B. Por ejemplo, cuando se transporta el servicio desde el elemento de red P hasta el elemento de red A y el punto de terminación es un elemento de red E, y si falla el elemento de red A, el elemento de red P transporta el servicio por la ruta de protección hasta el elemento de red B, y el elemento de red B transporta el servicio por una red en anillo hasta un elemento de red D y luego hasta un elemento de red E. Si falla el elemento de red D, el elemento de red B transporta el servicio por la red en anillo hasta un elemento de red C y luego hasta el elemento de red E.

- 25 Para la interconexión en red con doble adscripción es necesario que un elemento de red de agregación (el elemento de red A o B) realice una copia de seguridad en caliente de 1+1. Además, puede habilitarse una conmutación de protección de un servicio cuando falle un nodo de red intermedio o una ruta de trabajo. Así, se puede ahorrar efectivamente la inversión del operador.

- 30 Se aplica generalmente un sistema MSP (Multiplexing Section Protection – protección de secciones por multiplexado) para la protección de redes en anillo. Para la protección con doble adscripción es necesario configurar en un elemento de red de enlace ascendente (el elemento de red A o B) una ruta para reenvío o transporte del servicio. En otras palabras, se reserva un ancho de banda para el servicio del elemento de red P en, respectivamente, los elementos de red de enlace ascendente A y B. La protección de redes en anillo reservará un ancho de banda de protección adicional para el servicio de los elementos de red A y B. Así, el transporte del servicio desde el elemento de red P ocupa un ancho de banda cuatro veces mayor que su ancho propio. Como se muestra en la figura 2, solamente una cuarta parte del ancho de banda total actúa para el servicio y el resto tiene que ser reservado como ancho de banda de protección para la protección del servicio.

- 35 En general, es suficiente que la protección de redes en anillo reserve adicionalmente un ancho de banda de protección idéntico al ancho de la ruta de trabajo. Sin embargo, en la técnica anterior la combinación de la doble adscripción de elementos de red y la protección de redes en anillo da como resultado un uso de solamente un cuarto de ancho de banda, y, por tanto, se produce un desperdicio del ancho de banda de la red en anillo. Si los elementos de red A y B simplemente se adscriben por vía doble a una red en anillo de más convergencia, el ancho de banda ocupado por el servicio del elemento de red P será 16 veces mayor que en la red en anillo de la capa superior.

- 40 Además, dado que no existe un mecanismo relevante de conmutación rápida previsto en la técnica anterior para la interconexión en red con doble adscripción, se obtiene típicamente una ruta de protección por reencaminamiento cuando falle un servicio de trabajo. Sin embargo, este enfoque consume tiempo y necesita un periodo de tiempo escasamente inferior a 50 ms y, por tanto no puede soportar un servicio sensible a retardos de tiempo, tal como un servicio de voz o un servicio de vídeo.

- 45 La solicitud de patente US No. US 2003/031124 A1 describe un sistema de comunicación que incluye una primera red que tiene un origen dispuesto para transmitir datos y una segunda red que tiene un destino dispuesto para recibir los datos. Se reducen las interrupciones en la comunicación entre el origen y el destino disponiendo un primer nodo primario y un primer nodo secundario en la primera red, y disponiendo un segundo nodo primario y un segundo nodo

secundario en la segunda red.

Sumario de la invención

5 La invención proporciona un método para proteger una red que incluya un primer elemento de red mediante una combinación de doble adscripción de elementos de red y protección de redes en anillo, a fin de eliminar el desperdicio de recursos de red con la combinación de doble adscripción de elementos de red y protección de redes en anillo en la técnica anterior.

En vista de lo anterior, una realización de la presente invención proporciona la solución siguiente.

Un método para proteger una red que incluye un primer elemento de red que se adscribe a un segundo elemento de red y a un tercer elemento de red en la misma red en anillo, incluyendo el método los pasos de:

10 establecer y transportar en el segundo elemento de red un servicio desde el primer elemento de red hasta el segundo elemento de red, y detectar el estado del servicio;

notificar al tercer elemento de red información de configuración del servicio del segundo elemento de red, comprendiendo la información de configuración del servicio información de recursos de la red en anillo que se asignan al servicio;

15 enviar un mensaje de conmutación al tercer elemento de red al detectar un fallo del servicio transportado del primer elemento de red al segundo elemento de red;

establecer, por el tercer elemento de red, una ruta del primer elemento de red al tercer elemento de red para conmutar el servicio hacia la ruta en respuesta al mensaje de conmutación; y

20 establecer y transportar un servicio, fallido en el tránsito del primer elemento de red al segundo elemento de red, por medio del tercer elemento de red, utilizando el recurso de la red en anillo asignado en el segundo elemento de red para el servicio fallido antes del fallo del servicio, en respuesta al mensaje de conmutación.

25 En el método anterior el paso de notificación incluye: notificar al primer elemento de red, por el segundo elemento de red, la información de configuración del servicio del segundo elemento de red mediante un mensaje de sincronización de configuración tras el establecimiento del servicio del primer elemento de red; y notificar al tercer elemento de red la información de configuración del servicio mediante el mensaje de sincronización de configuración por el primer elemento de red. Como alternativa, la información de configuración de sincronización puede enviarse al tercer elemento de red a través de un administrador de la red.

En el método anterior, si se reservan recursos de red para proteger el servicio fallido cuando el segundo elemento de red establece el servicio del primer elemento de red, se cumple entonces que:

30 a. cuando el tercer elemento de red establece el servicio fallido en el tránsito del primer elemento de red al segundo elemento de red, utilizar los recursos de la red para proteger el servicio fallido a fin de transportar el servicio, con los recursos de la red originalmente utilizados por el segundo elemento de red para transportar el servicio fallido como recursos de la red para la protección del servicio; o

35 b. cuando el tercer elemento de red establece el servicio fallido en el tránsito del primer elemento de red al segundo elemento de red, utilizar los recursos de la red originalmente utilizados por el segundo elemento de red para transportar el servicio fallido a fin de transportar el servicio, con los recursos de la red para proteger el servicio fallido como recursos de red la para la protección del servicio.

40 El método anterior incluye además: verificar, por el tercer elemento de red, la corrección e integridad de la información de configuración del servicio, así como si puede establecerse en el tercer elemento de red una ruta disponible para el servicio fallido; y, en caso de fallo de la verificación, reportar una alarma y prohibir que el servicio fallido sea conmutado al tercer elemento de red.

El método anterior incluye además: cesar el transporte del servicio fallido del primer elemento de red al segundo elemento de red al detectarse el fallo del servicio en el tránsito del primer elemento de red al segundo elemento de red.

45 La red en anillo es una red en anillo de protección de secciones por multiplexado MSP, una red en anillo de canal, una red RPR o una red RMR.

En MSP un modo de protección para la red en anillo es un modo de protección de 1+1 o 1:1.

50 Comparado con la técnica anterior, el método según la presente invención utiliza, después de la conmutación, unos anchos de banda de trabajo y protección de una red en anillo utilizados por el elemento de red antes de la conmutación y, por tanto, la doble adscripción de un elemento de red a la red en anillo da como resultado un ancho

de protección adicional asignado en la red en anillo y se puede economizar un número grande de recursos de la red en anillo. Aún cuando un elemento de red en la red en anillo se adscriba a una red en anillo de más convergencia, no se producirá una replicación del ancho de banda de protección. Además, un elemento de red utilizado para protección puede obtener información de configuración del servicio en un elemento de red de trabajo y, por tanto, puede habilitar una rápida conmutación de un servicio fallido tras la recepción de un mensaje de conmutación.

Breve descripción de los dibujos

La figura 1 es un diagrama esquemático de una doble adscripción de elementos de red en la técnica anterior;

La figura 2 es un diagrama esquemático de un ancho de banda cuádruple ocupado en una red en anillo en la técnica anterior; y

La figura 3 es un diagrama esquemático de un ancho de banda doble ocupado en una red en anillo según una realización de la presente invención.

Descripción detallada de la invención

En vista de la circunstancia de que se ocupan muchos recursos de red, tal como el ancho de banda, entre dos elementos de red para la protección de doble adscripción cuando se combinan en la técnica anterior la doble adscripción de elementos de red y la protección de redes en anillo, se establece normalmente un servicio en un elemento de red de trabajo y se asignan y reservan recursos de red en el elemento de red de trabajo, según realizaciones de la presente invención. No se asigna ni reserva ningún recurso de red en un elemento de red de protección. Solamente durante la conmutación para protección se pueden asignar y reservar los recursos de red en el elemento de red de protección a fin de proteger un servicio y un nodo de red y tener un uso eficiente del ancho de banda.

Con referencia a la figura 3, un elemento de red P se adscribe por vía doble a un elemento de red A y un elemento de red B, los cuales están ambos situados en la misma red en anillo. Un protocolo de conmutación opera respectivamente entre el elemento de red P y los elementos de red A y B. Normalmente (ambos elementos de red A y B trabajan normalmente), se establece solamente un servicio del elemento de red P en el elemento de red A. Cuando se configura en una red en anillo un ancho de banda de protección de la red en anillo, se reserva un ancho de banda de protección en la red en anillo para un servicio desde el elemento de red A hasta el elemento P. En este caso, no se establece ningún servicio del elemento de red P en el elemento de red B y no se reserva ningún ancho de banda en el elemento de red B para ningún servicio de red del elemento de red P.

Tras la detección de un fallo completo (o un fallo parcial) del servicio en tránsito del elemento de red P al elemento de red A, es decir que falla el elemento de red A o falla una línea del elemento de red P al elemento de red A, el protocolo de conmutación en funcionamiento lo notifica al elemento de red P, un procedimiento específico del cual se describe en lo que sigue.

Un protocolo para mantener un estado de conexión de ruta, tal como el protocolo OAM, opera entre los elementos de red A y P. Si falla el elemento de red A, el elemento de red P no puede recibir ningún mensaje del estado de conexión de la ruta y entonces el elemento de red P envía un mensaje de conmutación al elemento de red B informando a este elemento de red B que establezca una ruta de servicio para el elemento de red P. A continuación, el servicio originalmente transportado del elemento de red P al elemento de red A es conmutado para transporte hacia la ruta de servicio del elemento de red P al elemento de red B. Si falla la línea del elemento de red P al elemento de red A, resulta fallida la ruta de servicio del elemento de red P al elemento de red A. En el caso de un fallo en la dirección del elemento de red P al elemento de red A, este elemento de red A no puede recibir ningún mensaje del estado de conexión de la ruta y entonces el elemento de red A envía al elemento de red P un mensaje de conmutación en la dirección del elemento de red A al elemento de red P. El elemento de red P inicia una conmutación y envía un mensaje de conmutación al elemento de red B informando a este elemento de red B que establezca una ruta de servicio para el elemento de red P. A continuación, el servicio originalmente transportado del elemento de red P al elemento de red A es conmutado para transporte hacia la ruta de servicio desde el elemento de red P hasta el elemento de red B. En caso de un fallo en la dirección del elemento de red A al elemento de red P, el proceso de conmutación es similar al del caso en el que falla el elemento de red A. La conmutación unidireccional anterior puede realizarse solamente para el servicio en la dirección del fallo o para ambas direcciones al mismo tiempo, tal como la dirección de P a A y la dirección de A a P.

Después de que se establece una ruta de servicio y se asignan los recursos de red en el elemento de red A, se puede enviar una información de configuración del servicio al elemento de red B mediante un mensaje o bien por parte de una persona operadora de la red a través de un administrador de la red. Así, la información de configuración del elemento de red A se almacena en el elemento de red B, pero en este momento no se establecerá ninguna ruta de protección y no se asignará ningún recurso de la red. El elemento de red B verifica la información de configuración del servicio enviada al mismo para determinar la corrección e integridad de la información y si se puede permitir que se establezca una ruta de servicio en el elemento de red B, es decir si existe un canal, ancho de

banda u otros recursos de red apropiados que permitan la configuración para un servicio sometido a protección. Si falla la verificación, el servicio prohibirá que se conmute al elemento de red B.

El elemento de red B no configura una ruta ni asigna un recurso relacionado de ancho de banda para el servicio conmutado hasta que se reciba el mensaje de conmutación del elemento de red P. Para la asignación de la ruta y el ancho de banda se pueden utilizar una ruta de trabajo y un ancho de banda utilizados previamente por un servicio transportado del elemento de red P al elemento de red A, o bien se puede utilizar una ruta de protección de red para una protección de red en anillo, es decir que se realiza la asignación en la ruta de protección de la red en anillo en vez de ocupar un ancho de banda de repuesto del elemento de red B en la red en anillo. Después de que el elemento de red B devuelva un mensaje LISTO al elemento de red P, este elemento de red P inicia el transporte del servicio hasta el elemento de red B y deja de transportar el servicio hasta el elemento de red A. Por tanto, se puede habilitar la protección de la red en anillo y no se desperdiciará ningún ancho de banda de dicha red en anillo.

En caso de que el protocolo de conmutación en funcionamiento detecte, utilizando el mismo modo de verificación que se ha descrito en relación con el procedimiento de conmutación, que falla solamente una parte del servicio transportado del elemento de red P al elemento de red A, solamente la parte fallida del servicio se conmutará del elemento de red A al elemento de red B, y no se conmutará la parte normal del servicio. De la misma manera, solamente la parte fallida del servicio entre los elementos de red P y A será establecida y transportada en el elemento de red B, y solamente se terminará el transporte de la parte fallida del servicio desde el elemento de red P hasta el elemento de red A.

Antes de la conmutación se tiene que, para permitir que el elemento de red B utilice un ancho de banda de trabajo y un ancho de banda de protección reservados originalmente en el elemento de red A para el servicio (es decir, el servicio fallido) del elemento de red P, este elemento de red P inicia un protocolo para vigilar el estado del elemento de red A después de que este elemento de red A establece el servicio del elemento de red P, y los elementos de red A y B inician un mensaje de sincronización de configuración para la sincronización de la información de configuración. El elemento de red A informa al elemento de red P, a través del mensaje de sincronización de configuración, sobre su propia información de configuración del servicio, tal como información sobre un canal de la red en anillo, un ancho de banda o similares utilizados por el elemento de red A. El elemento de red P informa al elemento de red B, mediante el mensaje de sincronización de configuración, sobre la información de configuración del servicio del elemento de red A. El elemento de red B verifica y almacena temporalmente la información de configuración del servicio del elemento de red A. Si falla la verificación, puede reportarse una alarma a un sistema de administración de la red informando a un usuario para que intervenga. En este caso, el sistema prohíbe que se conmute el servicio al elemento de red B, y el servicio permanece en la ruta entre los elementos de red P y A. Si tiene éxito la verificación, el elemento de red B puede utilizar la ruta de trabajo original del elemento de red A en la red en anillo, ya que esa ruta está todavía integrada en la red en anillo, y se puede utilizar también la ruta de protección del elemento de red A en la red en anillo. En este caso, la ruta de la dirección de trabajo del elemento de red B utiliza una ruta de la dirección de protección del elemento de red A, y la ruta de la dirección de protección del elemento de red B utiliza la ruta de la dirección de trabajo del elemento de red A. Así, se ocupará en la red en anillo un ancho de banda solamente dos veces mayor que el del servicio del elemento de red P. De la misma manera, la ruta de la dirección de trabajo del elemento de red B puede utilizar también la ruta de la dirección de trabajo del elemento de red A, y la ruta de la dirección de protección del elemento de red B utiliza la ruta de la dirección de protección del elemento de red A. Así, se ocupará en la red en anillo un ancho de banda solamente dos veces mayor que el del servicio del elemento de red P.

Según una realización de la presente invención, la red en anillo puede ser un anillo MSP, un anillo de canal, un RPR (Resilient Packet Ring – anillo de paquete resiliente) o un RMR (Resilient MPLS Ring – anillo MPLS resiliente), etc. Durante la conmutación de doble adscripción, un método para configurar recursos de red en el elemento de red B puede depender de un método para proteger la red en anillo. Por ejemplo, el anillo MSP utiliza un segmento de tiempo de protección, el anillo de canal utiliza un canal de protección, el RPR utiliza un flujo en la dirección de protección y emplea un ancho de banda dependiente del nivel del servicio, y el RMR utiliza un LSP de protección.

Con un método de protección de 1+1 para el MSP, se puede utilizar un segmento de tiempo reservado en el elemento de red B durante la conmutación de doble adscripción, y con un método de protección de 1:1 se puede dejar caer durante la conmutación de doble adscripción un servicio adicional más allá del segmento de tiempo reservado.

Como puede verse por lo anterior, las realizaciones de la invención son ventajosas al menos en los aspectos siguientes.

1. Se asigna un ancho de banda solamente al elemento de red A con un servicio en funcionamiento, y no se asigna ningún ancho de banda al elemento de red B, que no tiene ningún servicio en funcionamiento y se encuentra en una condición de protección.

2. La información de configuración del servicio del elemento de red A se almacena en el elemento de red B en una condición de protección, y el establecimiento de la configuración y la asignación de recursos de red son

desencadenados por el mensaje de conmutación.

3. Después de que se inicie la protección de doble adscripción, el servicio del elemento de conmutación P es conmutado del elemento de red A al elemento de red B. Se establece el servicio del elemento de red en el elemento de red B, el cual a su vez recibe el servicio del elemento de red P. Así, se puede habilitar la protección de doble adscripción.

5 4. El elemento de red B utiliza los anchos de banda de protección de la banda de trabajo originalmente utilizados por el elemento de red A para establecer el servicio.

10 5. Dado que se establece un servicio y se asigna un ancho de banda de la red en anillo para el elemento de red B solamente durante la conmutación de doble adscripción, la doble adscripción del elemento de red a la red en anillo no dará como resultado un ancho de banda de protección adicional asignado en la red en anillo.

6. Dado que no se establece un servicio de protección ni se asigna un ancho de banda de protección para el elemento de red B que opera normalmente, la doble adscripción de los elementos de red A y B a la red en anillo de más convergencia no dará como resultado una replicación del ancho de banda de protección.

15 Aunque las realizaciones preferidas de la presente invención han sido descritas de la manera anterior, el alcance de la presente invención no deberá limitarse a ellas y los expertos en la materia pueden hacer diversos cambios y modificaciones en las realizaciones sin apartarse del alcance de la presente invención. Se pretende que todas las variaciones y modificaciones caigan dentro del alcance de la presente invención, que deberá ser meramente como se define en las reivindicaciones de este documento.

REIVINDICACIONES

- 5 1. Un método para proteger una red mediante una combinación de doble adscripción de elementos de red y protección de redes en anillo, comprendiendo la red un primer elemento de red (P) que se adscribe a un segundo elemento de red (A) y a un tercer elemento de red (B) en la misma red en anillo, comprendiendo el método los pasos de:
- establecer y transportar en el segundo elemento de red (A) un servicio enviado del primer elemento de red (P) al segundo elemento de red (A), y detectar el estado del servicio;
- 10 notificar al tercer elemento de red (B) una información de configuración del servicio del segundo elemento de red (A), comprendiendo la información de configuración del servicio una información de recursos de red de la red en anillo que se asignan al servicio;
- enviar un mensaje de conmutación al tercer elemento de red (B) tras la detección de un fallo del servicio enviado del primer elemento de red (P) al segundo elemento de red (A);
- 15 establecer, por el tercer elemento de red (B), una ruta del primer elemento de red (P) al tercer elemento de red (B) para conmutar el servicio hacia la ruta en respuesta al mensaje de conmutación; y
- establecer y transportar, por el tercer elemento de red (B), un servicio fallido enviado del primer elemento de red (P) al segundo elemento de red (A), mediante la utilización del recurso de la red en anillo asignado en el segundo elemento de red (A) para el servicio fallido antes del fallo del servicio, en respuesta al mensaje de conmutación.
2. El método según la reivindicación 1, en el que el paso de notificación comprende:
- 20 notificar al primer elemento de red (P), por el segundo elemento de red (A), la información de configuración del servicio del segundo elemento de red (A) mediante un mensaje de sincronización de configuración tras el establecimiento del servicio enviado del primer elemento de red (P) al segundo elemento de red (A); y
- notificar al tercer elemento de conmutación (B), por el primer elemento de red (P), la información de configuración del servicio mediante el mensaje de sincronización de configuración.
- 25 3. El método según la reivindicación 1, en el que el paso de notificación comprende enviar, por el segundo elemento de red (A), la información de configuración del servicio al tercer elemento de red (B) a través de un administrador de red tras la el establecimiento del servicio enviado del primer elemento de red (P) al segundo elemento de red (A).
4. El método según una cualquiera de las reivindicaciones 1 a 3, en el que si se reservan recursos de red para protección del servicio cuando el segundo elemento de red (A) establece el servicio enviado del primer elemento de red (P) al segundo elemento de red (A), se cumple entonces que:
- 30 el tercer elemento de red (B) utiliza los recursos de red reservados para transportar el servicio, con los recursos de red originalmente utilizados por el segundo elemento de red (A) para transportar el servicio fallido como recursos de red para la protección del servicio; o
- el tercer elemento de red (B) utiliza para transportar el servicio los recursos de red originalmente utilizados por el segundo elemento de red (A) para transportar el servicio fallido, con los recursos de red reservados como recursos de red para la protección del servicio.
- 35 5. El método según la reivindicación 2, que comprende además:
- verificar, por el tercer elemento de red (B), la corrección e integridad de la información de configuración del servicio, así como si puede establecerse en el tercer elemento de red (B) una ruta disponible para el servicio fallido; y
- 40 en caso de fallo de la verificación, reportar una alarma y prohibir que se conmute el servicio fallido al tercer elemento de red (B).
6. El método según la reivindicación 1, que comprende dejar de transportar el servicio fallido desde el primer elemento de red (P) hasta el segundo elemento de red (A) al detectarse el fallo del servicio enviado del primer elemento de red (P) al segundo elemento de red (A).
- 45 7. El método según la reivindicación 1, en el que la red en anillo es una red en anillo de protección de secciones por multiplexado, una red en anillo de canal, una red en anillo de paquete resiliente o una red en anillo MPLS resiliente.
8. El método según la reivindicación 7, en el que en una red MSP un modo de protección para la red en anillo es un modo de protección de 1+1 o 1:1.

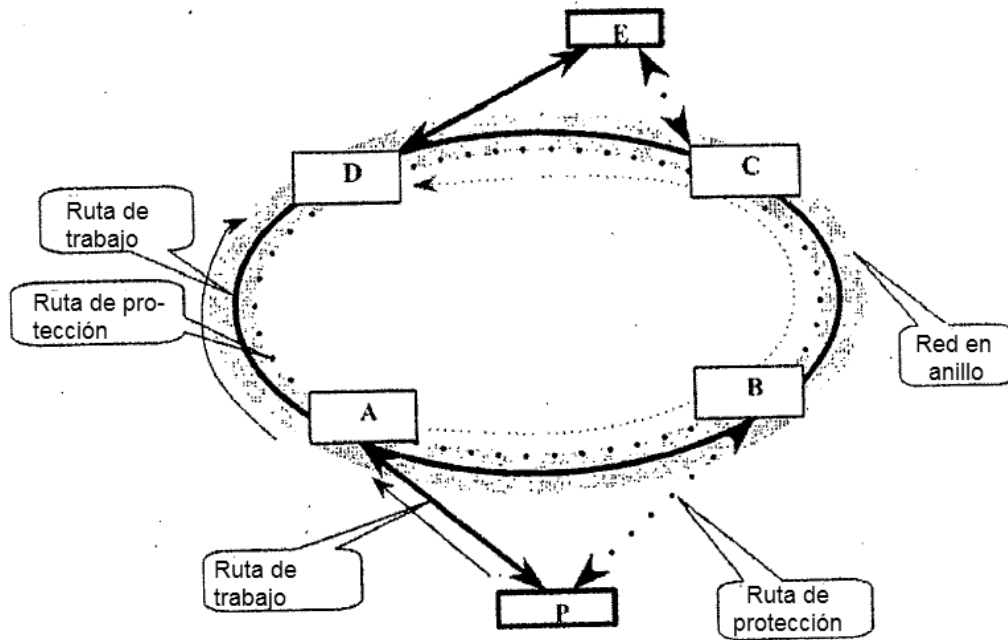


FIG.1

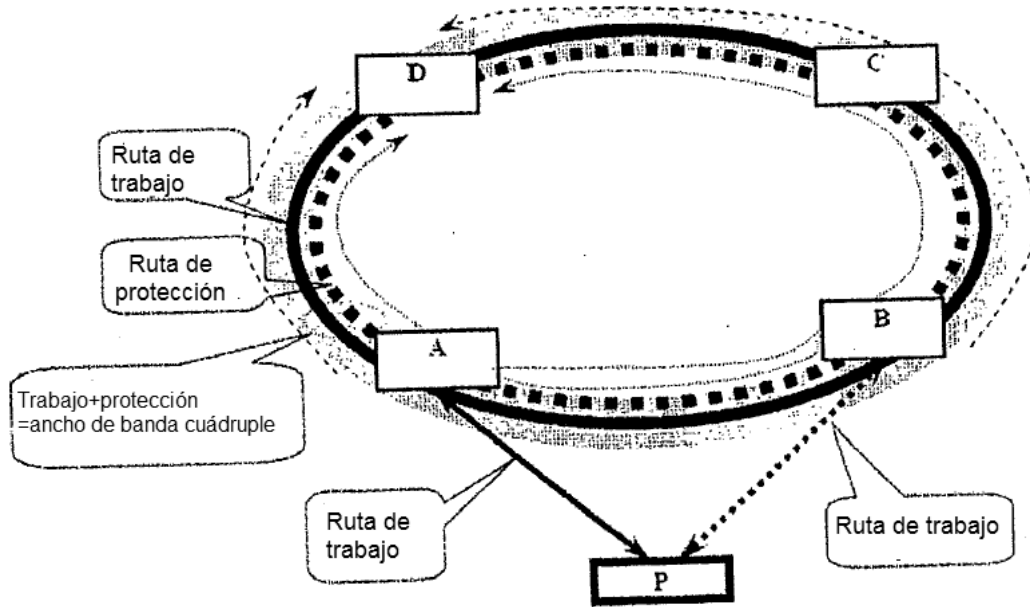


FIG.2

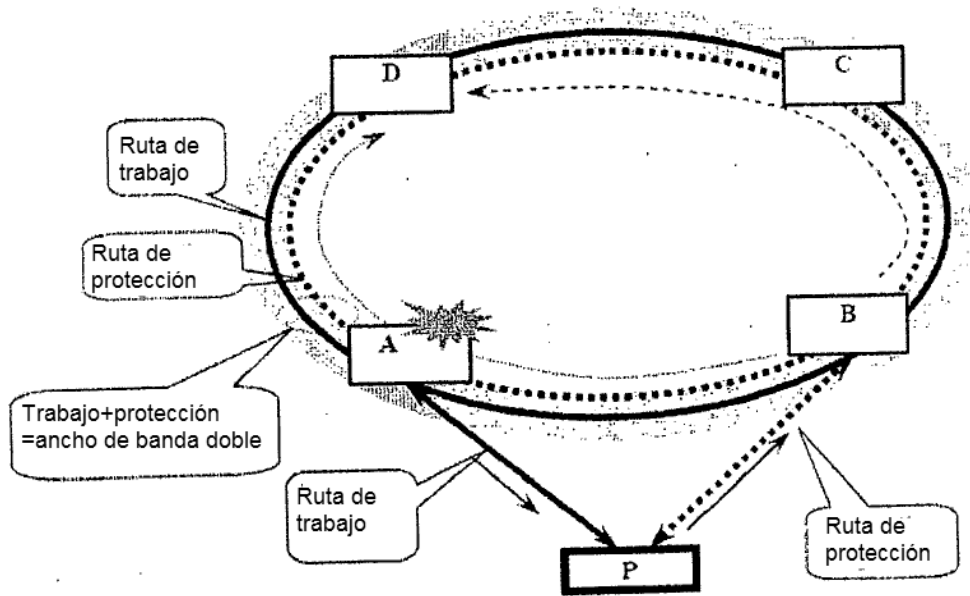


FIG.3