(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 429 314**

(51) Int. CI.:

H04L 12/723 (2013.01)
H04L 12/703 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.10.2009 E 09783645 (6)**

(97) Fecha y número de publicación de la concesión europea: **03.07.2013 EP 2478673**

(54) Título: **La presente invención se refiere a la recuperación de tráfico en una red orientada a conexión**

(30) Prioridad:

16.09.2009 EP 09170420

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.11.2013

(73) Titular/es:

TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) (100.0%)
Torshamnsgatan 23
164 83 Stockholm, SE

(72) Inventor/es:

FIORONE, RAOUL;
MARTINOTTI, RICCARDO y
CORTI, ANDREA

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

La presente invención se refiere a la recuperación de tráfico en una red orientada a conexión

CAMPO TÉCNICO
La presente invención se refiere a la recuperación de tráfico en una red orientada a conexión.

ANTECEDENTES
Las Redes por Conmutación de Paquetes están sustituyendo a las redes heredadas basadas en el Multiplexado por División de Tiempo (TDM), tales como las redes de Jerarquía Digital Síncrona (SDH), por su capacidad de gestionar tráfico de datos como Ethernet e IP de una manera más optimizada y flexible. Las Redes por Conmutación de Paquetes Orientadas a Conexión (CO-PS) son un candidato ideal para la migración desde redes TDMA heredadas hacia redes totalmente por paquetes, por su capacidad de flexibilidad de extremo-a-extremo y de monitorización del rendimiento y por su capacidad de gestión.

Para sustituir las redes SDH heredadas, se requiere que las Redes CO-PS garanticen un rendimiento de calidad para transporte y que proporcionen la misma flexibilidad a los fallos que la ofrecida por las redes de transporte heredadas. Típicamente, se requiere que las redes de transporte conmuten a un trayecto de protección antes de 50 ms tras producirse un fallo. El requisito de conmutación de protección por debajo de 50 ms es un requisito difícil de cumplir en redes SDH, especialmente cuando es necesario gestionar un número elevado de casos simultáneos de conmutación de protección, y constituye un desafío todavía mayor para Redes CO-PS.

Un tipo de tecnología de redes CO-PS es el Perfil de Transporte-Conmutación por Etiquetas Multi-Protocolo (MPLS-TP), el cual se está desarrollando como un perfil de transporte de Conmutación por Etiquetas Multi-Protocolo (MPLS). El MPLS-TP pretende proporcionar un “aspecto y sensación” similares a la SDH con capacidad de interoperabilidad inherente con redes IP/MPLS existentes. En las redes MPLS-TP, se crean túneles de Trayecto Conmutado por Etiquetas (LSP) entre nodos de red que es necesario que se comuniquen entre sí. Las unidades de transporte (por ejemplo, paquetes) incluyen un encabezamiento de corrección de compatibilidad que contiene la etiqueta que identifica un túnel específico. Para incrementar la disponibilidad de la red, habitualmente es necesario hacer que los túneles LSP sean redundantes, usando algún esquema de protección de red. En el caso de MPLS-TP, esto típicamente significa esquemas de protección de extremo-a-extremo de 1+1 ó 1:1.

En el MPLS, el cual también se puede usar como una tecnología CO, no existe ninguna protección de extremo-a-extremo sino únicamente restablecimiento y mecanismos de reparación locales. Un problema es que cuando, en una red, hay presente un número elevado de túneles LSP, y es necesario proteger los mismos, es probable que haya un número alto de conmutaciones de protección simultáneas en un nodo. El número de eventos de conmutación de protección simultáneos que pueden tener lugar en un nodo depende de las relaciones de tráfico entre los nodos, la topología de la red y el diseño de la misma, así como el tipo de fallo que se haya producido. La protección es gobernada por paquetes de Operaciones, Administración y Gestión (OAM) que, para una protección rápida, se envían a intervalos cortos (típicamente 3,3 ms) y que es necesario que sean procesados por el nodo de recepción. Los mecanismos para declarar una avería de un túnel LSP incluyen: falta de verificación de conectividad (por ejemplo, no se reciben tres paquetes OAM periódicos consecutivos) o mensajes explícitos de indicación de fallo tales como una Indicación de Defecto en Sentido Directo (FDI).

El número de casos de protección que puede resultar necesario conmutar simultáneamente en un nodo puede ser alto. Adicionalmente, cuando el tráfico se transporta sobre túneles LSP mediante Seudocables (PW), que es el caso típico para que el MPLS-TP transporte clientes de Ethernet y TDM/ATM, el nivel de PW se puede proteger con otro nivel de OAM, lo cual hace que aumente adicionalmente el número de conmutaciones de protección que se deben llevar a cabo. Una posible solución para cumplir el requisito de conmutación de protección de 50 ms es el anidamiento LSP. El anidamiento LSP crea una jerarquía de LSPs de manera que una multitud de LSPs internos es transportada por un LSP externo para una porción dada de la red. El LSP externo es la entidad sobre la cual se lleva a cabo la protección del tráfico en esa porción de la red. Esto requiere la creación de una capa adicional en la red y presenta la restricción de proporcionar una solución únicamente en esa porción de la red.

La Recomendación G.808.1 de la Unión Internacional de Telecomunicaciones (ITU-T) “Generic Protection Switching – Linear trail subnetwork protection” describe un mecanismo llamado Protección de Camino de Grupo. Entre un par común de puntos extremos de la red se configura un grupo de conexiones de trayectos de trabajo y trayectos de protección. Se requiere que todos los trayectos de trabajo y trayectos de protección conecten el mismo par de nodos extremos y sigan la misma ruta. El conjunto lógico en el nodo de recepción fusiona señales individuales de fallo de señal de camino (TSF) en un único Grupo de SF (SFG) y fusiona señales individuales de degradación de señal de camino (TSD) en un único Grupo de SD (SDG). En el caso de una protección 1:1, debe enviarse un mensaje de Conmutación de Protección Automática (APS) para el grupo entero. La protección se activa para el grupo entero cuando la señal de SFG está activa. La G.808.1 describe tres políticas para generar un SFG: (1) todos los miembros del grupo de protección fallan, es decir, se declara un SFG en caso de que haya señales individuales en TSF; (2) falla un miembro seleccionado, es decir, una señal individual se selecciona como señal de referencia y se declara un

SFG en el caso del que el TSF de la señal de referencia esté activo; (3) falla un porcentaje dado de miembros, es decir, únicamente si el número de TSF activo supera un umbral dado, el SFG está activo.

En la solicitud de patente EP 1788757 y en la publicación XP015038127 se dan a conocer otros métodos para la recuperación de tráfico en redes orientadas a conexión.

La presente invención busca proporcionar un método alternativo de protección de tráfico en una red.

SUMARIO

Un aspecto de la presente invención proporciona un método para llevar a cabo una detección de fallos y una recuperación de tráfico en un primer nodo en una red orientada a conexión, comprendiendo la red una pluralidad de conexiones que terminan en el primer nodo, comprendiendo el método:

configurar en el primer nodo un grupo de recuperación que comprende por lo menos dos de la pluralidad de conexiones;
llevar a cabo una detección de fallos sobre cada una de la pluralidad de conexiones en el grupo de recuperación;
determinar si se cumple por lo menos una condición de fallo de grupo de recuperación, basándose en los resultados de las detecciones de fallos llevadas a cabo sobre la pluralidad de conexiones en el grupo de recuperación y:

cuando se cumple la por lo menos una condición de fallo del grupo de recuperación, conseguir que el tráfico sobre la pluralidad de conexiones en el grupo de recuperación se transfiera a trayectos de reserva y:
cuando no se cumple la por lo menos una condición de fallo del grupo de recuperación, y se ha detectado un fallo en una conexión del grupo de recuperación, provocar que el tráfico se transfiera desde esa conexión a un trayecto de reserva.

El término “recuperación” está destinado a incluir “protección”, lo cual típicamente significa que un trayecto de reserva se preconfigura con antelación a la detección de cualquier fallo o avería, así como un “restablecimiento”, lo cual típicamente significa que la señalización para configurar un trayecto de reserva se produce después de la detección de la avería. El método permite que la conmutación a un trayecto de reserva se produzca más rápidamente para un grupo de conexiones, en la medida en la que no es necesario esperar hasta que el nodo haya detectado un fallo en cada conexión individual en el grupo. Una realización ventajosa del método se usa para la conmutación de protección a un trayecto de (protección) reserva preconfigurado.

El método se puede aplicar a cualquier topología de red y es aplicable a una gama de diferentes mecanismos de recuperación de extremo-a-extremo sin depender del mecanismo de protección específico usado realmente. El método puede funcionar sin ninguna señalización OAM adicional con respecto a la ya usada en redes, y sin requerir la gestión de una capa de red adicional. Únicamente el nodo en el cual terminan las conexiones necesita tener conocimiento de la existencia del grupo de recuperación. Esto permite una gestión en un solo extremo y resulta ventajoso cuando el nodo de recepción está ubicado en un dominio de red diferente a otros nodos de terminación de las conexiones.

No existe ningún requisito para que las conexiones dentro del grupo de recuperación sigan la ruta del mismo trayecto dentro de la red y las conexiones dentro del grupo de recuperación pueden tener diferentes nodos remotos.

Esta invención se puede aplicar a cualquier tipo de tecnología orientada a conexión, tal como una red de Conmutación por Etiquetas Multi-Protocolo Generalizada (GMPLS), de Conmutación por Etiquetas Multi-Protocolo (MPLS), de Perfil de Transporte - Conmutación por Etiquetas Multi-Protocolo (MPLS-TP), Ethernet orientada a conexión o Ingeniería de Tráfico por Puentes entre Redes Dorsales de Proveedores (PBB-TE), IEEE 802.1Qay.

Otro aspecto de la invención proporciona un aparato para llevar a cabo el método en un nodo.

Un aspecto adicional de la invención proporciona un método para configurar la detección de fallos y la recuperación de tráfico en un primer nodo en una red orientada a conexión, comprendiendo la red una pluralidad de conexiones que se hacen terminar en el primer nodo (N6), comprendiendo el método, en un nodo aparte del primer nodo:

señalización para configurar un grupo de recuperación en el primer nodo, en donde la señalización:
define un grupo de recuperación que comprende por lo menos dos de la pluralidad de conexiones que terminan en el primer nodo;
define por lo menos una condición de fallo de grupo de recuperación que se debe cumplir, para conseguir que se declare una condición de fallo de grupo de recuperación para todas las conexiones en el grupo de recuperación;
en donde, cuando se cumple la por lo menos una condición de fallo de grupo de recuperación, el tráfico sobre la pluralidad de conexiones en el grupo de recuperación se transferirá a trayectos de reserva y cuando no se cumpla la

por lo menos una condición de fallo de grupo de recuperación, y se haya detectado un fallo en una conexión del grupo de recuperación, se transferirá tráfico desde esa conexión a un trayecto de reserva.

La funcionalidad descrita en la presente se puede implementar en software, hardware o una combinación de los mismos. La funcionalidad se puede implementar por medio de hardware que comprenda varios elementos diferenciados y por medio de un aparato de procesado programado de forma adecuada. El aparato de procesado puede comprender un ordenador, un procesador, una máquina de estados, una matriz lógica o cualquier otro aparato de procesado adecuado. El aparato de procesado puede ser un procesador de propósito general que ejecute software con el fin de conseguir que el procesador de propósito general lleve a cabo las tareas requeridas, o el aparato de procesado puede estar dedicado a llevar a cabo las funciones requeridas. Otro aspecto de la invención proporciona instrucciones (software) legibles por máquina que, cuando son ejecutadas por un procesador, llevan a cabo cualquiera de los métodos descritos. Las instrucciones legibles por máquina se pueden almacenar en un dispositivo de memoria electrónico, un disco duro, un disco óptico u otro soporte de almacenamiento legible por máquina. Las instrucciones legibles por máquina se pueden descargar a un aparato de procesado por medio de una conexión de red.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se describirán, únicamente a título de ejemplo, realizaciones de la invención en referencia a los dibujos adjuntos, en los cuales:

la Figura 1 muestra una red de ejemplo con conexiones y grupos de recuperación;
la Figura 2 muestra un fallo que se produce en la red de la Figura 1;
la Figura 3 muestra trayectos de reserva para los trayectos de trabajo en el grupo de recuperación (protección);
la Figura 4 muestra un escenario en el cual se producen múltiples fallos en la red;
la Figura 5 muestra un escenario en el cual se produce un fallo en un trayecto de reserva de una de las conexiones en la red de la Figura 1;
la Figura 6 muestra una tabla de formas posibles de funcionamiento de los miembros de un grupo de protección;
la Figura 7 muestra un aparato en un nodo en la red de la Figura 1;
las Figuras 8A y 8B muestran un método de funcionamiento de un nodo en la red de la Figura 1.

DESCRIPCIÓN DETALLADA

La Figura 1 muestra una red de comunicaciones de ejemplo que comprende un conjunto de nodos conectados mediante enlaces 11 de comunicación, los cuales pueden usar tecnología óptica, eléctrica, inalámbrica o cualquier otra. Se muestran conexiones entre cada uno de los nodos N1 a N4 y el nodo N6. Una conexión LSP1-6 conecta N1 al nodo N6 por medio de los nodos N2 y N5. Una conexión LSP2-6 conecta el nodo N2 al nodo N6 por medio del nodo N5. Una conexión LSP3-6 conecta N3 al nodo N6 por medio de los nodos N2 y N5. Una conexión LSP4-6 conecta el nodo N4 al nodo N6 por medio del nodo N5. Cada conexión mostrada en la Figura 1 se puede implementar como un Trayecto Conmutado por Etiquetas (LSP), un SeudoCable (PW) sobre un LSP, o cualquier otra forma de tecnología orientada a conexión. Se pueden transportar múltiples conexiones a través de un trayecto físico común entre un par de nodos, o mediante múltiples trayectos físicos entre un par de nodos.

La señalización de Operaciones, Administración y Gestión (OAM) se lleva a cabo en la red. Un tipo de señalización OAM es la señalización de verificación de la conectividad. Este tipo de señalización envía periódicamente un mensaje que incluye un campo de Comprobación de Continuidad (CC) entre nodos de punto extremo de cada una de las conexiones mostradas en la Figura 1. Por tanto, por ejemplo, los nodos N1 y N6 intercambian mensajes de señalización de CC. Si no se reciben mensajes de CC en un periodo de tiempo predeterminado, esto es indicativo de un fallo a lo largo de la conexión.

Otros tipos de señalización OAM incluyen: un tipo de mensaje de indicación de defecto en sentido directo (FDI), cuya función es informar inmediatamente al nodo de recepción sobre una avería detectada por un nodo intermedio a lo largo del trayecto, acelerando así la conmutación de protección; un tipo de mensaje de Conmutación de Protección Automática. En la red puede haber presentes un tipo, o múltiples tipos, de mensajes OAM, y los mismos pueden ser usados por el nodo que gestiona el grupo de recuperación.

En el ejemplo de la Figura 1, un grupo de recuperación A está configurado para el conjunto de cuatro conexiones (LSP1-6, LSP2-6, LSP3-6, LSP4-6) que terminan en el nodo N6. Un grupo de recuperación diferente B se configura para el conjunto de conexiones mostradas en la mitad inferior de la Figura 1. El grupo de recuperación permite que el nodo N6 gestione en conjunto el grupo de conexiones con fines relacionados con la recuperación de tráfico. Por motivos de claridad, en la Figura 1 se muestra un pequeño número de túneles LSP aunque el número de los casos de protección, que pueden estar asociados a túneles LSP y/o PWs, puede ser significativo, para una red metropolitana de alta densidad o para una red central puede ser fácilmente del orden de varios cientos.

El grupo de recuperación dispone de una condición, o un conjunto de condiciones, que se usan para decidir cuándo

se producirá una recuperación de tráfico (por ejemplo, conmutación de protección) para el grupo de conexiones. Una condición adecuada es un valor de umbral de conexiones que informan sobre un fallo. El umbral se puede expresar como un valor absoluto (por ejemplo, 5, 10) o un porcentaje o proporción del número total de conexiones en el grupo (por ejemplo, el 50%). Una vez que se ha alcanzado el valor de umbral, el grupo completo de conexiones en el grupo de recuperación se declara como fallido y se inicia el procedimiento de protección para todos los miembros de grupo de acuerdo con las características del mecanismo de protección en vigor. Tras este punto, no es necesario que se produzca ningún procesado adicional de mensajes OAM para conexiones individuales dentro del grupo con el fin de que tenga lugar la conmutación de protección. Una conmutación de protección se produce (inmediatamente) en cualquier conexión, o conexiones, individual sobre la cual se haya detectado un fallo. La conmutación de protección de conexiones individuales se produce con independencia de si se han cumplido los requisitos para que el grupo se declare fallido, permitiéndose así que el tráfico se conmute desde conexiones fallidas individuales sin retardo.

El grupo de recuperación se configura en el nodo N6. Una característica del grupo de recuperación es que puede ser configurado y gestionado localmente por un nodo, y no es necesario que la existencia del grupo de recuperación sea conocida por ningún otro nodo de la red. En resumen, el grupo de recuperación se puede gestionar en un solo extremo. Esto permite usar el mecanismo de grupo de recuperación con sistemas terceros, tales como otros dominios de red u operadores de red, que no tengan conocimiento de los grupos de recuperación. Otra característica del mecanismo de grupo de recuperación es que no requiere que una capa de red específica u OAM gestione el grupo de recuperación.

La Figura 1 muestra un conjunto de ejemplo de LSPs entre nodos de la red. Un único LSP puede transportar múltiples SeudoCables (PW). Cada PW puede tener su propia señalización OAM y puede tener un caso de protección preconfigurado asociado al mismo. En la Figura 1 se muestran únicamente trayectos de trabajo. Para cada trayecto de trabajo existe un trayecto de reserva preconfigurado. Puede existir una relación de 1:1 entre un trayecto de trabajo y un trayecto de reserva (es decir, existe un trayecto de reserva dedicado para cada trayecto de trabajo) o una relación de N:1 entre un trayecto de trabajo y un trayecto de reserva (es decir, un trayecto de reserva se comparte entre N trayectos de trabajo). Al grupo de conexiones se le denominará “grupo de protección” en la siguiente descripción, en la medida en la que los trayectos de trabajo tienen, cada uno de ellos, un trayecto de reserva (protección) preconfigurado.

En un sistema convencional, un fallo sobre una conexión particular provoca que una protección conmute a un trayecto de reserva solamente para esa conexión. En la presente invención, un nodo que gestiona un grupo de protección (A) provoca que se produzca la conmutación de una protección para el grupo de conexiones del grupo (A) cuando la señalización de fallo recibida por el nodo cumple una cierta condición, o conjunto de condiciones. Por ejemplo, la condición puede ser que por lo menos el 50% de las conexiones del grupo de protección informe sobre un fallo.

La Figura 2 muestra un escenario en el cual se ha producido un fallo 21 sobre el enlace entre los Nodos N2 y N5. Se supondrá que las conexiones LSP1-6, LSP2-6 y LSP3-6 son transportadas todas ellas por el mismo enlace físico que está afectado por el fallo 21. Considérese que el nodo N6 está configurado para provocar una conmutación de protección para todas las conexiones en el grupo A cuando el 50% de las conexiones en el grupo A informa sobre un fallo. Esto requiere que dos de las cuatro conexiones informen sobre un fallo. Tras la aparición del fallo 21, los mecanismos de señalización OAM sobre cada una de las conexiones informarán al nodo N6 de que las conexiones están defectuosas. Por ejemplo, si la señalización de CC periódica para LSP2-6 y LSP3-6 no es recibida por el nodo N6 dentro del periodo predeterminado, el nodo N6 cumplirá la condición de fallo para el grupo A y provocará que se declare una condición de fallo. Una vez que el Nodo N6 detecta que dos de los túneles LSP en el grupo de protección A han fallado, se lleva a cabo una conmutación de protección inmediata, de acuerdo con el esquema de protección concreto usado, para la totalidad de las conexiones en el grupo A. No es necesario que el Nodo N6 espere a que ningún otro miembro del grupo de protección A informe sobre una condición de fallo. Por lo tanto, el nodo N6 no espera a que LSP1-6 informe sobre el fallo 21. Evidentemente, el procesado de detección puede continuar sobre las otras conexiones. En este ejemplo, el trayecto de trabajo de LSP4-6 no está defectuoso, pero la operación de conmutación de protección para el grupo A se llevará a cabo sobre LSP4-6 debido a su pertenencia al grupo de protección A.

La Figura 3 muestra un conjunto de trayectos de reserva B1-6, B2-6, B3-6, B4-6 para los trayectos de trabajo LSP1-6, LSP2-6, LSP3-6, LSP4-6. El trayecto de reserva B1-6 conecta el nodo N1 al nodo N6 por medio de un encaminamiento diferente al trayecto de trabajo de LSP1-6. Un trayecto de reserva pasará típicamente por uno o más nodos intermedios que, por motivos de claridad, no se muestran en la Figura 3. La Figura 3 muestra esquemáticamente tres trayectos de reserva encaminados de manera diferente, aunque es posible que múltiples trayectos de reserva compartan por lo menos algunos recursos físicos.

Si la flexibilidad contra una única avería es suficiente, el mecanismo descrito hasta el momento es satisfactorio. Son deseables algunos mecanismos adicionales, si se requiere flexibilidad contra fallos dobles. La Figura 4 muestra un escenario en el cual se ha producido un fallo 21 sobre el enlace físico entre los Nodos N2 y N5 y, adicionalmente, se

ha producido un fallo 22 sobre el trayecto de reserva B4-6 entre los Nodos N4 y N6. El trayecto de reserva B4-6 entre los Nodos N4 y N6 es el trayecto de reserva para LSP4-6. Si el grupo de protección A se comporta como se ha descrito previamente, se transferirá tráfico desde el trayecto de trabajo LSP4-6 al trayecto de reserva B4-6 sobre el cual existe el fallo 22. Esto no es deseable, por lo tanto, se requiere un comportamiento diferente cuando se produce una condición de fallo sobre un trayecto de reserva. El trayecto de trabajo LSP4-6 correspondiente al trayecto de reserva sobre el cual se ha producido el fallo 22 se elimina temporalmente del grupo de protección A. La máquina de estados finitos que activa el mecanismo de protección debe llevar a cabo una acción diferente ya que el Fallo de Señal (SF) del trayecto de reserva tiene una prioridad mayor que cualquier acción que conmute tráfico al trayecto defectuoso.

Existe otro escenario a considerar. En un caso en el que se ha producido un fallo 21 sobre el enlace físico entre los Nodos N2 y N5, se produce una conmutación de protección para la totalidad de los trayectos de trabajo en el grupo de protección A. después de que se ha producido la conmutación de protección, puede producirse un fallo sobre el trayecto de reserva B4-6. No obstante, puesto que el trayecto de trabajo original LSP4-6 no era responsable del fallo, el mismo sigue siendo un trayecto válido para transportar tráfico entre los nodos N4 y N6. Por lo tanto, este miembro (LSP4-6) se elimina temporalmente del grupo de protección y se trata de manera independiente, de manera que el tráfico puede usar el trayecto inicial (no defectuoso) LSP4-6.

También se puede aplicar el mismo mecanismo de eliminación temporal de un miembro del grupo de protección cuando el trayecto de reserva está defectuoso sin presencia de ninguna otra avería, tal como se muestra en la Figura 5. En este caso, aún cuando no haya ningún impacto sobre el grupo debido a la avería del trayecto de protección de LSP4-6, el LSP4-6 de trabajo se eliminará temporalmente del grupo de protección, hasta que su trayecto de reserva asociado esté disponible nuevamente. De esta manera, incluso en caso de dobles fallos que puedan afectar a un grupo de protección, como en el ejemplo proporcionado en la Figura 4, no se producirá ningún comportamiento desviado. De hecho, no se producirá nunca ninguna conmutación a un recurso defectuoso y no se producirá nunca ninguna desalineación de estado entre los miembros del grupo.

Para los comportamientos recién descritos, el nodo N6 requiere un conocimiento del estado administrativo (es decir, trabajo o protección) de las conexiones dentro del grupo. En el ejemplo recién descrito, el miembro LSP4-6 se devuelve al grupo de protección en cuanto vuelve al mismo estado que los otros miembros del grupo de protección.

Existen dos formas principales en las cuales puede funcionar la conmutación de protección: (i) funcionamiento con reversión y (ii) funcionamiento sin reversión. Con el funcionamiento con reversión, se usa siempre el mismo trayecto de red como trayecto de trabajo para una conexión entre un par de nodos, en ausencia de un fallo. Cuando se produce un fallo sobre el trayecto de trabajo, se transfiere el tráfico desde el trayecto de trabajo a un trayecto de reserva entre el par de nodos. Cuando se repara el fallo, el tráfico se transfiere (revierte) al trayecto de trabajo original. Con el funcionamiento sin reversión, el tráfico se transfiere a un trayecto de reserva cuando se produce un fallo sobre el trayecto de trabajo. A continuación, el trayecto de reserva se designa como el trayecto de trabajo nuevo, y no se produce ninguna operación subsiguiente para transferir (revertir) tráfico al trayecto que sirvió originalmente como trayecto de trabajo.

Se ha resumido anteriormente cómo un conjunto de conexiones en un grupo de protección se trata normalmente como un único grupo, y cómo el tráfico se conmuta normalmente para todas las conexiones del grupo cuando se cumple una condición. Se ha descrito también cómo existen algunas situaciones en las que es deseable eliminar una conexión, o múltiples conexiones, del grupo. La Figura 6 muestra una tabla que resume las formas de gestionar el movimiento de miembros hacia y fuera de un grupo de protección. En general, para el funcionamiento tanto con reversión como sin reversión, se saca una conexión de un grupo de protección: (i) cuando el trayecto de trabajo designado está proporcionando servicio y el trayecto de reserva asociado a esa conexión es responsable de un fallo, (ii) cuando el trayecto de reserva designado está proporcionando servicio y el trayecto de trabajo asociado a la conexión es responsable de un fallo. Para un funcionamiento sin reversión, el tráfico permanece sobre el trayecto de reserva tras un fallo, convirtiéndose el trayecto de reserva en el nuevo trayecto de trabajo. La conexión se puede devolver al grupo de protección cuando hay disponible un trayecto alternativo. También es posible aplicar el esquema a un grupo mixto (es decir, algunas conexiones en el grupo son con reversión, otras conexiones en el grupo son sin reversión), aunque esto es un caso improbable ya que un operador de red habitualmente elegirá una estrategia de protección única. Para un grupo mixto, una conexión puede permanecer fuera del grupo de protección cuando se transporta tráfico sobre el trayecto de reserva.

La Figura 7 muestra esquemáticamente un nodo 40 de red que gestiona un grupo de protección, tal como el nodo N6 de la Figura 1. El nodo 40 de red tiene interfaces 41, 42 de red para recibir unidades de transporte (por ejemplo, paquetes o tramas de datos) de otros nodos de red. Las interfaces 41, 42 de red terminan las conexiones de trayectos de trabajo y las conexiones de trayectos de reserva descritas previamente. Las interfaces 41, 42 de red también reciben mensajes OAM desde otros nodos de red. El nodo 40 también tiene interfaces 43, 44 para reenviar tráfico a otros nodos. Si el nodo 40 es un nodo de borde de una red, el mismo está provisto de un conjunto de interfaces 43 de cliente para reenviar unidades de transporte recibidas a clientes.

El controlador 60 comprende un conjunto de módulos funcionales 61 a 65 que controlan el funcionamiento del nodo 40 de red. El módulo 63 de reenvío de plano de datos lleva a cabo el reenvío normal de unidades de transporte de acuerdo con una tabla de reenvío almacenada localmente. Esta es una función convencional de un nodo y no es necesario que se describa de forma adicional. El módulo 64 de procesado OAM soporta funcionalidades OAM. Envía y recibe señalización OAM 50, 51. Recibe señalización OAM, tal como señalización de Comprobación de Continuidad y FDI, desde interfaces 41, 42 de red y usa esto para determinar la aparición de un fallo/avería de un enlace o nodo. Un módulo 65 de grupo de protección recibe entradas 52 desde el módulo OAM 64 y ejecuta una lógica (mostrada en las Figuras 8A y 8B) para determinar cuándo debería producirse una conmutación a un trayecto de reserva. El módulo 64 del grupo de protección incluye: condiciones 66 que deben cumplirse para declarar el grupo de protección como defectuoso y para conseguir que se produzca una conmutación de protección para el grupo completo de conexiones; miembros 67 de grupo para los cuales se aplica el grupo de protección; miembros individuales 68 que se eliminan de los miembros 67 del grupo y para los cuales se aplica la protección individual.

El motor 45 de protección lleva a cabo una conmutación de tráfico para los miembros del grupo y miembros individuales sobre la base de entradas 53 del módulo 65 de grupo de protección.

El controlador 60 también puede comprender un módulo 61 de plano de control que recibe señalización 56 de plano de control desde las interfaces 41, 42 de red. El módulo 61 de plano de control recibe señalización 56 de plano de control para configurar un grupo de protección, y emitir instrucciones 54 con el fin de configurar el módulo 65 de grupo de protección. El controlador también puede comprender un módulo 62 de plano de gestión que recibe señalización de plano de gestión desde las interfaces 41, 42 de red. El módulo 62 de plano de gestión recibe señalización de plano de gestión para configurar un grupo de protección, y emitir instrucciones 55 con el fin de configurar el módulo 65 del grupo de protección. Aunque no se muestra en la Figura 7, el controlador 60 también puede tener una entrada para recibir señalización de configuración desde un Terminal de Dispositivo Local.

El conjunto de módulos mostrados en la Figura 7 se puede implementar como bloques de código ejecutable por máquina, los cuales se ejecutan mediante un procesado de propósito general o mediante uno o más procesadores o aparatos de procesado dedicados. Los módulos se pueden implementar como hardware, o una combinación de hardware y software, por ejemplo, como una Matriz de Puertas Programables in Situ (FPGA), un Circuito Integrado de Aplicación Específica (ASIC) o un Producto Convencional de Aplicación Específica (ASSP). Aunque la funcionalidad del aparato se muestra como un conjunto de módulos independientes, se apreciará que un conjunto de menor, o mayor, tamaño, de módulos puede llevar a cabo la funcionalidad.

Las Figuras 8A y 8B muestran una realización de un método de funcionamiento de un modo N6 en una red. Las etapas 81 y 82 se refieren a la configuración inicial de conexiones en el nodo. La configuración se puede llevar a cabo localmente en el nodo, por ejemplo usando un Terminal de Dispositivo Local, mediante la señalización de plano de gestión (MP) o de plano de control (CP). En la etapa 81, el nodo (por ejemplo, el nodo N6 de la Figura 1) está configurado para formar parte de un trayecto de trabajo de una conexión y para formar parte de un trayecto de reserva de una conexión.

En la etapa 82, el nodo configura un grupo de protección. La configuración de un grupo de protección se puede producir en un tiempo posterior con respecto a la configuración inicial de conexiones en la etapa 81. El nodo puede recibir instrucciones para configurar el grupo de protección de varias maneras, tales como por medio del MP o el CP, o mediante configuración local del nodo. El grupo de protección es un grupo de conexiones para las cuales se producirá una conmutación de protección para todos los miembros del grupo una vez que se cumpla una condición de umbral (por ejemplo, un número de conexiones que informa sobre un fallo). La configuración de un Grupo de Protección incluye identificar conexiones que van a formar parte del mismo grupo y detalles de la condición, o condiciones, de umbral usadas para tomar una decisión de conmutación de protección. Los operadores de red configurarán de forma administrativa los miembros de los grupos de protección que pretenden usar en función de sus requisitos de red y del análisis de aparición de fallos en sus redes. A continuación, en función de la topología de la red y de los patrones de tráfico, decidirán qué umbral de avería de grupo de protección es apropiado para sus redes (es una especie de umbral de “sensibilidad”). Cuanto más alto sea el umbral, más tiempo puede que sea necesario para completar realmente la conmutación de protección del grupo completo. Cuanto más bajo sea el umbral, más probable será que se lleve a cabo una conmutación de protección sobre LSPs o PWs no defectuosos.

Las etapas 83 a 102 se refieren al funcionamiento del grupo de protección. En la etapa 83, cada conexión del grupo se monitoriza de una manera convencional, por ejemplo detectando mensajes de CC en un periodo de tiempo predeterminado, recibiendo un mensaje de FDI o recibiendo un mensaje de APS. También se monitorizan trayectos de reserva en relación con los fallos. Las etapas 84 y 88 usan los resultados de la monitorización llevada a cabo en la etapa 83. En la etapa 84 se realiza una comprobación sobre si se detectó un fallo en un trayecto de reserva. Si se detectó un fallo en un trayecto de reserva, entonces el trayecto de trabajo asociado a ese trayecto de reserva se elimina del grupo de detección de fallos en la etapa 85. El tráfico se puede transferir al trayecto de trabajo asociado al trayecto de reserva, si el trayecto de trabajo no es responsable del fallo. Este es el escenario descrito con respecto a la Figura 4. La etapa 86 detecta cuándo se repara el fallo en el trayecto de reserva. Cuando se repara el fallo, el método prosigue hacia la etapa 87 y el trayecto de trabajo asociado a ese trayecto de reserva se vuelve a

insertar en el grupo de protección.

Volviendo al procesado de los resultados de la etapa 83, la etapa 88 comprueba si se detectó un fallo en un trayecto de trabajo. Si no se detectó ninguna avería en un trayecto de trabajo particular, entonces el método prosigue hacia la etapa 89 y el trayecto del trabajo permanece en el grupo de protección, o se vuelve a insertar en el grupo de protección. Si se detectó una avería en un trayecto de trabajo particular, entonces el método prosigue hacia la etapa 90. Si el trayecto de trabajo ya está en un estado de protección, entonces no se requiere ninguna acción adicional. No obstante, si esta es la primera detección de la aparición de un fallo en el trayecto de trabajo, entonces el método prosigue hacia la etapa 91. El tráfico se transfiere desde el trayecto de trabajo al trayecto de reserva asociado y se incrementa un parámetro F, indicativo del número de trayectos de trabajo que están averiados. El método prosigue hacia la Figura 8B. La etapa 91 garantiza que el nodo actúa rápidamente cuando se observa que un trayecto de trabajo individual es responsable de un fallo.

La etapa 92 comprueba si este es el primer incremento del parámetro F. Si este es el primer incremento del parámetro F, en la etapa 93 se inicia un periodo de observación. Si no, el método prosigue hacia la etapa 94. La etapa 94 comprueba si el parámetro F tiene un valor mayor que un valor de umbral F_{TH}. Esto indica que se ha observado que por lo menos el número de umbral de miembros del grupo de protección es responsable de un fallo.

En la etapa 94, si el parámetro F tiene un valor menor que el valor de umbral F_{TH}, esto indica que se ha observado que un número menor que el número de umbral de miembros del grupo de protección son responsables de un fallo. La etapa 95 comprueba si se ha producido la expiración del periodo de observación. Si no se ha producido la expiración del periodo de observación, el método vuelve al punto A para continuar monitorizando las conexiones. Si se ha producido la expiración del periodo de observación, el método prosigue hacia la etapa 96 y elimina, del grupo de protección, todos los trayectos de trabajo para los cuales se ha transferido tráfico a trayectos de reserva. La etapa 97 reinicializa el tiempo de observación y el parámetro F. Opcionalmente, en la etapa 97, el método puede calcular un valor nuevo para el parámetro de umbral F_{TH} basándose en el número de conexiones activas que quedan en el grupo de protección, es decir, el número de conexiones que no se han eliminado del grupo en la etapa 96.

Volviendo a la etapa 94, si el parámetro F tiene un valor igual al, o mayor que el, valor de umbral F_{TH}, el método prosigue hacia la etapa 98 y se transfiere tráfico desde los trayectos de trabajo de todos los miembros del grupo de protección a trayectos de reserva respectivos. Debería entenderse que el tráfico de miembros individuales del grupo que se ha observado que es responsable del fallo ya se habrá transferido en la etapa 91 a un trayecto de reserva respectivo durante esta iteración del método, o una de las iteraciones anteriores del método. Solamente el tráfico de otros miembros del grupo de protección que aún tienen que informar sobre un fallo es el que todavía es necesario transferir en la etapa 98. La etapa 99 reinicializa el tiempo de observación y el parámetro F. La etapa 100 elimina la totalidad de los trayectos de trabajo del grupo de protección. La etapa 101 comprueba cuándo un trayecto alternativo está disponible nuevamente y, en la etapa 102, devuelve el trayecto de trabajo asociado al grupo de protección y vuelve al punto A. Las etapas 101 y 102 se repiten para cada trayecto que se eliminó en la etapa 100. La acción llevada a cabo en la etapa 98 en ocasiones tendrá el efecto de transferir tráfico desde un trayecto de trabajo que no sea responsable del fallo. Este es el escenario mostrado en la Figura 2, en donde un fallo 21 no afecta al trayecto de trabajo LSP4-6, aunque se transfiere tráfico desde LSP4-6 a B4-6 debido a que forma parte del grupo de protección A. Las conexiones que no son responsables de un fallo ya tienen un trayecto alternativo en funcionamiento y se pueden devolver al grupo de protección en la etapa 102. Esto se puede producir inmediatamente, o después de un tiempo configurable.

Para un funcionamiento sin reversión, el tráfico permanece en el trayecto al cual se transfirió tráfico en la etapa 91 ó 98 y no se requieren etapas adicionales. El trayecto que se está usando actualmente se considera el “trayecto proveedor de servicio” y el trayecto que no transporta actualmente tráfico se considera el “trayecto en espera”. Para el funcionamiento con reversión, el tráfico se transfiere posteriormente de vuelta al trayecto de trabajo designado cuando se repara el fallo.

El periodo de observación usado en las etapas 93 y 95 es un parámetro configurable. Una avería en la red es probable que provoque que todas las conexiones relevantes estén defectuosas aproximadamente al mismo tiempo. Existe cierto grado de incertidumbre puesto que no todos los mensajes OAM son síncronos. El periodo de observación permite que el método espere un periodo breve por otros mensajes de fallo. Como ejemplo práctico, considérese que se envían mensajes OAM cada 3,3 ms, con un fallo declarado después de 3,5 x 3,3 ms (=11,55 ms). El primer incremento de F se produce después de la primera detección de un fallo en 11,55 ms, y el periodo de observación se inicia también en este punto. Debería sucederse una “tormenta” de detecciones de averías. El periodo de observación se puede fijar, por ejemplo, a un valor de un par de ms, permitiéndose así que el nodo detecte una condición de fallo en la mayoría de las conexiones, sin necesidad de esperar a que todas las conexiones informen sobre una condición de fallo. Es posible fijar el valor de umbral F_{TH} a un valor de 1, de tal manera que el grupo completo de trayectos de trabajo se conmuta cuando un único trayecto de trabajo informa de un fallo. En este caso, no se requiere el periodo de observación y se omiten las etapas 92, 93, 97 del método que usan el periodo de observación.

Las Figuras 8A y 8B muestran una realización ventajosa de la invención en la que existe un trayecto de reserva (protección) preconfigurado para cada trayecto de trabajo. Al grupo de trayectos de trabajo se le denomina grupo de protección. La invención se puede aplicar al restablecimiento de tráfico, en el cual se configuran trayectos de reserva bajo demanda. Para una realización de restablecimiento de tráfico, el método mostrado en las Figuras 8A y 8B se adapta de tal manera que la etapa 83 únicamente monitoriza trayectos de trabajo (puesto que no existe ningún trayecto de reserva antes de que se detecte un fallo) y pueden omitirse las etapas 84 a 87. En las etapas 91 y 95, se configura un trayecto de reserva bajo demanda en el momento de llevar a cabo dichas etapas.

La Figura 7 muestra un nodo en el que se configura el grupo de recuperación. Otros nodos de la red se pueden adaptar para soportar la configuración del grupo de recuperación. Otros nodos que soportan la configuración del grupo de recuperación pueden incluir una Entidad de Gestión de Red, una entidad de Plano de Control y un Terminal de Dispositivo Local. Para configurar un grupo de recuperación, se señaliza información de configuración desde uno de estos otros nodos al nodo en el que se va a configurar el grupo de recuperación. Extensiones de los protocolos de señalización pueden transportar la información de configuración. La información de configuración incluye:

- información que identifica las conexiones que van a formar parte del grupo de recuperación;
- información que identifica el trayecto de reserva asociado a cada conexión;
- una condición, o condiciones, para provocar que el tráfico del grupo se conmute a trayectos de reserva (por ejemplo, el valor de umbral F_{TH});
- cualquier otro parámetro usado por el motor de protección, tal como la longitud del periodo de observación.

La descripción anterior se refiere a “eliminar” y “devolver” miembros de un grupo de recuperación/protección. Se entenderá que los datos correspondientes a un miembro no tienen que eliminarse físicamente de una lista de miembros del grupo. Un campo o bandera se puede fijar a “1” o “0” para indicar si un miembro particular está actualmente “dentro” o “fuera” de la lista de miembros del grupo de recuperación/protección.

En el caso de patrones de tráfico con concentradores en la red, tal como se produce típicamente con aplicaciones residenciales, el nodo de extremo de cabecera típicamente recogerá la totalidad, o la mayoría, del tráfico que llega desde nodos periféricos. El nodo del extremo de cabecera afronta la necesidad de terminar un número potencialmente enorme de túneles LSP, con su protección pertinente. Un mecanismo de señalización puede permitir un rendimiento incluso mayor informando al lado de transmisión que conmute un cierto número de conexiones (por ejemplo, túneles LSP o PWs) que pertenecen a un grupo de protección dado en el lado de recepción. Los grupos de protección en los puntos extremos típicamente no comprenderán los mismos miembros. Como ejemplo, el extremo de recepción comprenderá un superconjunto de miembros en comparación con el extremo de transmisión. Esto significa que en general será necesario intercambiar dicha señalización entre cada nodo de recepción y una serie de nodos de transmisión. No obstante, esta extensión es gestionable y requiere el intercambio de mensajes privativos o “mensajes de grupo” basados en normas entre el nodo de recepción y los nodos de transmisión asociados a un grupo de protección dado. En particular, el nodo N6 puede enviar mensajes ad-hoc (por medio de OAM o el plano de control) a los nodos fuente de las conexiones que pertenecen a un grupo de recuperación para informarles sobre el estado de sus conexiones, permitiendo así también que el otro extremo de las conexiones actúe. Esto es particularmente ventajoso para mecanismos de restablecimiento.

A los expertos en la materia se les ocurrirán modificaciones y otras realizaciones de la invención dada a conocer que disfruten del beneficio de las enseñanzas presentadas en las descripciones anteriores y los dibujos asociados. Por lo tanto, debe entenderse que la invención no se limitará a las realizaciones específicas dadas a conocer y que se pretende que dentro del alcance de esta exposición se incluyan modificaciones y otras realizaciones. Aunque en la presente se pueden utilizar términos específicos, los mismos se usan en un sentido genérico y descriptivo únicamente y no con fines limitativos.

REIVINDICACIONES

1. Método para llevar a cabo una detección de fallos y una recuperación de tráfico en un primer nodo (N6) en una red (5) orientada a conexión, comprendiendo la red una pluralidad de conexiones (LSP1-6, LSP2-6, LSP3-6, LSP4-6) que terminan en el primer nodo (N6), comprendiendo el método:

configurar (82) en el primer nodo (N6) un grupo (A) de recuperación que comprende por lo menos dos de la pluralidad de conexiones;
llevar a cabo una detección (83) de fallos sobre cada una de la pluralidad de conexiones en el grupo (A) de recuperación;
determinar (94) si se cumple por lo menos una condición de fallo de grupo de recuperación, basándose en los resultados de las detecciones de fallos llevadas a cabo sobre la pluralidad de conexiones en el grupo (A) de recuperación y:

cuando se cumple la por lo menos una condición de fallo del grupo de recuperación, conseguir (98) que el tráfico sobre la pluralidad de conexiones en el grupo (A) de recuperación se transfiera a trayectos de reserva
y **caracterizado porque**, cuando no se cumple la por lo menos una condición de fallo del grupo de recuperación, y se ha detectado (88) un fallo en una conexión del grupo (A) de recuperación, provocar (91) que el tráfico se transfiera desde esa conexión a un trayecto de reserva.

2. Método según la reivindicación 1, que comprende además cambiar dinámicamente el número de conexiones en el grupo de recuperación basándose en por lo menos una de: la transferencia de tráfico a trayectos de reserva; detecciones de fallos llevadas a cabo sobre trayectos de reserva.

3. Método según la reivindicación 2, que comprende eliminar temporalmente una conexión del grupo (A) de recuperación cuando se transfiere tráfico desde esa conexión en el grupo (A) de recuperación a un trayecto de reserva.

4. Método según la reivindicación 3, en el que la conexión se devuelve al grupo (A) de recuperación cuando la conexión está disponible nuevamente.

5. Método según la reivindicación 2, en el que una primera conexión (N4 a N6) se elimina temporalmente del grupo (A) de recuperación cuando se detecta un fallo en un trayecto de reserva asociado a la primera conexión (N4 a N6).

6. Método según la reivindicación 5, en el que la primera conexión se devuelve al grupo (A) de recuperación cuando el trayecto de reserva está disponible nuevamente.

7. Método según una cualquiera de las reivindicaciones 2 a 6, en el que por lo menos una de las conexiones en el grupo (A) de recuperación se hace funcionar de una manera sin reversión tras la transferencia de tráfico desde una conexión a un trayecto de reserva, permaneciendo el tráfico sobre el trayecto de reserva y devolviéndose la conexión al grupo de recuperación cuando hay disponible nuevamente un trayecto alternativo.

8. Método según una cualquiera de las reivindicaciones anteriores, en el que la por lo menos una condición de fallo del grupo de recuperación es la detección de un fallo en una proporción, o número, predeterminados de las conexiones en el grupo (A) de recuperación.

9. Método según la reivindicación 8, que comprende además calcular la proporción, o número, de las conexiones en el grupo (A) de recuperación requeridas para la declaración de la condición de fallo del grupo de recuperación sobre la base del número de conexiones activas en el grupo de recuperación.

10. Método según una cualquiera de las reivindicaciones anteriores, en el que por lo menos una de las conexiones en el grupo (A) tiene un nodo extremo diferente (N1, N2, N3, N4) a otras conexiones en el grupo.

11. Método según una cualquiera de las reivindicaciones anteriores, en el que por lo menos uno de los trayectos de reserva en el grupo (A) tiene un nodo extremo diferente (N1, N2, N3, N4) a otros trayectos de reserva en el grupo.

12. Método según una cualquiera de las reivindicaciones anteriores, en el que por lo menos uno de los trayectos de reserva es un trayecto de protección preconfigurado.

13. Método según una cualquiera de las reivindicaciones anteriores, en el que la detección de fallos comprende recibir señalización de Operaciones, Administración y Mantenimiento (OAM).

14. Método según una cualquiera de las reivindicaciones anteriores, en el que las conexiones son por lo menos una de: Conmutación por Etiquetas Multi-Protocolo (MPLS); Perfil de Transporte – Conmutación por Etiquetas Multi-

Protocolo (MPLS-TP); Ethernet Orientada a conexión.

15. Aparato para ser usado en un primer nodo (N6) de una red (5) orientada a conexión, comprendiendo la red una pluralidad de conexiones que terminan en el primer nodo (N6), comprendiendo el aparato:

una entrada para recibir instrucciones con el fin de configurar un grupo (A) de recuperación que comprende por lo menos dos de la pluralidad de conexiones;
un primer módulo (64) dispuesto para llevar a cabo una detección de fallos sobre cada una de la pluralidad de conexiones en el grupo (A) de recuperación;
un segundo módulo (65) dispuesto para determinar si se cumple por lo menos una condición de fallo del grupo de recuperación, basándose en los resultados de las detecciones de fallos llevadas a cabo sobre la pluralidad de conexiones en el grupo (A) de recuperación, estando dispuesto además el segundo módulo para:

cuando se cumple la por lo menos una condición de fallo del grupo de recuperación, provocar que el tráfico sobre la pluralidad de conexiones en el grupo (A) de recuperación se transfiera a trayectos de reserva
y **caracterizado porque** el segundo módulo (65) está dispuesto para, cuando no se cumple la por lo menos una condición de fallo del grupo de recuperación, y se ha detectado un fallo sobre una conexión en el grupo (A) de recuperación, provocar que se transfiera tráfico desde esa conexión a un trayecto de reserva.

16. Método para configurar la detección de fallos y la recuperación de tráfico en un primer nodo (N6) en una red (5) orientada a conexión, comprendiendo la red una pluralidad de conexiones que terminan en el primer nodo (N6), comprendiendo el método, en un nodo aparte del primer nodo (N6):

señalización para configurar un grupo (A) de recuperación en el primer nodo (N6), en donde la señalización:

define un grupo de recuperación que comprende por lo menos dos de la pluralidad de conexiones que terminan en el primer nodo (N6);
define por lo menos una condición de fallo de grupo de recuperación que se debe cumplir, para conseguir que se declare una condición de fallo de grupo de recuperación para todas las conexiones en el grupo (A) de recuperación;
en donde, cuando se cumple la por lo menos una condición de fallo de grupo de recuperación, el tráfico sobre la pluralidad de conexiones en el grupo (A) de recuperación se transferirá a trayectos de reserva y **caracterizado porque**, cuando no se cumpla la por lo menos una condición de fallo de grupo de recuperación, y se haya detectado un fallo en una conexión del grupo (A) de recuperación, se transferirá tráfico desde esa conexión a un trayecto de reserva.

17. Instrucciones legibles por máquina para conseguir que un procesador lleve a cabo el método según una cualquiera de las reivindicaciones 1 a 14 ó 16.

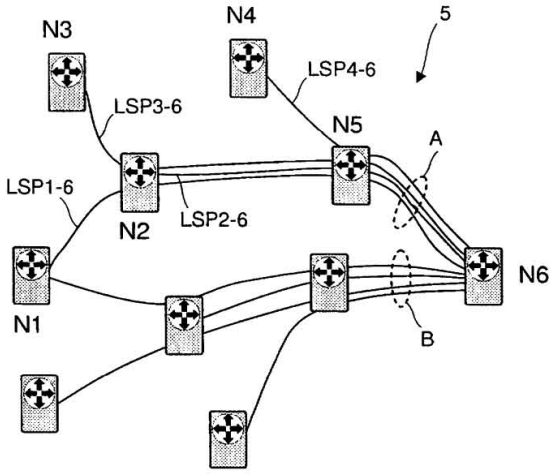

Fig. 1

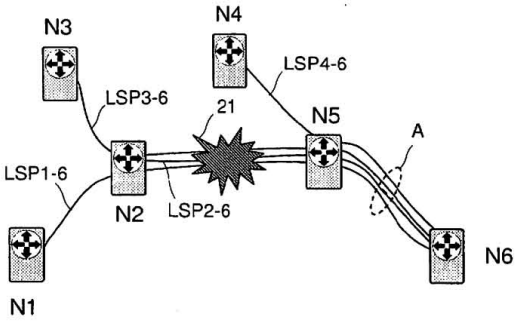
N3
N4
LSP4-6
LSP3-6
21
N5
A
LSP1-6
N2
LSP2-6
N6
N1

Fig. 2

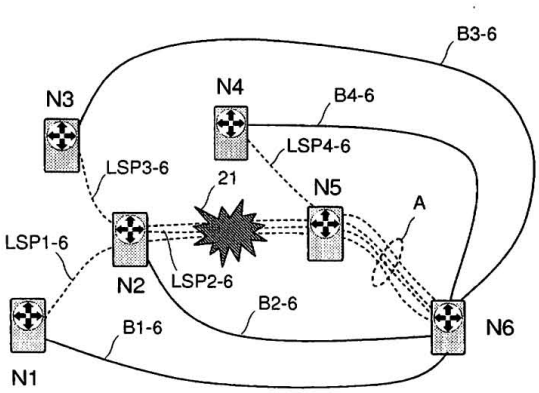
B3-6
N3
N4
B4-6
LSP4-6
LSP3-6
21
N5
A
LSP1-6
N2
LSP2-6
B2-6
B1-6
N6
N1

Fig. 3

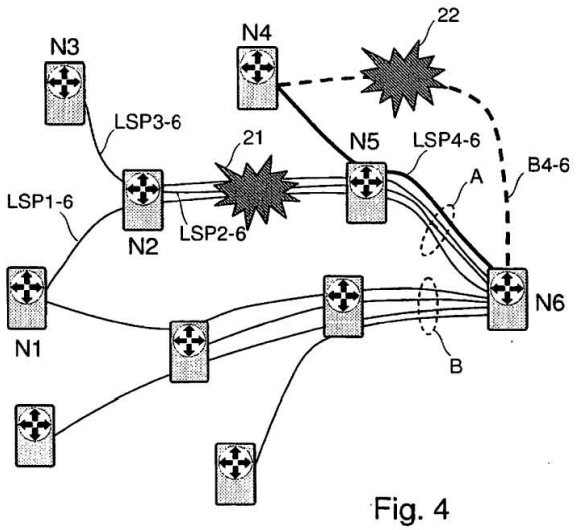

Fig. 4

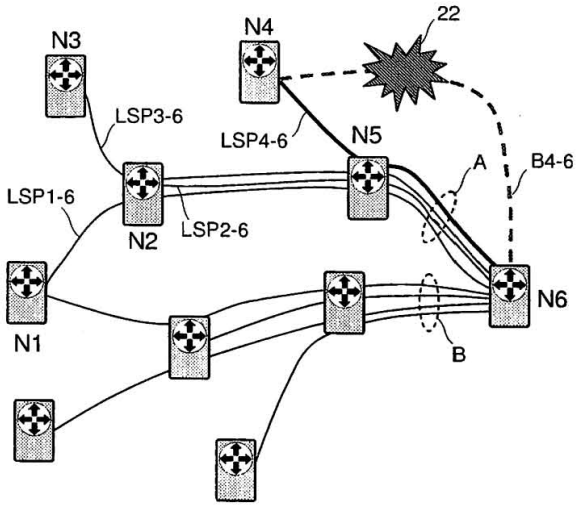

Fig. 5

Estado administrativo de la conexión	Estado del trayecto de trabajo	Estado del trayecto de protección	Acción	
			Con reversión	Sin reversión
El trayecto de trabajo está proporcionando servicio	activo	activo	Mantener en grupo de protección	Mantener en grupo de protección
El trayecto de trabajo está proporcionando servicio	activo	defectuoso		Sacar de grupo de protección
El trayecto de protecc. está proporcionando servicio	defectuoso	activo	Sacar de grupo de protección (1)	Sacar de grupo de protección (1)
El trayecto de protecc. está proporcionando servicio	activo	activo	- (2)	Mantener en o sacar de grupo de protección (3)
Están en vigor en las órdenes manuales	-	-	Sacar de grupo de protección	Sacar de grupo de protección

(1) esto puede ocurrir o bien para una conmutación de conexión individual o bien para una conmutación de grupo de protección
(2) en caso de funcionamiento con reversión, en cuanto el trayecto de trabajo resulte disponible nuevamente, el tráfico se transfiere de vuelta al mismo (habitualmente después de un tiempo de espera de restablecimiento)
(3) si todas las conexiones en el grupo son sin reversión, un comportamiento típico podría ser mantener la conexión en el grupo de protección.

N.B. si no todas las conexiones en el grupo son sin reversión, el operador de la red puede optar por sacar la conexión del grupo de protección o mantenerla en el grupo de protección

Fig. 6

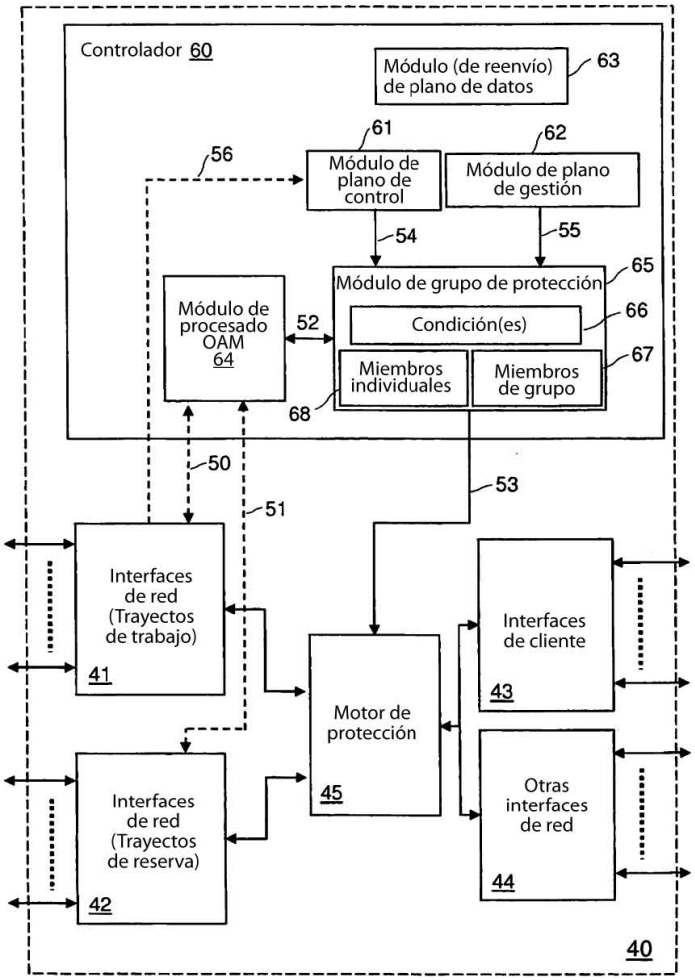
Controlador 60
Módulo (de reenvío) de plano de datos
63
61
62
56
Módulo de plano de control
Módulo de plano de gestión
54
55
65
Módulo de grupo de protección
Módulo de procesado OAM 64
52
Condición(es)
66
Miembros individuales
Miembros de grupo
67
68
50
53
51
Interfaces de red (Trayectos de trabajo)
41
Interfaces de cliente
43
Motor de protección
45
Interfaces de red (Trayectos de reserva)
42
Otras interfaces de red
44
40

Fig. 7

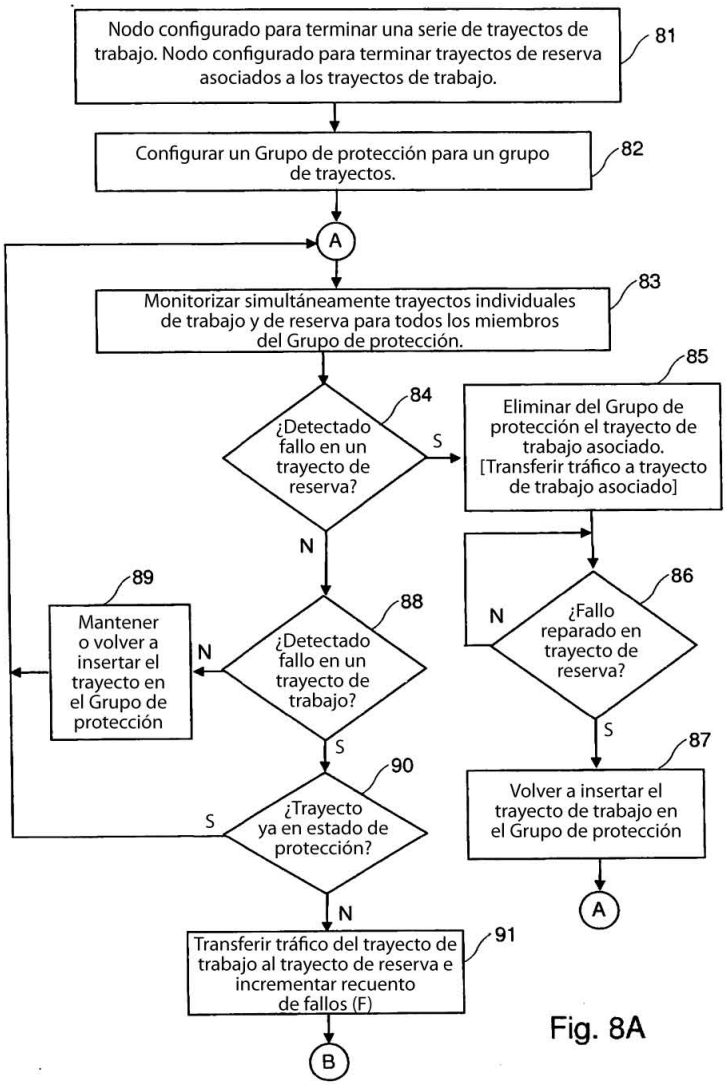
Nodo configurado para terminar una serie de trayectos de trabajo. Nodo configurado para terminar trayectos de reserva asociados a los trayectos de trabajo.
81
Configurar un Grupo de protección para un grupo de trayectos.
82
A
Monitorizar simultáneamente trayectos individuales de trabajo y de reserva para todos los miembros del Grupo de protección.
83
¿Detectado fallo en un trayecto de reserva?
84
S
Eliminar del Grupo de protección el trayecto de trabajo asociado. [Transferir tráfico a trayecto de trabajo asociado]
85
N
¿Fallo reparado en trayecto de reserva?
86
N
S
Volver a insertar el trayecto de trabajo en el Grupo de protección
87
A
¿Detectado fallo en un trayecto de trabajo?
88
N
Mantener o volver a insertar el trayecto en el Grupo de protección
89
S
¿Trayecto ya en estado de protección?
90
S
N
Transferir tráfico del trayecto de trabajo al trayecto de reserva e incrementar recuento de fallos (F)
91
B

Fig. 8A

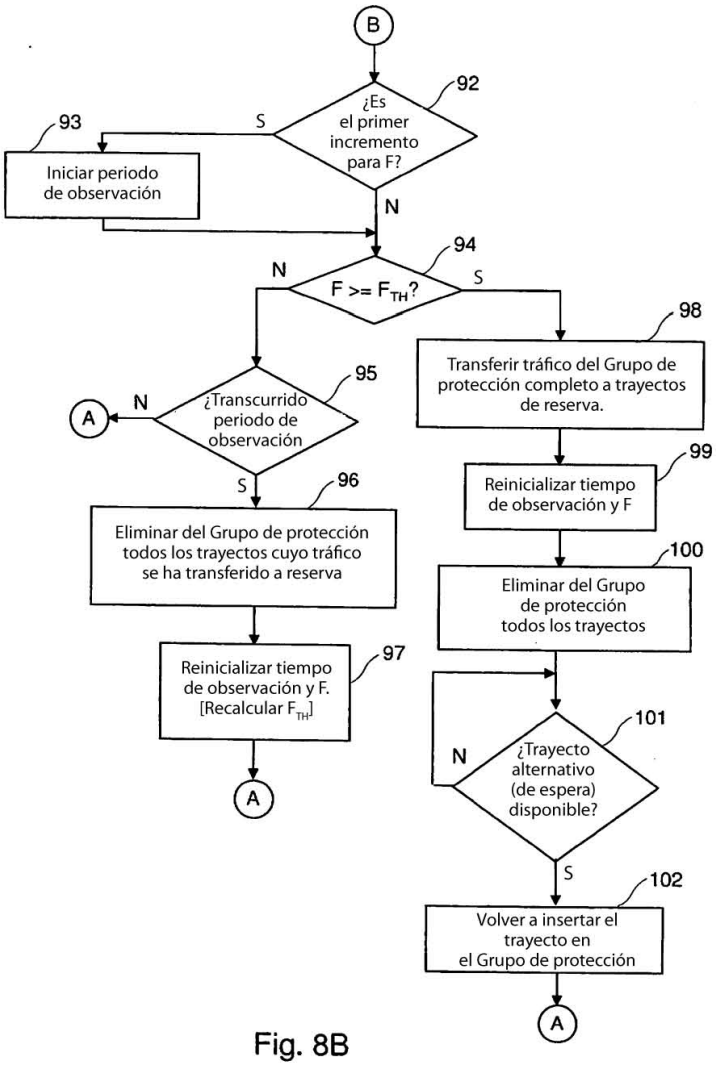
B
92
¿Es el primer incremento para F?
S
93
Iniciar periodo de observación
N
94
N
F >= F_TH?
S
98
Transferir tráfico del Grupo de protección completo a trayectos de reserva.
95
A
N
¿Transcurrido periodo de observación
S
96
Eliminar del Grupo de protección todos los trayectos cuyo tráfico se ha transferido a reserva
97
Reinicializar tiempo de observación y F. [Recalcular F_TH]
A
99
Reinicializar tiempo de observación y F
100
Eliminar del Grupo de protección todos los trayectos
101
N
¿Trayecto alternativo (de espera) disponible?
S
102
Volver a insertar el trayecto en el Grupo de protección
A

Fig. 8B