(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 345 714**

(51) Int. Cl.:
H04J 3/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03817939 .6**
(96) Fecha de presentación : **05.08.2003**
(97) Número de publicación de la solicitud: **1652325**
(97) Fecha de publicación de la solicitud: **03.05.2006**

(54) Título: **Método para proporcionar rutas de tráfico adicional con protección de la conexión en una red de comunicación, y producto de programa informático y red relacionados con lo mismo.**

(45) Fecha de publicación de la mención BOPI:
30.09.2010

(45) Fecha de la publicación del folleto de la patente:
30.09.2010

(73) Titular/es: **TELECOM ITALIA S.p.A.**
Piazza degli Affari 2
20123 Milano, IT

(72) Inventor/es: **Allasia, Andrea;**
Rita, Roberto;
Serra, Laura y
Varetto, Luigi Giuseppe

(74) Agente: **Ponti Sales, Adelaida**

DESCRIPCIÓN

Método para proporcionar rutas de tráfico adicional con protección de la conexión en una red de comunicación, y producto de programa informático y red relacionados con lo mismo.

Campo de la invención

La presente invención se refiere a redes de telecomunicaciones y fue desarrollada prestando especial atención a su posible aplicación a las arquitecturas en anillo en redes de Jerarquía Sincrónica Digital (SDH, de sus siglas en inglés) del tipo que comúnmente es designado como MS-SPRing (Anillo de Protección de la Sección del Multiplexor).

Sin embargo, la referencia a este posible campo de aplicación no tiene que entenderse como el único de aplicación de la invención.

Descripción de la técnica relacionada

Las redes de transmisión a larga distancia proporcionan una amplia variedad de diferentes servicios de telecomunicaciones, como voz y datos de Internet o líneas de alquiler a diferentes velocidades.

Estas redes incluyen generalmente una pluralidad de nodos, cada uno situado normalmente en una ciudad u otro lugar de tráfico alto, emparejados juntos en un bucle cerrado en una arquitectura en malla/anillo, por ejemplo: por cables de fibra óptica. La información viaja por la fibra de acuerdo a estándares de transmisión óptica como por ejemplo: los que comúnmente se conocen como Red Óptica Sincrónica (SONET, de sus siglas en inglés) o red de Jerarquía Digital Sincrónica (SDH, siglas en inglés).

En las arquitecturas en anillo, se puede llevar a cabo fácilmente la protección del tráfico creando dos enlaces separados sobre el bucle destinando el primero al flujo normal y el segundo a la protección, para así asegurar el servicio cuando ocurra un fallo en el primer enlace.

Esta disposición de protección es comúnmente designada protección de conexión de sub-red (SNCP, de sus siglas en inglés). En este tipo de disposición de protección no existen mecanismos para coordinar ambos extremos del enlace. Esto significa que no hay un protocolo específico para intercambiar información entre terminaciones de protección al respecto de los estados “conmutador” y “puente” (por ejemplo: protección).

Una posible implementación de un esquema de protección de conexión de sub-red implica dos equipos que llevan el tráfico a lo largo de una determinada infraestructura (p. ej. un anillo). El elemento de red en el extremo origen del tramo de protección transmite por el canal protegido sobre los dos lados del anillo como un grupo de protección. El elemento de red en el extremo receptor del tramo de protección hace salir el grupo de protección recibido como elección de los “mejores” lados dependiendo del criterio de conmutación. En caso de que no se detecten defectos en las señales de recorrido/SNC (conexión de sub-red), estas señales se seleccionarán como las señales normales. Los recorridos/SNCs seleccionados por el extremo receptor son denominados SNCs/recorridos activos, mientras que los otros son denominados SNCs/recorridos en espera.

Los esquemas de protección de recorrido existen (como el esquema designado Protección de la Sección del Multiplexor o MSP) de tal modo que ofrecen la posibilidad de utilizar un protocolo de banda para sincronizar ambas terminaciones. Esta característica se puede explotar para establecer canales adaptados para ser enrutados a través del recorrido/sección/ruta en condición de espera. Las señales transmitidas sobre tales canales son llamadas normalmente tráfico adicional (ET siglas en inglés), ver p. ej. ETSI EN 300 417-1-1, v1.2.1, (2001/10), “Transmission multiplexing; generic requirements of transport functionality of equipment; Parte1-1: generic process and performance; página 18.

Un esquema de protección denominado MS-SPring se puede implementar por medio de Anillo con Protección Compartida de la Sección del Multiplexor de dos o cuatro fibras (MS-SPRing). En cada tramo, la mitad de la capacidad (con uno o dos pares de fibras) está dedicada a los canales “de funcionamiento” y la otra mitad a los canales “de protección”. El tráfico puede fluir en el anillo en el sentido de las agujas del reloj o en sentido contrario. En caso de fallo de una sola fibra, se aplicará el esquema de protección de tramo, y el tráfico se re-enrutará a lo largo del tramo de protección adyacente al que ha fallado. En caso de fallos de segundo orden (p. ej. fallos en las fibras de protección o funcionamiento o fallos de nodo) se implementa un esquema de protección del anillo y el tráfico es re-enrutado a lo largo del lado del anillo que no ha fallado.

La figura 1 incluye cuatro porciones designadas de a) a d) respectivamente, y de forma esquemática representa la operación de un esquema de protección MS-SPRing típico que implica cuatro nodos designados como a, n1, n2, y Z.

En la figura 1, se muestran las fibras “de funcionamiento” y de “protección”, las fibras de protección se representan mediante áreas discontinuas y los fallos mediante aspas.

En concreto, en la figura 1 se muestran las siguientes cuatro condiciones:

- (a) operación normal;
- (b) protección de tramo activa;
- (c) protección de anillo contra fallo de tramo doble y;
- (d) protección de anillo contra aislamiento de nodo.

Además del algoritmo de protección MS-SPRing normal (que ofrece canales protegidos con altos niveles de prioridad), existe la posibilidad de explotar canales de tráfico desprotegido no apropiable (NUT, siglas en inglés) para ofrecer un nivel de prioridad intermedio y canales de tráfico adicional (ET) teniendo niveles de baja prioridad.

En particular, algunos canales de protección y de funcionamiento en una disposición MS-SPRing se pueden utilizar para llevar NUT, con el tráfico no-protegido viajando en canales en rutas de protección y de funcionamiento del anillo. En caso de fallo, estos canales no se pueden cortar para soportar la protección del tráfico normal.

En esquemas de protección bi-direccionales, donde está disponible un protocolo de coordinación de terminación, la banda normalmente reservada a la protección se puede explotar para llevar tráfico adicional cuando el canal de protección está en modo de espera. Obviamente, cuando se da un fallo en la ruta de funcionamiento, y el esquema de protección conmuta de la ruta de funcionamiento a la de protección, el canal de tráfico adicional es interrumpido y su recuperación no se garantiza.

Tal y como se muestra en la figura 2, una arquitectura de protección 1+1 tiene una señal de tráfico normal, un SNC/recorrido de funcionamiento, un SNC/recorrido de protección y un puente permanente.

Una arquitectura de protección m:n tiene señales de tráfico normal n, SNCs/recorridos de funcionamiento n y SNCs/recorridos de protección m. Las señales en los SNCs/recorridos de funcionamiento son las señales de tráfico normal. La señal en un SNC/recorrido es o bien una de las señales de tráfico normal, una señal de tráfico adicional, o una señal nula. En el extremo origen, cualquiera de las señales mencionadas se pueden conectar a los SNCs/recorridos de protección. En el extremo receptor, las señales provenientes de los SNCs/recorridos de funcionamiento se seleccionan como señales de tráfico normal. En caso de condición defectuosa en un SNC/recorrido en funcionamiento, la señal transportada se enruta sobre uno de los SNCs/recorridos de protección. En el extremo receptor, la señal proveniente de este SNC/recorrido de protección es entonces seleccionada en su lugar.

La recomendación UIT-T G.841 “Series G: Transmission systems and media, digital systems and network- Types and characteristics of SDH network protection architectures”, de octubre de 1998 indica que se puede alcanzar una diferenciación más en los niveles de prioridad al considerar un mecanismo de protección de conexión de sub-red parcialmente embebido en un MS-SPRIng utilizando NUT En otras palabras, el NUT se puede proteger a lo largo de un MS-SPRing con la implementación de una ruta de Protección de Conexión de Sub-red (SNCP). Este tipo de protección preserva el NUT de fallos dobles sobre un tramo.

Los canales NUT se encuentran, sin embargo, afectados por dos desventajas principales, a saber:

- para usar un canal de NUT, es necesario crear más rutas de las necesarias; por ejemplo, para un canal de NUT en el ancho de banda de funcionamiento, es necesario dedicarle el número uno de ranura de todos los tramos de protección y de funcionamiento que forman el anillo;
- para crear un enlace no planeado en una configuración de NUT, es necesario realizar una nueva puesta en marcha del anillo.

En WO-A-02/073903 se revela una disposición para lograr una diferenciación en la disponibilidad a través de la definición de una tecnología diferente también conocida como tecnología de Anillo Resistente de Paquetes (RPR, de sus siglas en inglés). En esta disposición, se obtienen diferentes niveles de disponibilidad al definir tres clases de servicio, cada uno con un nivel de prioridad diferente. Las tres clases de tráfico son las siguientes: trafico protegido (es decir alta prioridad), tráfico desprotegido (es decir prioridad media); y tráfico interrumpible (es decir baja prioridad).

La principal desventaja de esta solución es que los operadores que deseen desarrollar instalaciones de redes para hacer uso de diferentes niveles de servicio se encontrarán inevitablemente forzados a cambiar el equipo, suponiendo un gran impacto en los gastos de capital.

El documento WO-A-01/030006 describe una variante de esquema de protección SNCP tratado anteriormente proporcionando otra implementación de un esquema de protección 1+1. En concreto, se sugiere la posibilidad de llevar a cabo señales de tráfico adicional no enrutado y desprotegido en la ruta de protección de un esquema de protección de sub-red 1+1, cuando el recorrido de protección está en condición de espera.

El documento EP 1 014 611 desvela un método para optimizar, en presencia de un fallo, la disponibilidad de canales de baja prioridad en una red transoceánica de fibra óptica de transmisión. En particular el método asegura la selección de canales de baja prioridad que pueden ser mantenidos y que no son interrumpidos en beneficio del tráfico de alta prioridad, llevando a cabo la conmutación sobre aquellos otros canales de baja prioridad realmente necesarios para proporcionar temporalmente tráfico de alta prioridad en caso de fallo.

Objeto y resumen de la invención

Por consiguiente, existe la necesidad de disposiciones mejoradas que puedan ser adaptadas para crear rutas con diferentes niveles de disponibilidad que prescindan de las desventajas intrínsecas en la disposición de la técnica previa, anteriormente tratada.

El objeto de la presente invención consiste, en efecto, en proporcionar tal disposición mejorada.

De acuerdo a la invención, se logra tal objeto por medio del método que tiene las características que se exponen en las reivindicaciones que siguen. La invención está relacionada con el sistema correspondiente, además de con el producto de programa informático correspondiente que se puede cargar en la memoria de al menos un ordenador y las porciones de código de software que lo componen, para realizar los pasos del método de la invención cuando el producto es ejecutado en al menos un ordenador. La referencia de "al menos uno" se propone para destacar la posibilidad de que la disposición de la invención pueda ser llevada a cabo de forma descentralizada.

Una realización preferida de la invención se basa en la forma mejorada de proteger los canales de tráfico adicional (ET), al explotar un esquema de protección de conexión de sub-red aplicado a la arquitectura MS-SPRing.

La protección se basa en los principios que subraya el modelo funcional del Sector de Normalización de las Comunicaciones (UIT-T) en su Recomendación G.803.

Tal y como se usa aquí, el significado propuesto de "protección de conexión de sub-red" no se limita a la disposición específica comúnmente identificada con el acrónimo SNCP, sino que también se extiende a esquemas de protección equivalentes como p. ej. aquellos conocidos como MS-SPRing, Restablecimiento y Conmutación Multi-protocolo mediante etiquetas (MPLS) o la MPLS Generalizada.

Dicho esquema de protección hace preferiblemente uso de capacidad pre-asignada entre nodos. La arquitectura más simple tiene capacidad de protección 1 y de funcionamiento 1, la arquitectura más compleja tiene capacidades de funcionamiento n y capacidades de protección m (m:n), respectivamente.

La disposición descrita aquí ofrece la posibilidad de crear un servicio protegido de ruta utilizando dos canales de tráfico adicional (ET) de baja prioridad, presente en una disposición de MS-SPRing de cuatro fibras. Los canales de tráfico adicional pueden ser protegidos en una estructura MS-SPRing al doblar el canal de tráfico adicional a lo largo de los lados del anillo en el sentido de las agujas del reloj y a la inversa, y, al aplicar un protocolo de protección de conexión de sub-red.

Esta estrategia de protección ofrece una oportunidad para diferenciar más los niveles de prioridad del servicio. De hecho, la protección de conexión de sub-red en los canales de tráfico adicional permite la recuperación de tal tráfico de baja prioridad en caso de un fallo aislado a lo largo de cualquier tramo del anillo. Como consecuencia, se logra un nuevo nivel intermedio de protección entre los niveles asegurados por el NUT y por el NUT protegido de SNCP.

Como se indicó, los canales NUT tienen dos desventajas principales, a saber:

- para usar un canal de NUT, es necesario crear más ancho de banda de la necesaria, para un canal de NUT en el ancho de banda de funcionamiento, la ranura "número uno", ranura de todos los tramos de protección y de funcionamiento formando el anillo se debe dedicar a ello, y

- para crear un enlace no planeado en una configuración de NUT, es necesario realizar una nueva puesta en marcha del anillo.

En referencia a las desventajas de los canales de NUT descritos en la sección previa, el tráfico adicional no reserva de forma permanentemente un canal a lo largo de la ruta de protección.

La disposición aquí descrita es independiente de la tecnología. Esto significa que existen sólo dos requerimientos básicos para el protocolo de red de la transmisión, a saber:

- tener una forma de protección de circuito; y

- tener la posibilidad de configurar trafico de prioridad baja con respecto al que es protegido normalmente.

La correspondencia entre las capacidades de la protección de conexión de sub-red y la ruta de prioridad baja se puede conseguir o bien en el mismo equipo de red o bien en un equipo diferente. En otras palabras, casi todos los

equipos de red que tienen capacidades de tráfico de prioridad baja están adaptados para usar la combinación con la protección SNCP.

Por medio de comparación directa, mientras la disposición mostrada en WO-A-01/030006 revela la posibilidad de transportar tráfico adicional sobre un esquema de protección SNCP 1+1 (que i.a. no es descrito en documentos normativos), en la disposición descrita aquí, la ruta de protección de un esquema MS-SPRing es explotada para llevar señales de tráfico adicional y se muestra un método para proteger el ET mediante un esquema de implementación SNCP 1+1.

Una realización preferida de la disposición aquí revelada proporciona en efecto rutas de tráfico adicional en una red de comunicación incluyendo al menos dos canales de protección asociados a su respectivos canales de transmisión.

Cada canal de protección admite:

- un estado activo para llevar, en presencia de un fallo en el mencionado canal de transmisión asociado, tráfico para ser transportado por el canal de transmisión asociado, y

- un estado de espera, en el que el canal de protección se adapta para llevar tráfico adicional.

Los canales de protección se ejecutan en un esquema de protección de conexión de sub-red, por medio del cual uno de los canales de protección en su estado de espera se adapta para asegurar la recuperación del trafico adicional transportado por el otro canal de protección, mientras el otro canal de protección es conmutado a su estado activo o está sujeto a fallo.

Las realizaciones preferidas de la disposición desvelada aquí proporcionan:

- al menos una estructura de anillo incluyendo rutas no coextensivas y asociando los al menos dos canales de protección a las rutas no coextensivas respectivas en el anillo (es decir, recurriendo a lo que es comúnmente designado como “diversidad de enrutamiento”, y

- una pluralidad de estructuras en anillo y asociando los al menos dos canales de protección a sus respectivos anillos diferentes de la pluralidad de anillos.

Breve descripción de los dibujos

Ahora se describirá la invención, por medio únicamente de ejemplos, al referirse a las figuras de dibujo adjuntas, en las que:

las figuras 1 y 2 relacionadas con la técnica anterior, han sido descritas previamente,

la figura 3 muestra una ruta protegida SNCP a través de dos canales de tráfico adicional entre dos nodos diferentes,

la figura 4 muestra una disposición de anillo implementando un esquema de protección de MS-SPRing de cuatro fibras,

las figuras 5 y 6 muestran dos posibles circunstancias de fallo ocurriendo en la disposición de la figura 4

la figura 7 muestra dos canales de tráfico adicional protegidos con un esquema de protección de conexión de sub red,

la figura 8 muestra una disposición alternativa a la disposición de la figura 7,

las figuras 9 y 10 muestran varias disposiciones para la diferenciación de enrutamiento sobre dos anillos,

las figuras 11, 12 y 13 muestran varias configuraciones para la evaluación de disponibilidad/indisponibilidad,

la figura 14 es una representación general de tráfico adicional protegido por medio de un esquema de protección de conexión de sub-red.

Descripción detallada de la realización preferida de la invención

La figura 3 del dibujo es una representación de una ruta protegida SNCP entre dos equipos 10 y 12.

Una red troncal basada en una arquitectura interconectada de anillo con protección MS-SPRing de cuatro fibras puede ofrecer una amplia cartera de servicios de red basada en diferentes niveles de disponibilidad. La disposición descrita aquí aumenta las posibilidades de diferenciación de nivel de servicio en una red SDH de MS-SPRing.

Esta disposición es esencialmente la aplicación del esquema de protección de SNCP para los canales de tráfico adicional A, B en una red N extendiéndose entre dos equipos 10 y 12. Los dos canales de tráfico adicional A y B se envían a lo largo de los recorridos de protección y funcionamiento de una arquitectura de protección SNCP. En concreto, la figura 4 muestra una ruta protegida de SNCP incluyendo dos canales de tráfico adicional entre dos nodos diferentes 10 y 12.

La figura 4 muestra una arquitectura de esquema de protección MS-SPRing de cuatro fibras, con tráfico adicional en el ancho de banda de las secciones de protección.. En concreto, la figura 4 (y las figuras 5 a 8 también) se refieren a una disposición en anillo proporcionada entre dos nodos 100, 200, incluyendo su respectivos módulos de control de intercambio de datos (DXC, siglas en inglés) e incluyendo cuatro multiplexores de inserción/extracción de ADM1 a ADM4 (siglas en inglés). Se describen dos canales de tráfico adicional, enrutados en los dos lados opuestos del anillo.

En el anillo con esquema de protección de MS-SPRing de cuatro fibras, el ancho de banda de las rutas de protección se puede dedicar al tráfico adicional, tal y como se muestra con dos canales de tráfico adicional, en los dos lados opuestos del anillo. Las rutas terminan en dos conexiones cruzadas digitales.

La figura 5 muestra la interrupción del canal número 1, cuando se da un fallo de tramo, con el canal número 2 funcionando con normalidad y el estado de dos canales de tráfico adicional en caso de que la protección de tramo: ruta número 1 esté apagada porque la ruta de protección se utiliza para la protección de tramos de tráfico normal, mientras que la ruta número 2 está en servicio regularmente.

La figura 6 muestra interrupción de los canales número 1 y número 2 cuando se da un doble fallo de tramo. El anillo funciona en modo de protección de anillo, en el que ambas rutas de tráfico han sido interrumpidas para permitir el re-enrutamiento del tráfico de alta prioridad.

La disposición del nivel de servicio comúnmente requiere que, cuando se da esta condición de fallo, los equipos y/o las fibras del anillo deben de estar reparados en unas pocas horas (normalmente en menos de un día laborable).

Como ya se mencionó anteriormente, en referencia a los canales de NUT, se debe lograr más diferenciación en los niveles de prioridad gracias a una solución compuesta, utilizando los canales de NUT en un MS-SPRing de cuatro fibras con un esquema de protección de conexión de sub-red superpuesto. En otras palabras, el NUT se puede proteger a lo largo de un MS-SPRing con la implementación de una ruta de protección de conexión de sub-red. Este tipo de protección preserva el NUT de fallos dobles a lo largo de un tramo.

Las diferentes soluciones analizadas hasta ahora no están exentas de ciertos aspectos críticos.

Los canales de NUT permiten ambos canales, protegido y desprotegido en la misma infraestructura pero, cuando un anillo está en la fase de puesta en marcha, necesita planear con exactitud los requerimientos del ancho de banda porque cualquier diferencia implica una nueva fase de vuelta a poner en marcha, con el objetivo de optimizar el ancho de banda del anillo reutilizado.

La protección de conexión de sub-red de los canales de NUT implica que, en la fase de planes de la red, p. ej.: en la fase de puesta en marcha del anillo, los canales de NUT requieran llevar a cabo demandas de trafico que deben ser definidas. Para solo una demanda de trafico es necesario definir una ranura para el anillo entero como NUT (esto implica que el ancho de banda encontrado es mayor que el que es usado efectivamente).

El uso de canales de tráfico adicional en una infraestructura MS-SPRing ofrece un nivel de disponibilidad que es mucho más bajo en comparación con los canales protegidos. Además, la disponibilidad del tráfico adicional también se ve afectada por largos periodos de interrupción debido a actividad de mantenimiento planeada.

Una realización preferida de la disposición descrita aquí ofrece la posibilidad de crear a) un servicio protegido de ruta utilizando dos canales de tráfico adicional (ET) de baja prioridad presentes en un MS-SPRing de cuatro fibras.

Tal y como se trató previamente, en el caso de NUT, los canales de tráfico adicional pueden estar protegidos en una estructura de MS-SPRing al doblar el canal de tráfico adicional a lo largo de los lados del anillo en el sentido de las agujas del reloj o a la inversa y al aplicar un protocolo de protección de conexión de red.

Este esquema de protección ofrece una oportunidad para diferenciar más los niveles de prioridad del servicio. De hecho, la protección de conexión de sub-red en los canales de tráfico adicional permite la recuperación del tráfico de baja prioridad en caso de un fallo asilado a lo largo de cualquier tramo del anillo.

La evaluación de la disponibilidad muestra que el nivel de protección obtenido es más elevado que en el caso de canales NUT simples (esto ocurre porque la ruta está protegida en dos vías diferentes del anillo) pero más bajo con respecto al NUT protegido de SNCP.

En comparación con la implementación de NUT, una ventaja de utilizar canales de tráfico adicional con el esquema de protección de conexión de sub-red se encuentra a la hora de planear la capacidad del anillo para servicios de trafico adicional, por lo que una actividad de puesta en marcha no es requerida en cualquier momento que un canal de trafico adicional vaya a ser suministrado.

En este contexto, al menos dos realizaciones son posibles, a saber:

- dos canales de trafico adicional protegidos con un esquema de protección de conexión de sub-red habiendo realizado la función puente/selector en los mismos multiplexores de inserción/extracción (ADMs) que forman el anillo; y

- dos canales de tráfico adicional protegidos con un esquema SNCP habiendo realizado la función puente/selector en las conexiones cruzadas digitales (p. ej. DXCs, en inglés).

En concreto, la figura 7 muestra dos canales de trafico adicional protegidos con un esquema de protección de conexión de sub-red habiendo realizado la función puente/selector en los mismos multiplexores de inserción/extracción (ADMs) que forman el anillo.

A la inversa, la figura 8 muestra dos canales de trafico adicional protegidos con un esquema de protección de conexión de sub-red habiendo realizado la función puente/selector en las conexiones digitales cruzadas (DXCs).

En la implementación del esquema de protección de conexión de sub-red sobre los multiplexores de inserción/extracción (ADMs) formando la infraestructura del anillo que lleva los patrones del tráfico, se crea un punto de finalización de sub-red que incluye dos rutas de trafico adicional sobre los lados opuestos del anillo como se representa en la Figura 4.

En la implementación del esquema de protección de tráfico adicional de conexión de sub-red sobre los DXCs, el equipo representa la finalización de la ruta, en un dominio de red específico, de una ruta creada por dos sub-rutas de trafico adicional protegidas a través de un esquema de protección de conexión de sub-red. En este último caso, existen diferentes posibilidades para establecer servicios de tráfico adicional, que dependen de la estrategia de enrutamiento aplicada a la infraestructura (p. ej. enrutamiento a través de un número mínimo de anillos).

En concreto pueden aparecer las siguientes situaciones:

- en el caso de rutas de tráfico adicional protegidas a través del algoritmo SNCP sobre un único anillo; como se describió anteriormente, el mecanismo de la SNCP puede configurarse sobre los ADMs mientras que la infraestructura del anillo hace uso de las rutas de ET en diversidad de enrutamiento (ver de nuevo figura 7);

- en el caso de que las rutas de tráfico adicional protegidas a través del algoritmo de protección de conexión de sub-red sobre el mismo anillo, el mecanismo de protección de conexión de sub-red se puede configurar sobre las DXCs como variante del esquema previo (ver, al respecto, la figura 8);

- en el caso de rutas de tráfico adicional protegidas a través del algoritmo de SNCP sobre diferentes anillos, el mecanismo de conexión de la sub-red se puede configurar sobre la DXC y la infraestructura del anillo debe ser representada como rutas de tráfico adicional llevado sobre dos anillos diferentes que pertenecen a la misma clase (es decir un número de anillo “uno” un O, un anillo número “dos”).

Las rutas de tráfico adicional también se pueden llevar sobre dos anillos que pertenezcan a diferentes clases de anillos (es decir un anillo número “uno” de clase A y un anillo número “uno” de clase B).

Al respecto de esta última opción mencionada, es importante entender que esta estrategia logra una mejor en términos de capacidad de supervivencia y, en concreto, ofrece un nivel de protección bueno cuando una actividad de mantenimiento planeada afecta a la condición de operatividad de una de las rutas de tráfico adicional usadas en el esquema de protección SNCP.

Para conseguir la máxima ventaja teorética desde las rutas de tráfico adicional llevadas a cabo sobre dos anillos diferentes de la misma clase, las rutas de protección y funcionamiento están planeadas en diferente enrutamiento. Si el enrutamiento diferente se representa por dos anillos que pertenecen a la misma clase (sobre la misma infraestructura de cable se hace uso de dos o más sistemas de anillos diferentes, a. Una forma de obtener diversificación de enrutamiento es enrutar una ruta de tráfico adicional en uno de los lados del primer anillo y el segundo tráfico adicional en el lado opuesto del segundo anillo. Esto significa que solo dos fallos sobre el mismo tramo (funcionamiento y protección) puede llevar a un apagado de la condición de servicio.

En concreto, la figura 9 muestra la diferenciación de enrutamiento sobre dos anillos de la misma clase, lo conlleva una ventaja significativa desde la protección de trafico adicional a través del esquema de protección de conexión de la sub-red.

En caso de rutas de tráfico adicional llevadas a cabo sobre dos anillos que pertenezcan a diferentes clases de anillos, es posible una diversificación completa de enrutamiento (es decir, diferentes equipos e infraestructuras), para que el nivel de disponibilidad llegue a su máximo.

A este respecto, la figura 10 muestra la diferenciación de enrutamiento sobre dos anillos de la misma clase, lo que lleva a una ventaja significativa desde la protección de trafico adicional a través del esquema de protección de conexión de la sub-red.

Se agradecerá que dos ADMs adicionales (a saber ADM5 y ADM6) se muestren en el anillo número uno de clase Y para destacar que la estructura del anillo considerada aquí pueda incluir cualquier número de equipos de red tal y como se proporciona en la especificación UIT-T G.841.

A continuación se muestra un estudio de investigaciones realizadas en una estructura de anillo interconectando dos lugares geográficos (de nuevo designados como 100 y 200 con dos rutas diferentes con nombre dirección roja (R) y dirección azul (B).

Las figuras de indisponibilidad de NUT y los canales de tráfico adicional (ET) se han calculado en tres casos.

En el primer caso (figura 11), el cálculo se realiza en un enlace de punto a punto, a lo largo de las rutas rojas (R) o azules (B).

En el segundo caso (figura 12), dos canales de NUT o ET se han creado a lo largo de las rutas rojas(R) y azules (B), para realizar un esquema de protección de conexión de sub-red (la ruta más corta se ha considerado como “de funcionamiento” y la más larga como “protección”).

En el tercer caso (figura 13) el esquema de protección de conexión de sub-red se ha realizado en el equipo DXC, permitiendo, en efecto, la diversificación de los canales de protección y funcionamiento (anillo 1 y anillo 2).

Los valores de indisponibilidad de infraestructura y equipos se indican en la Tabla 1 a continuación

TABLA 1

Elemento de red	Bloqueo funcional	Indisponibilidad [absoluta]
ADM	Puertos STM1	1.36711E-05
	Matriz	1.37079E-10
	Partes comunes	3.52434E-05
	Puertos de línea	2.53672E-05
RED	Puertos STM1	4.11369E-06
	Matriz	1.0824E-09
	Partes comunes	1.46034E-05
Características del anillo	Fibra /km	0,000003
	Circunferencia de los anillos	1000 km
	n. ADM/anillo	4

La tabla 2 resume los resultados obtenidos en los tres casos descritos anteriormente.

TABLA 2

Caso	Nodo A	Nodo Z	Ruta	Tipo de protección	Indisponibilidad [absoluta]	Disponibilidad [%]	Indisp. min/año
1	A	Z1	roja	ET	0,0082183	99180	431
	A	Z2	azul	ET	0,0090064	99100	473
	A	Z1	roja	NUT	0,0047427	99526	249
	A	Z2	azul	NUT	0,0054540	99455	286
2	A	Z	anillo 1	ADM de SNCP de ET	0,00011064	99990	58
	A	Z	anillo 1	ADM de SNCP de NUT	0,00002587	99,997	14
	A	Z	anillo 1	ADM protegido de MS-SPRing	0,00002055	99998	11
3	A	Z	anillo 1-2	RED de SNCP de ET	0,00013148	99989	69
	A	Z	anillo 1-2	RED de SNCP de NUT	0,00004420	99,996	23
	A	Z	anillo 1	RED protegido de MS-SPRing	0,00004175	99,996	22
	A	Z	anillo 2	RED protegido de MS-SPRing	0,00004162	99,996	22

Los datos muestran que los canales NUT tienen menos minutos de indisponibilidad cuando se comparan con canales ET. Para ambos tipos de protección, el orden de la magnitud comprende desde miles de minutos en el caso no-protegido hasta decenas de minutos para las SNCPs. La indisponibilidad la SNCP protegida de canales ET se sitúa entre la indisponibilidad de las cifras de desprotegido y el NUT protegido de SNCP.

La disposición descrita aquí es adaptada para uso en redes de arquitectura en malla donde las sub-rutas de ET utilizan el ancho de banda definido para restablecimiento de tráfico. Esto se muestra, en términos bastante generales, en la figura 14 donde tal red se indica con el número de referencia 1000.

La infraestructura en malla mostrada allí se implementa vía conexiones digitales cruzadas interconectada con los terminales de línea. Cada rama en el plan de red tiene asociada una cierta cantidad de banda ancha para recuperar los fallos de cables o equipos. Cuando la eficiencia de red está exenta de fallos, la banda reservada para recuperación, está sin utilizar y puede ser configurada para llevar a cabo ET. Para incrementar la razón de disponibilidad es posible proteger dos canales con un esquema de protección de conexión de sub-red.

Lo importante de la disposición aquí descrita es la protección de rutas realizadas en configuración de baja prioridad. La realización descrita concierne a la tecnología SDH con arquitectura en malla o en anillo.

En este tipo de red, los datos se transmiten vía TDM (Multiplexión por División de Tiempo) en esos canales protegidos (es decir: canales de alta prioridad) cuya longitud es fija (VC, canales virtuales). Cada canal transporta

uno o más flujos de datos de circuitos definidos por el protocolo implementado. Las redes de este tipo incluyen, por ejemplo, SDH (Jerarquía Sincrónica Digital) o redes SONET (Red Óptica Sincrónica).

En este tipo de red, con canal de alta prioridad, canales de tráfico adicional (es decir canales de prioridad baja) puede ser configurada de varias formas.

En redes WDM (Multiplexión por División de Longitud de Onda), los datos se transmiten en diferentes longitudes de onda, que reemplazan los periodos de tiempo de la multiplexación. Con esta tecnología es posible crear la conocida como rutas protegidas "lambda"; a la lambda (es decir: la longitud de onda) reservada a la protección de la lambda principal, o compartida con un conjunto de otras lambdas, se le puede asignar el papel de transportar tráfico de baja prioridad. Desde un punto de vista técnico, el tráfico adicional en redes SONET y SDH, y en lambdas de baja prioridad en redes WDM se puede considerar equivalente. Ambos son canales interrumpibles cuando se da un estado de fallo, sin tener en cuenta la implementación física real de la red.

También, las redes SDM (Multiplexión por División de Espacio) o FDM (Multiplexión por División de Frecuencia) se pueden implementar de una forma similar. En estos casos, el concepto de rutas de Tráfico Adicional se asocia a intervalos de espacio o frecuencia. Como se sabe, la tecnología FDM fue la dominante antes de que se desarrollara la tecnología TDM.

La invención se refiere a todos los tipos de redes basados en el concepto de protección de circuito descrito anteriormente. En concreto, la referencia realizada en la descripción a las redes TDM (SDH y SONET) y WDM es principalmente dictada por su actual popularidad.

Una aplicación de restablecimiento hace uso de cualquier capacidad disponible entre nodos. En general, el restablecimiento implicará re-enrutamiento. Cuando se utiliza el restablecimiento, un porcentaje de la capacidad de la red de transporte se reservará para el tráfico de funcionamiento de re-enrutamiento. El restablecimiento es iniciado (de una manera conocida) por el operador de red y como tal, no entra en el campo del presente documento.

Es en efecto evidente que, los principios básicos de la invención permanecen sin modificación, los detalles y realizaciones pueden variar ampliamente con respecto a lo que se ha descrito e ilustrado a través de ejemplos, sin apartarse del campo de la presente invención tal y como se define en las reivindicaciones anexas.

Referencias citadas en la descripción

Esta lista de referencias citadas por el solicitante está prevista únicamente para ayudar al lector y no forma parte del documento de patente europea. Aunque se ha puesto el máximo cuidado en su realización, no se pueden excluir errores u omisiones y la OEP declina cualquier responsabilidad al respecto.

Documentos de patente citados en la descripción

- WO 02073903 A [0020]
- WO 01030006 A [0022] [0037]
- EP 1014611 A [0023]

REIVINDICACIONES

1. Un método para proporcionar rutas de tráfico adicional (ET) en una red de comunicaciones incluyendo al menos dos canales de protección (A, B) asociados a sus canales de transmisión respectivos, cada uno de los mencionados con al menos dos canales de protección (A, B) admitiendo un estado activo para transportar, en presencia de un fallo en el canal de transmisión asociado mencionado, tráfico para ser llevado por el canal de transmisión asociado y un estado de espera, en el que el canal de protección se adapta a llevar tráfico adicional (ET), **caracterizada** porque: incluye un paso de ejecución, mencionados al menos dos canales de protección (ET) en un esquema de protección de conexión de sub-red, según el cual uno de los mencionados de al menos dos canales de protección (A, B) en el mencionado estado de espera se adapta para asegurar la recuperación de tráfico adicional transportado por el otro de los mencionados al menos dos canales de protección (A, B) mientras que se de una de la siguientes condiciones:

- el otro mencionado de los mencionados al menos dos canales de protección (A, B) es conmutado al estado activo mencionado,
- el otro mencionado de los mencionados al menos dos canales de protección (A, B) está sujeto a fallo.

2. El método de la reivindicación 1 **caracterizado** porque incluye los pasos de:

- asociar a cada uno de los mencionados al menos dos canales de protección (A, B) correspondiendo a la conexiones digitales cruzadas de (DXCs) salida y entrada, y
- ejecutar el mencionado esquema de protección de sub-red a las mencionadas conexiones digitales cruzadas (DXCs) de salida y entrada.

3. El método de la reivindicación 1 **caracterizado** porque incluye los pasos de:

- asociar a cada uno de los mencionados al menos dos canales de protección (A, B) sendos multiplexores de inserción/extracción (ADM) de salida y entrada, y
- ejecutar el mencionado esquema de protección de conexión de sub-red en los mencionados multiplexores de inserción/extracción (ADM) de entrada y salida.

4. El método de la reivindicación 1 **caracterizado** porque incluye los pasos de proporcionar en la mencionada red de comunicación al menos una estructura de anillo incluyendo rutas no-coextensivas y el paso de asociar los mencionados al menos dos canales de protección (A, B) a sus respectivas rutas no-coextensivas en el mencionado anillo.

5. El método de la reivindicación 1 **caracterizado** porque incluye los pasos de proporcionar en la mencionada red de comunicación una pluralidad de estructuras de anillo y el paso de asociar los mencionados al menos dos canales de protección (A, B) a sus respectivos anillos diferentes de la mencionada pluralidad de anillos.

6. El método de la reivindicación 5 **caracterizado** porque incluye el paso de seleccionar dos anillos diferentes ya mencionados como anillos que pertenecen a la misma clase de anillos.

7. El método de la reivindicación 5 **caracterizado** porque incluye el paso de seleccionar dos anillos diferentes ya mencionados como anillos que pertenecen a diferentes clases de anillos.

8. El método de la reivindicación 1 **caracterizado** porque incluye el paso de proporcionar tráfico desprotegido no apropiable (NUT) transportado en canales no apropiables en la red mencionada además de canales no apropiables protegidos por el esquema de protección de conexión de sub-red (SNCP), en el que el mencionado tráfico adicional es asegurado en un nivel intermedio de disponibilidad entre los niveles de protección proporcionados por los mencionados canales no apropiables y por los mencionados canales no apropiables protegidos por el esquema de protección de conexión de sub-red (SNCP).

9. Una red de comunicación que comprende una pluralidad de nodos emparejados juntos mediante canales de transmisión, con dicha red incluyendo al menos dos canales de protección (A, B) asociados a sus respectivos canales de transmisión, cada uno de los mencionados al menos dos canales de protección (A, B) que son capaces de admitir un estado activo para llevar, en presencia de un fallo en el mencionado canal de transmisión asociado, tráfico para ser llevado por el canal de transmisión asociado y un estado de espera en que el canal de protección se adapta para llevar tráfico adicional (ET), **caracterizada** porque al menos dos canales de protección (ET) son ejecutados en un esquema de protección de conexión de sub-red, según el cual uno de los mencionados de al menos dos canales de protección (A, B) en el mencionado estado de espera asegura la recuperación de tráfico adicional llevado por el otro mencionado de al menos dos canales de protección (A, B) mientras que se dé una de la siguientes condiciones:

- el otro mencionado de los mencionados al menos dos canales de protección (A, B) está conmutado al estado activo mencionado,
- el otro mencionado de los mencionados al menos dos canales de protección (A, B) está sujeto a fallo.

10. La red de la reivindicación 9 **caracterizada** porque incluye las conexiones digitales cruzadas de salida y entrada correspondientes (DXCs) asociadas a cada uno de los mencionados al menos dos canales de protección (A, B) y en el que las conexiones digitales cruzadas (DXC) de salida y entrada mencionadas definen conjuntamente el mencionado esquema de protección de conexión de sub-red.

11. La red de la reivindicación 9 **caracterizada** porque incluye los multiplexores de inserción/extracción (ADM) de salida y entrada correspondientes

- asociados a cada uno de los mencionados al menos dos canales de protección (A, B) y en el que los multiplexores de inserción/extracción (ADM) de salida y entrada mencionados definen conjuntamente el mencionado esquema de protección de conexión de sub-red.

12. La red de la reivindicación 9 **caracterizada** porque incluye al menos una estructura de anillo incluyendo rutas no-coextensivas y en el que los mencionados al menos dos canales de protección (A, B) están asociados a sus rutas no-coextensivas respectivas en el mencionado anillo.

13. La red de la reivindicación 9 **caracterizada** porque incluye una pluralidad de estructuras de anillo y en la que los mencionados al menos dos canales de protección (A, B) están asociados a dos respectivos anillos diferentes de la mencionada pluralidad de anillos.

14. La red de la reivindicación 13 **caracterizada** porque los mencionados dos anillos diferentes pertenecen a la misma clase.

15. La red de la reivindicación 13 **caracterizada** porque los mencionados dos anillos diferentes pertenecen a diferentes clases de anillos.

16. Un producto informático de ordenador, que se puede cargar en la memoria de al menos un ordenador incluyendo porciones de código de software.

Fig. 1

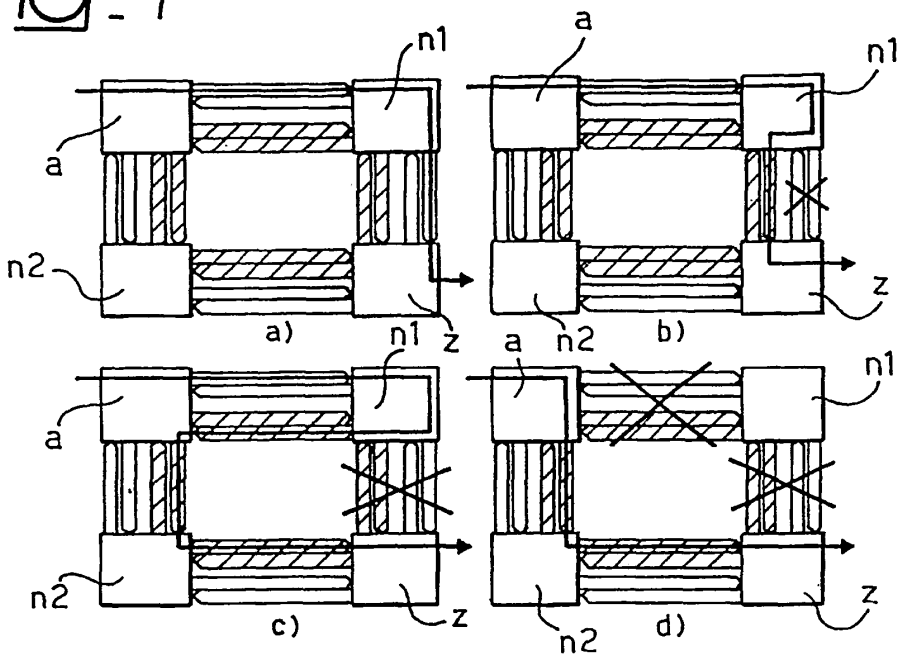


Fig. 2

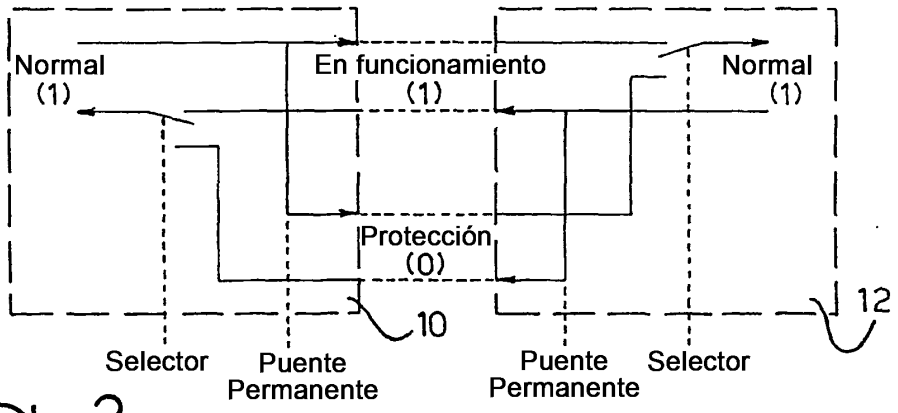
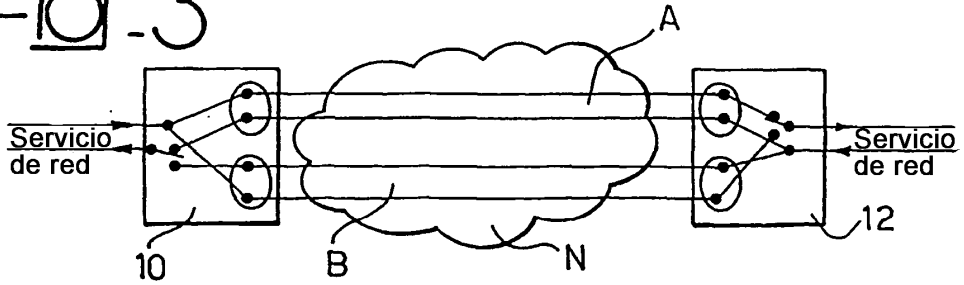


Fig. 3



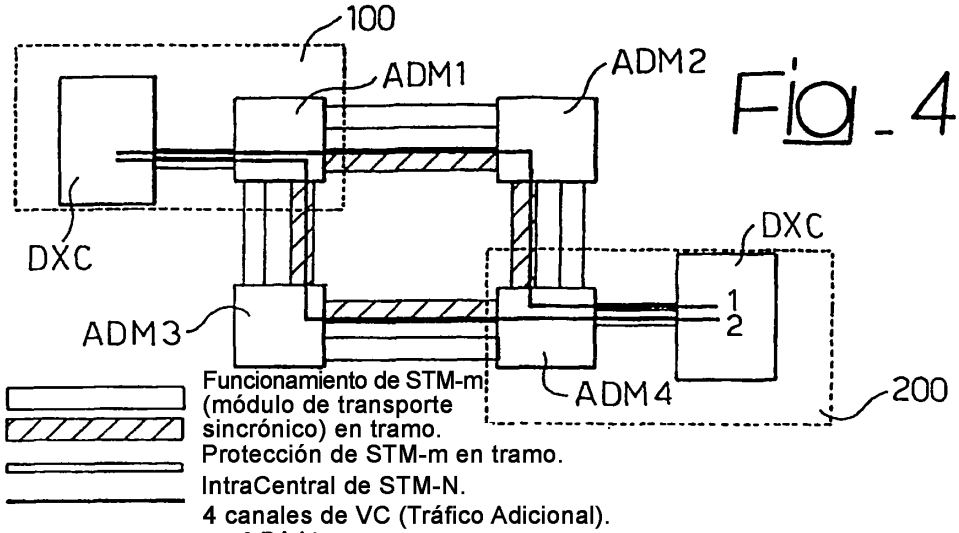


Fig. 4

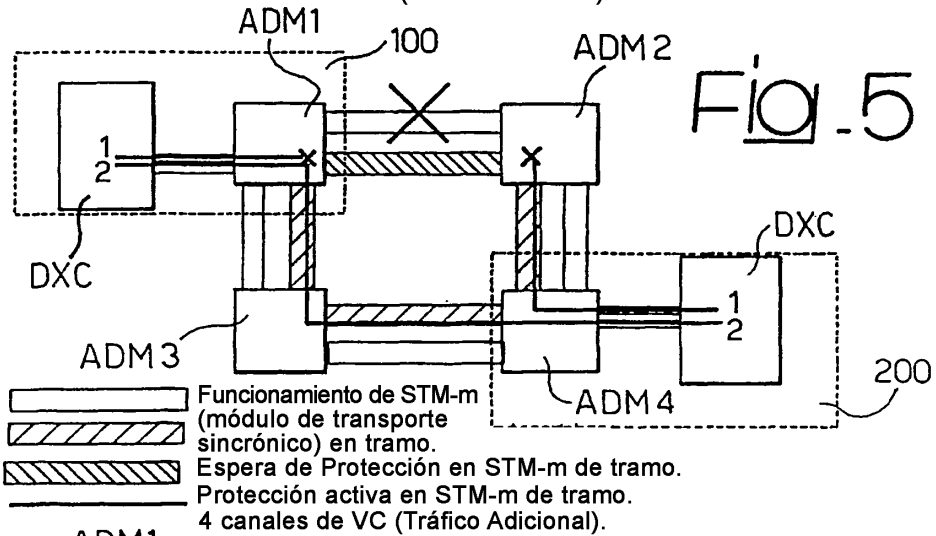


Fig. 5

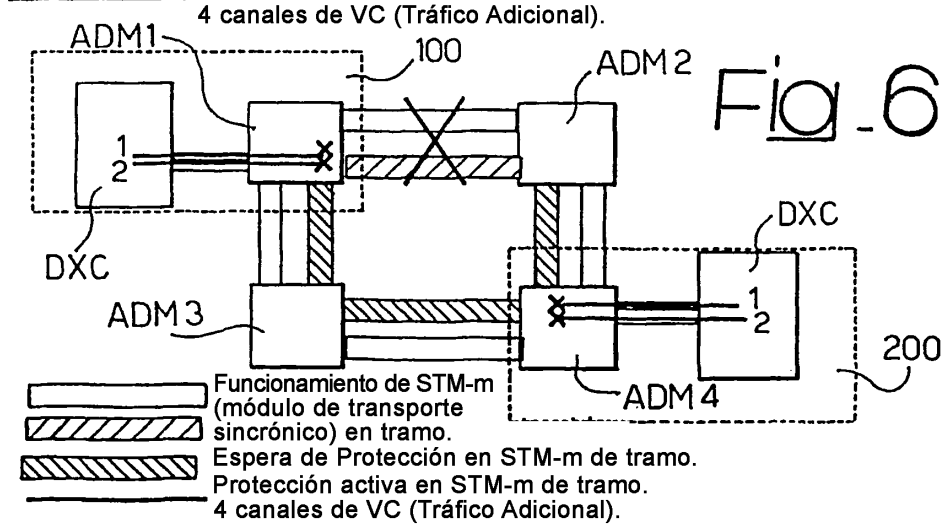


Fig. 6

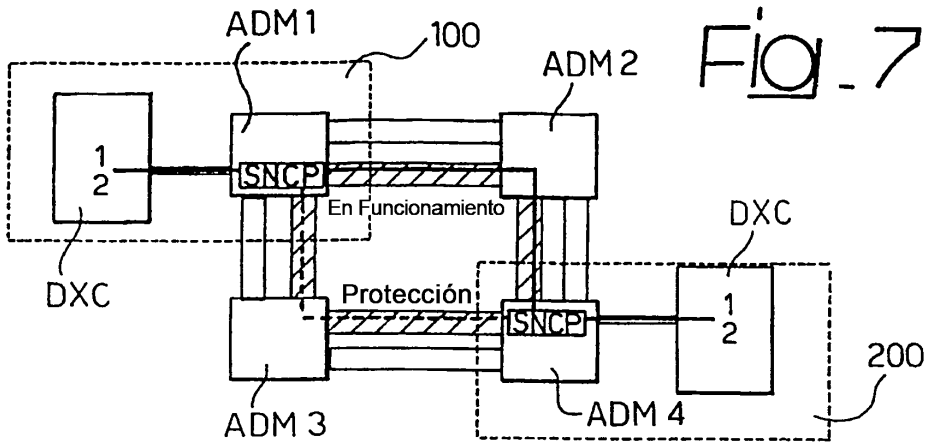


Fig. 7

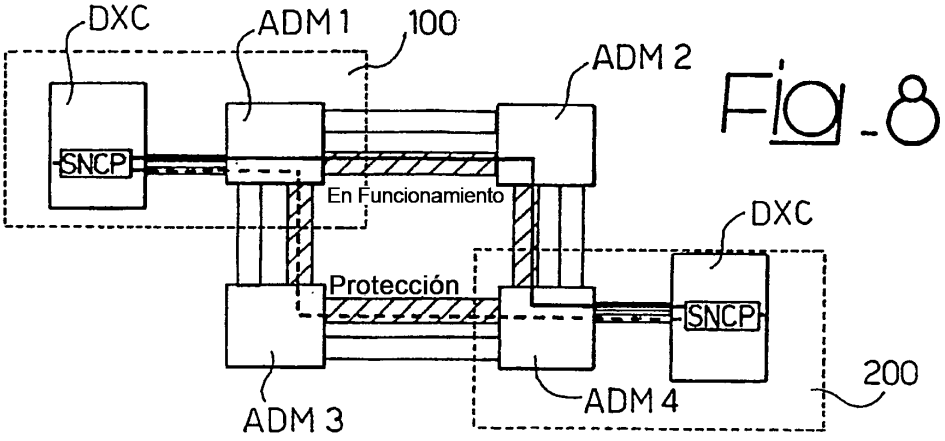


Fig. 8

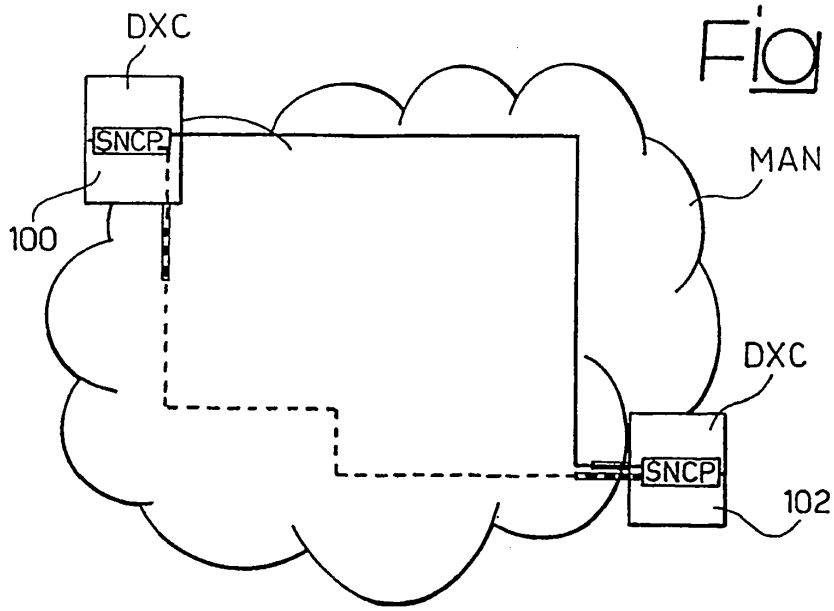


Fig. 14

Fig. 9

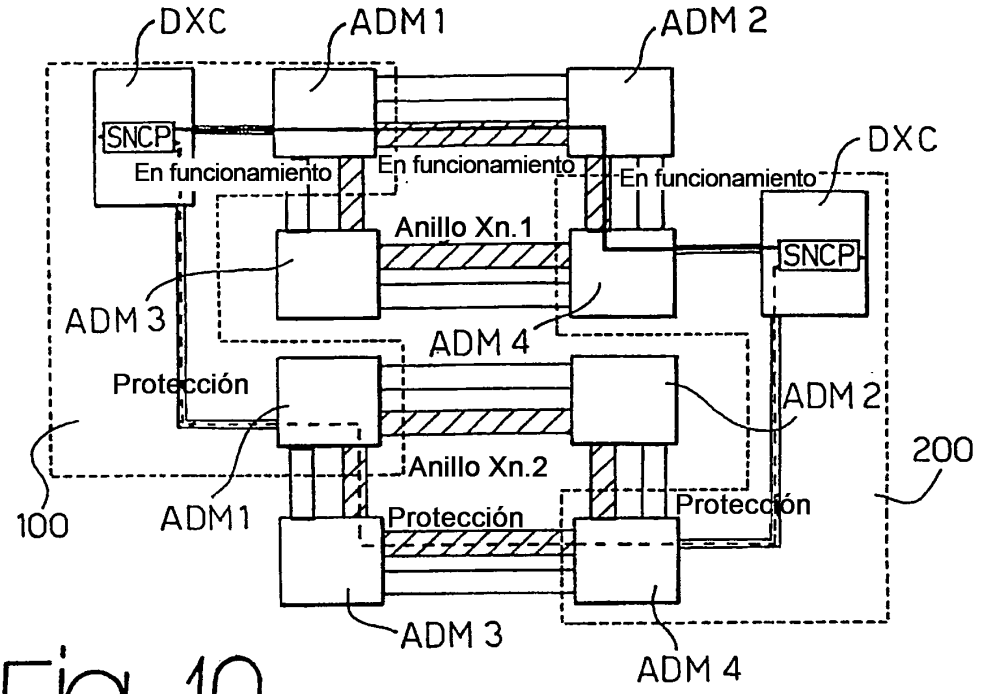

DXC
ADM 1
ADM 2
SNCP
En funcionamiento
En funcionamiento
En funcionamiento
DXC
Anillo Xn.1
SNCP
ADM 3
ADM 4
Protección
ADM 2
200
Anillo Xn.2
100
ADM 1
Protección
Protección
ADM 3
ADM 4

Fig. 10

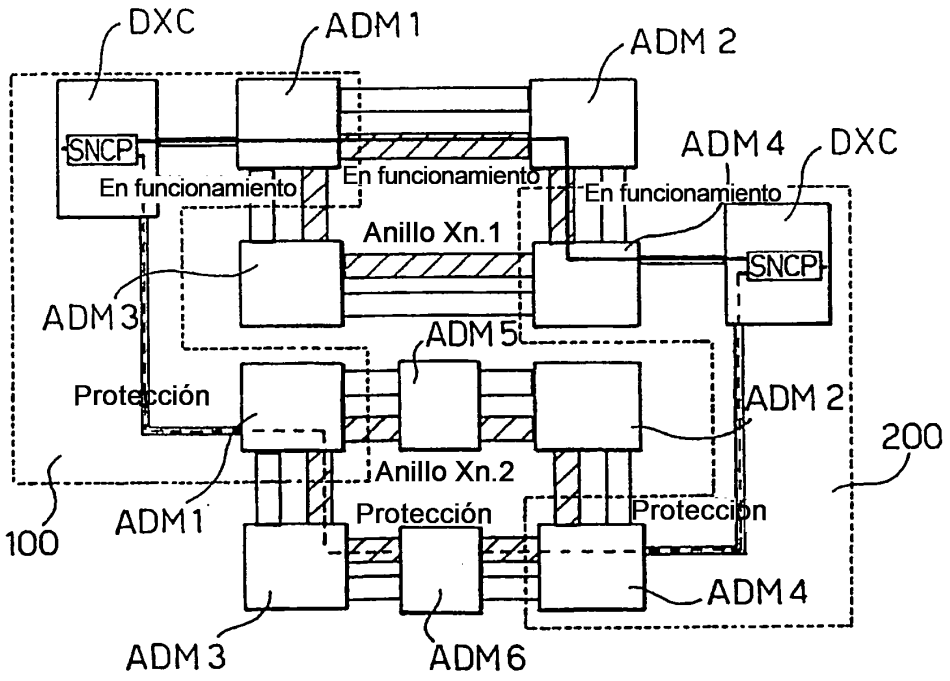

DXC
ADM 1
ADM 2
SNCP
ADM 4
DXC
En funcionamiento
En funcionamiento
Anillo Xn.1
SNCP
ADM 3
ADM 5
Protección
ADM 2
200
Anillo Xn.2
100
ADM 1
Protección
Protección
ADM 4
ADM 3
ADM 6

Fig. 11

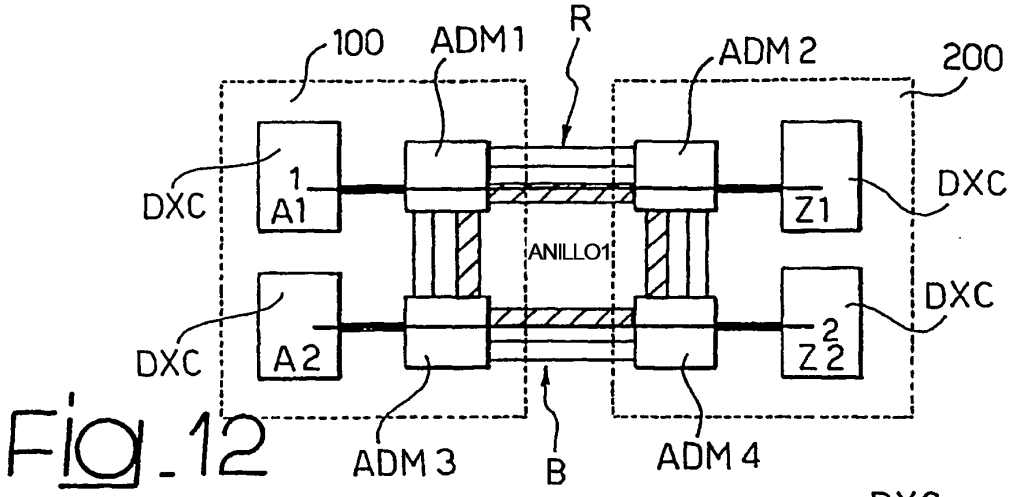


Fig. 12

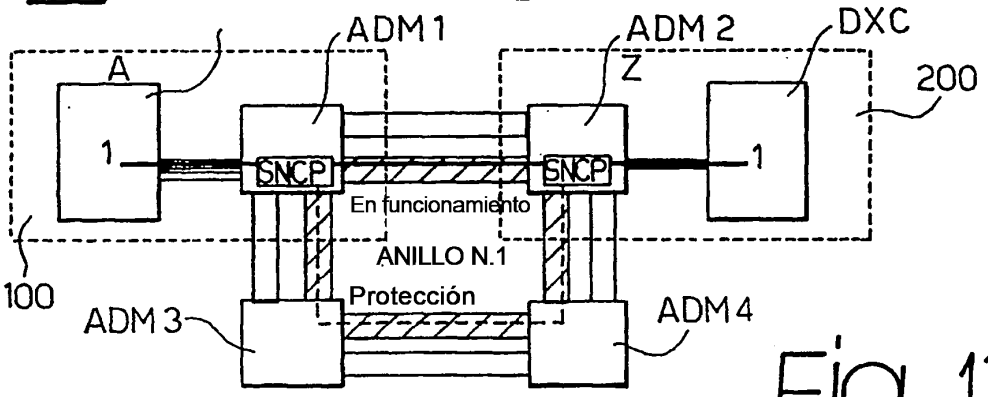


Fig. 13