(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 463 101**

(51) Int. CI.:

H04L 12/24 (2006.01)
H04L 12/70 (2013.01)
H04L 12/46 (2006.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.11.2010 E 10833670 (2)**

(97) Fecha y número de publicación de la concesión europea: **26.03.2014 EP 2507944**

(54) Título: **Método y aparato para soportar detección de desacuerdo**

(30) Prioridad:

30.11.2009 US 265042 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.05.2014

(73) Titular/es:

TELEFONAKTIEBOLAGET LM ERICSSON (PUBL) (100.0%)
164 83 Stockholm, SE

(72) Inventor/es:

DING, ZHEMIN y
SALTSIDIS, PANAGIOTIS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método y aparato para soportar detección de desacuerdo

Campo técnico

La presente invención se refiere a las redes de comunicación, y en particular a métodos y disposiciones para la gestión de instancias de servicios que proporcionan soporte para detección de desacuerdo.

Antecedentes

La Gestión de Fallos de Conectividad (CFM – Connectivity Fault Management, en inglés), tal como se describe en el estándar IEEE Std 802.1ag – 2007, es un componente de operación, administración y mantenimiento clave para la Ethernet portadora. El estándar IEEE 802.1ag especifica protocolos, procedimientos y objetos gestionados para la detección, verificación y aislamiento de fallos de extremo a extremo. El estándar IEEE 802.1ag establece que los objetos gestionados, denominados Asociaciones de Mantenimiento (MAs – Maintenance Associations, en inglés) verifiquen la integridad de una única instancia de servicio intercambiando mensajes de CFM. El alcance de una MA es determinado por su Dominio de Gestión (MD – Management Domain, en inglés), que describe una región de red en la cual son gestionados la conectividad y el rendimiento. Cada MA asocia dos o más Puntos de Extremo de Asociación de Mantenimiento (MEPs – Maintenance Association Endpoints, en inglés) y permite que los Puntos Intermedios de Asociación de Mantenimiento (MIPs – Maintenance Association Intermediate Points, en inglés) soporten detección y aislamiento de fallos.

Se utiliza un protocolo de comprobación de continuidad para la detección de fallos. Cada MEP transmite periódicamente Mensajes de Comprobación de Continuidad (CCMs – Continuity Check Messages, en inglés) y rastrea los CCMs recibidos desde otros MEPSs en la misma asociación de mantenimiento.

Puentes de Red Troncal de Proveedor – Ingeniería del Tráfico (PBB-TE – Provider Backbone Bridging – Traffic Engineering, en inglés), tal como se describe en el estándar IEEE Std 802.1Qay – 2009, fue diseñada para proporcionar ingeniería del tráfico completa de las rutas en una red con puentes. La PBB-TE elimina la necesidad de que los dispositivos de red troncal lleven a cabo aprendizaje e inundación. En lugar de utilizar el Protocolo de Árbol de Expansión Múltiple / Protocolo de Árbol de Expansión Rápida (MSTP/RSTP – Multiple Spanning Tree Protocol / Rapid Spanning Tree Protocol, en inglés) para evitar bucles, la PBB-TE utiliza un plano de gestión o un plano de control externo para crear entradas de tabla de filtrado estático en los puentes de componente.

La PBB-TE es una tecnología de Ethernet orientada a la conexión que utiliza una tupla estadísticamente configurada que consiste en la Dirección de Destino de ESP (ESP-DA – ESP Destination Address, en inglés), Dirección de Fuente de ESP (ESP-SA – ESP Source Address, en inglés) e ID de VLAN de ESP (ESP-VID – ESP VLAN ID, en inglés) para crear una ruta de PBB-TE. La ruta provista se denomina una Ruta Conmutada de Ethernet (ESP – Ethernet Switched Path, en inglés). Dos ESPs de punto a punto con la misma ruta con las mismas direcciones de MAC de Puerto de Red Troncal de Abonado (CBP – Customer Backbone Port, en inglés) forman un servicio de MAC bidireccional, que se denomina una Instancia de Servicio de Ingeniería del Tráfico (TESI – Traffic Engineering Service Instance, en inglés) de punto a punto.

La PBB-TE soporta conmutación de protección de ruta bidireccional de 1:1. Dos TESIs de punto a punto son proporcionadas como un grupo de protección de TE (TEPG – TE Protection Group, en inglés). Una TESI está configurada como una TESI “de trabajo” y la otra como una TESI “de protección”. En condiciones normales, el tráfico es transmitido sobre la TESI de trabajo. En el caso de un fallo de la TESI de trabajo o una solicitud administrativa específica, el tráfico es conmutado a la TESI de protección.

Opcionalmente, las rutas protegidas de 1:1 de PBB-TE pueden estar configuradas para permitir compartición de carga. En el modo de compartición de carga, las TESIs que están asignadas a un grupo de protección de TE pueden ser reutilizadas en un número de grupos de protección de TE, permitiendo que una lista de diferentes instancias de servicios de red troncal sean distribuidas entre un conjunto de grupos de protección de TE independientes. En otras palabras, en el modo de compartición de carga, una TESI puede ser una TESI de protección en un grupo de protección de TE y ser una TESI de protección o de trabajo en otro grupo de protección.

Cada TESI es monitorizada por una MA independiente, y cada MA tiene dos MEPs. Uno está situado en un CBP de extremo cercano; el otro está situado en un CBP del extremo lejano. Cuando el MEP de extremo cercano detecta la pérdida de CCMs, lo notifica al MEP de extremo lejano enviando un CCM con una marca de Indicador de Defecto Remoto (RDI – Remote Defect Indicator, en inglés). Los dos extremos conocen el fallo (bien por pérdida de CCMs o recibiendo el CCM con la marca del RDI), de manera que la conmutación de protección a la TESI es llevada a cabo en ambos extremos. Cuando un fallo es eliminado, el tráfico puede ser conmutado de nuevo a la TESI de trabajo o puede permanecer en la TESI de protección de acuerdo con el modo configurado (reversible o no reversible).

Bajo ciertas condiciones de mal funcionamiento y/o configuración errónea del equipo, puede producirse un desacuerdo entre el mapeo de las instancias de servicio de red troncal a las TESIs apropiadas en el CBP de

finalización. Para mantener la adecuada operación de la red, este desacuerdo debe ser detectado y reportado al operador de la red. Entonces el operador de la red puede eliminar el defecto. Existen dos tipos de desacuerdo en la conmutación de protección bidireccional de 1:1:

- Desacuerdo incompleto de conmutación de protección; y
- Desacuerdo de configuración de Trabajo / de protección.

El desacuerdo incompleto de la conmutación de protección puede producirse, por ejemplo, si el extremo cercano, debido a un mal funcionamiento del hardware, falla al conmutar, pero envía un RDI al extremo lejano. El extremo lejano conmuta a la TESI de protección mientras que el extremo cercano está todavía en la TESI de trabajo. De manera similar, puede producirse también un desacuerdo cuando el extremo cercano conmuta a la TESI de protección, pero el extremo lejano falla en conmutar cuando recibe el RDI.

Un desacuerdo puede producirse también debido a una configuración errónea. Por ejemplo, un extremo puede ser configurado para enviar tráfico en la TESI de trabajo mientras que el otro extremo está configurado para enviar tráfico en la TESI de protección. De manera similar, un extremo puede estar configurado en el modo reversible mientras que el otro extremo está configurado en el modo no reversible. En este caso, el desacuerdo se produce cuando se elimina un fallo.

La PBB-TE soporta la protección de un grupo de TESIs atravesando una secuencia común de Puertos de Red de Proveedor (PNP – Provider Network Ports, en inglés). Tal secuencia de PNPs, junto con los repetidores y LANs de Puente que intervienen se denomina segmento de infraestructura o en ocasiones simplemente segmento. El grupo de TESIs está protegido de que se produzca un fallo de conectividad en algún sitio a lo largo del segmento de infraestructura, incluidos los PNPs del punto final. El método de protección no afecta a las porciones de las TESIs que se encuentran fuera del segmento; esto es, el alcance de la protección está limitado al segmento especificado. Este tipo de protección se denomina Protección de Segmento de Infraestructura, lo que se especifica en el estándar IEEE P802.1Qbf/D0.0.

Existen dos tipos de Conmutación de Protección de Infraestructura (IPS – Infrastructure Protection Switching, en inglés): IPS de 1:1 e IPS de M:1. En la IPS de 1:1 un segmento de trabajo y un segmento de protección asociado se dice que forman un grupo de protección de infraestructura (IPG – Infrastructure Protection Group, en inglés). En IPS de M:1 se proporcionan segmentos de protección adicionales. Cada uno de tales segmentos de protección adicionales se denomina segmento de protección alternativo. Un segmento de protección alternativo puede asumir la función del segmento de protección si se ha detectado un fallo de conectividad del segmento de protección. La IPS de M:1 requiere que todos los segmentos asociados con el IPG sean disjuntos entre sí. A cada Segmento de Protección Alternativo se le asigna una prioridad de selección única dentro del IPG. Cuando se detecta un fallo asociado con el segmento de protección, la función del segmento de protección es asumida por el segmento de protección alternativo que tiene la prioridad más alta (menor número) y para la cual no se ha detectado un fallo de conectividad.

La Protección de Segmento de infraestructura de PBB-TE también soporta el modo de compartición de carga de una manera similar a la conmutación de protección de TESI, permitiendo que un segmento esté asociado con más de un IPG. Por ejemplo, el operador puede designar un Segmento 1 como el segmento de trabajo de un IPG1 y el Segmento 2 como el segmento de protección del IPG1. El operador puede a la vez designar el Segmento 2 como el segmento de trabajo de un IPG2 y el Segmento 1 como el segmento de protección del IPG2. En este caso, la misma MA proporciona la monitorización del Segmento 1 en el IPG1 y en el IPG2.

La solicitud de patente internacional WO2009/127931 sugiere utilizar un campo del tráfico en los CCMs para indicar el estado del tráfico, por ejemplo si se transmite tráfico en la TESI monitorizada por los CCMs. Si el campo del tráfico de los CCMs de un MEP recibidos y transmitidos no coincide durante un periodo de tiempo predeterminado se detecta un desacuerdo. No obstante, el campo del tráfico soportado en los MEPs de PBB-TE puede no ser suficiente para detectar un defecto de desacuerdo en un modo de compartición de carga de la conmutación de protección de ruta bidireccional de 1:1 de PBB-TE o de la Protección de Segmento de Infraestructura de PBB-TE. El campo del tráfico puede indicar si existe o no tráfico en una TESI o segmento de infraestructura específicos, pero en caso de compartición de carga el tráfico en la TESI del segmento de infraestructura puede ser asociado con varios grupos de protección de TE o grupos de protección de infraestructura diferentes.

Compendio

Un objeto de la presente invención es proporcionar un método y aparato para la gestión de instancias de servicios que proporciona soporte para la detección de desacuerdo. El objeto presentado anteriormente se consigue por medio de un método y de un nodo de red de acuerdo con las reivindicaciones independientes.

Una primera realización proporciona un método para la gestión de instancias de servicios en un primer nodo de red de una red de comunicación. El método comprende monitorizar una pluralidad de rutas de red bidireccionales y distintas para transportar un número de instancias de servicios desde el primer nodo de red a un segundo nodo de

red. Las rutas de red forman un grupo de protección asociado con una respectiva instancia de servicio o grupo de instancias de servicios. La monitorización de las rutas de red incluye el envío continuo y periódico de Mensajes de Comprobación de Continuidad (CCMs – Continuity Check Messages, en inglés) en una ruta de red monitorizada al segundo nodo de red. En respuesta a la ocurrencia de un evento predeterminado, se incluye un bit de indicación en los CCMs, que son enviados en la ruta de red monitorizada durante un primer periodo de tiempo predeterminado tras la ocurrencia del evento predeterminado. El bit de indicación indica la presencia de un elemento de información de desacuerdo en el CCM que incluye el bit de indicación. El elemento de información de desacuerdo incluye información que especifica, para cada grupo de protección que la ruta de red monitorizada es un miembro de, estado del tráfico de una ruta de red de trabajo y de una ruta de red de protección del grupo de protección.

Una segunda realización proporciona un nodo de red para su uso en una red de comunicación. El nodo de red comprende un número de entidades de Operación, Administración y Gestión, OAM (Operation, Administration and Management, en inglés) configuradas para monitorizar una pluralidad de rutas de red bidireccionales y distintas para transportar un número de instancias de servicios desde el nodo de red a otro nodo de red. Las rutas de red forman un grupo de protección asociado con una respectiva instancia de servicio o grupo de instancias de servicios. Las entidades de OAM están configuradas para enviar continua y periódicamente Mensajes de Comprobación de Continuidad (CCMs – Continuity Check Messages, en inglés), en una ruta de red monitorizada al otro nodo de red. Las entidades de OAM están configuradas para, en respuesta a la ocurrencia de un evento predeterminado, incluir un bit de indicación en los CCMs, que son enviados en la ruta de red monitorizada durante un primer periodo de tiempo predeterminado tras la ocurrencia del evento predeterminado. El bit de indicación indica la presencia de un elemento de información de desacuerdo en el CCM que incluye el bit de indicación. El elemento de información de desacuerdo incluye información que especifica, para cada grupo de protección, que la ruta de red monitorizada es un miembro de, estado del tráfico de una ruta de red de trabajo y de una ruta de red de protección del grupo de protección.

Una ventaja de algunas realizaciones descritas en esta memoria es que proporcionan más posibilidades de detección de desacuerdo en el modo de compartición de carga.

Otra ventaja es que las realizaciones presentadas en esta memoria proporcionan una simple mejora del CCM basada en la arquitectura del hardware existente, con poco impacto en los estándares existentes.

Otra ventaja es que ciertas realizaciones evitan aumentar la complejidad del procesamiento de CCM limitando la transmisión del elemento de información de desacuerdo a un periodo de tiempo limitado tras la ocurrencia de un evento predeterminado que podría provocar un desacuerdo. El bit de indicación que se utiliza para indicar la presencia del elemento de información de desacuerdo en el CCM puede ser generalizado para indicar que existe un TLV especial unido al CCM para una futura extensión del CCM.

Otra invención más es que algunas realizaciones presentadas son aplicables tanto a la PBB-TE como a la protección de segmento de infraestructura de PBB-TE.

Otras ventajas y características de las realizaciones de la presente invención resultarán evidentes con la lectura de la siguiente descripción detallada junto con los dibujos.

Breve descripción de los dibujos

Las Figs. 1a y 1b son diagramas de bloques esquemáticos que ilustran una configuración de PBB-TE de acuerdo con una realización en operación normal y en situación de desacuerdo respectivamente.

La Fig. 2a y la Fig. 2b son diagramas de bloques esquemáticos que ilustran una configuración de protección de segmento de infraestructura de PBB-TE en operación normal y en un modo de protección respectivamente.

La Fig. 3 es un diagrama de bloques esquemático que ilustra una configuración de Conmutación de Protección de Infraestructura de M:1.

Las Figs. 4a y 4b son diagramas de bloques esquemáticos que ilustran una subsección de la configuración de Conmutación de Protección de Infraestructura de M:1 de la Fig. 3 en operación normal y en una situación de desacuerdo según una realización.

La Fig. 5 es un diagrama de flujo que ilustra una realización de un método para la gestión de instancias de servicios que proporciona soporte para la detección de desacuerdo.

La Fig. 6 es un diagrama de flujo que ilustra una realización alternativa de un método para la gestión de instancias de servicios que proporciona soporte para la detección de desacuerdo en un CCM recibido.

La Fig. 7 es un diagrama de bloques esquemático que ilustra una realización de un nodo de red para la gestión de instancias de servicios con soporte para la detección de desacuerdo.

La Fig. 8 es un diagrama de bloques esquemático que ilustra una realización alternativa de un nodo de red para la gestión de instancias de servicios con soporte para la detección de desacuerdo.

Las Figs. 9a, 9b y 9c son diagramas de bloques esquemáticos que ilustran un formato de cabecera de CFM, un formato de un campo de Marcas de un CCM, y un formato de un TLV de desacuerdo de acuerdo con las realizaciones de ejemplo presentadas en esta memoria.

Descripción detallada

La presente invención se describirá ahora con mayor profundidad en lo que sigue con referencia a los dibujos que se acompañan, en los cuales se muestran realizaciones preferidas de la invención. Esta invención puede, no obstante, ser puesta en práctica de muchas formas diferentes y no debe ser considerada como limitada a las realizaciones presentadas en esta memoria; por el contrario, estas realizaciones están proporcionadas para que esta descripción sea profunda y completa, e contenga completamente el alcance de la invención para los expertos en la materia. En los dibujos, signos de referencia iguales se refieren a elementos iguales.

La Fig. 1 ilustra una parte de una red de comunicación 1 que incluye una configuración de Puentes de Red Troncal de Proveedor – Ingeniería del Tráfico (PBB-TE – Provider Backbone Bridging –Traffic Engineering, en inglés) para transportar tráfico entre un extremo lejano (también llamado Componente-B Oeste) 2 y un extremo cercano (también llamado Componente-B Este) 3. El extremo lejano 2 incluye un Puerto de Red Troncal de Abonado (CBP – Customer Backbone Port, en inglés) 4 y los Puertos de Red de Proveedor (PNPs – Provider Network Ports, en inglés) 6a y 6b. El extremo cercano 3 incluye un CBP 5 y los PNPs 6c y 6d. Se ilustran dos rutas de red distintas y bidireccionales entre el extremo cercano 3 y el extremo lejano 2 en forma de una primera y una segunda Instancia de Servicio de Ingeniería del Tráfico (TESI – Traffic Engineering Service Instance, en inglés) 7 y 8. Cada TESI está monitorizada por una Asociación de Mantenimiento MA (Maintenance Association, en inglés) independiente, y cada MA tiene dos MEPs. Uno está situado en el CBP 4 del extremo lejano; el otro está situado en el CBP 5 del extremo cercano. Así el CBP 4 se ilustra incluyendo un MEP 9a asociado con la primera TESI 7 y un MEP 9b asociado con la segunda TESI 8, mientras que el CBP 5 se ilustra incluyendo un MEP 9c asociado con la primera TESI 7 y un MEP 9d asociado con la segunda TESI 8. La Fig. 1a ilustra un modo de compartición de carga. El tráfico relativo a las instancias de servicios 10a, 10b y 10c, que en este ejemplo son servicios de red troncal, es transportado en las TESIs 7 y 8. Las TESIs 7 y 8 forman grupos de protección de Ingeniería del Tráfico (TE – Traffic Engineering, en inglés) asociados con los respectivos servicios de red troncal. Se asume en este ejemplo que A, B y C se utilizan como identidades de grupo de protección para referirse a los respectivos grupos de protección asociados con los respectivos servicios de red troncal 10a, 10b y 10c. En el grupo de protección de TE A la primera TESI 7 es la TESI de trabajo y la segunda TESI 8 es la TESI de protección. En el grupo de protección de TE B, la primera TESI 7 es la TESI de trabajo y una tercera TESI (no ilustrada por simplificación) es la TESI de protección y en el grupo de protección de TE C, la segunda TESI 8 es la TESI de trabajo y una cuarta TESI (no ilustrada por simplificación) es la TESI de protección. En la Fig. 1a se ilustra la operación normal, lo que implica que la primera TESI 7 transporta tráfico relativo a los grupos de protección de TE A y B, correspondientes a los servicios de red troncal 10a y 10b respectivamente, mientras que la segunda TESI transporta tráfico relativo al grupo de protección de TE C, correspondiente al servicio de red troncal 10c.

Cada MEP 9a – d transmite periódicamente Mensajes de Comprobación de Continuidad (CCMs – Continuity Check Messages, en inglés) 11 y rastrea los CCMs recibidos de otros MEPs en la misma asociación de mantenimiento. Si por ejemplo el MEP de extremo cercano 9b detecta pérdida de CCMs 11, lo notifica al extremo lejano MEP 9a enviando un CCM con una marca de Indicador de Defecto Remoto (RDI – Remote Defect Indicator, en inglés). Los dos extremos conocen el fallo (bien por pérdida de CCMs o recibiendo el CCM con la marca de RDI), así que la conmutación de protección para la TESI de protección va a ser a continuación ejecutada en ambos extremos. Puesto que la primera TESI es la TESI de trabajo tanto para el grupo de protección de TE A como para el grupo de protección de TE B en este ejemplo de compartición de carga, los dos grupos de protección A y B deberían conmutar a sus respectivas TESIs de protección. Cuando se elimina el fallo, el tráfico puede ser conmutado de nuevo a la primera TESI 7 ó puede permanecer en la TESI o TESIs de protección de acuerdo con el modo configurado (reversible o no reversible) de los respectivos grupos de protecciones A y B.

Como se ha mencionado anteriormente existen diferentes tipos de desacuerdo que pueden producirse en la conmutación de protección bidireccional de 1:1. Un ejemplo de desacuerdo incompleto de conmutación de protección se describe en la Fig. 1b. En este ejemplo, debido a cierto mal funcionamiento del hardware, el extremo cercano 3 falla en conmutar el grupo de protección de TE A a la TESI de protección pero envía un RDI 14 al extremo lejano 2. El extremo lejano conmuta a la TESI de protección para el grupo de protección de TE A, mientras que el extremo cercano está aún en la TESI de trabajo. De manera similar, puede producirse también un desacuerdo cuando el extremo cercano 3 conmuta a la TESI de protección pero el extremo lejano 2 falla en conmutar cuando recibe el RDI. Resulta deseable detectar y reportar cualquier desacuerdo a un operador o a un Sistema de Gestión de Red NMS (Network Management System, en inglés) (12) lo antes posible.

Puede producirse también un desacuerdo debido a una configuración errónea. Por ejemplo, un extremo está configurado para enviar tráfico en la TESI de trabajo mientras que el otro extremo está configurado para enviar

tráfico en la TESI de protección. Otra situación en la cual puede aparecer un desacuerdo es cuando el otro extremo está configurado como modo no reversible. El desacuerdo se produce cuando se elimina un fallo.

Si los MEPs 9a – d soportan el campo del tráfico anteriormente mencionado de los CCMs, el desacuerdo puede ser detectado en un modo de operación no compartido. El campo del tráfico puede ser uno de cuatro bits reservados en un campo de marcas del CCM. Este bit indica el estado del tráfico, es decir, si se transmite o no tráfico en la TESI monitorizada por el CCM. El desacuerdo se detecta en uno de los MEPs cuando el campo del tráfico de los CCMs transmitidos y los CCMs recibidos no coincide durante un periodo de tiempo (por ejemplo 50 ms o más). El defecto de desacuerdo es eliminado cuando el correspondiente MEP recibe el primer CCM que indica el mismo campo del tráfico que los CCMs transmitidos desde el MEP.

Las Figs. 2a y 2b son diagramas de bloques esquemáticos que ilustran la Conmutación de Protección de Infraestructura (IPS – Infrastructure Protection Switching, en inglés) de 1:1, donde un segmento es terminado en los puertos PNP de los Puentes de Núcleo de Red Troncal (BCBs – Backbone Core Bridges, en inglés) 22. Los BSBs 22 se denominan Puentes de Extremo Final de Segmento (SEBs – Segment Endpoint Bridges, en inglés) y un puente 23 en el interior del segmento se denomina un Puente Intermedio de Segmento (SIB – Segment Intermediate Bridge, en inglés). Los BCBs 21 exteriores al segmento y los puentes de Borde de Red Troncal de IP (IP-BEBs - IP Backbone Edge Bridges, en inglés) 20 se ilustran también en las Figs. 2a y 2b. Una TESI 24 y una TESI 25 atraviesan un segmento de trabajo 26 en operación normal, como se ilustra en la Fig. 2a. Se proporciona un segmento de protección 27 para permitir la conmutación de protección de las TESIs 24, 25. El segmento de trabajo 26 y el segmento de protección 27 son disjuntos pero terminan en el mismo par de SEBs 22. El segmento de trabajo 26 y el segmento de protección 27 asociado se dice que forman un Grupo de Protección de Infraestructura (IPG – Infrastructure Protection Group, en inglés).

Cuando se detecta un fallo de conectividad en el nodo de red de trabajo 26 ó como resultado de una orden administrativa, los SBSs 22 redirigen las TESIs 24, 25 asociadas con el segmento de trabajo 26 al segmento de protección 27 tal como se muestra en la Fig. 2b.

Un ejemplo de IPS de M:1 se muestra en la Fig. 3. Los elementos ilustrados en la Fig. 3 corresponden a los elementos ilustrados en las Figs. 2a y 2b con la adición de los segmentos de protección alternativos 28 y 29. A cada segmento de protección alternativo provisto se le asigna una prioridad de selección dentro del IPG. Cuando se detecta un fallo asociado con el segmento de protección 27, la función del segmento de protección es asumida por el segmento de protección alternativo 28 ó 29 que tiene la prioridad más alta (número menor) y para el cual no se ha detectado un fallo de conectividad.

Los inventores se han dado cuenta de que el campo del tráfico anteriormente mencionado soportado en los MEPs de PBB-TE puede no ser suficiente para detectar desacuerdos en el modo de compartición de carga de la conmutación de protección de ruta bidireccional de 1:1 de PBB-TE o de Protección de Segmento de Infraestructura de PBB-TE.

En el modo de compartición de carga de la conmutación de segmento de ruta bidireccional de 1:1 de PBB-TE, las TESIs asignadas a un grupo de protección de TE pueden ser reutilizadas en otros grupos de protección de TE. Esto hace al campo del tráfico insuficiente para detectar defectos de desacuerdo, puesto que sólo puede indicar si existe tráfico en una TESI específica, y la presencia o no de tráfico en las TESIs que son compartidas entre un conjunto de grupos de protección de TE no está directamente asociada con la adecuada operación de los mecanismos de conmutación de protección. Lo mismo sigue siendo cierto en el modo de compartición de carga de la protección de Segmento de Infraestructura de PBB-TE puesto que el campo del tráfico sólo puede decir si hay tráfico en un Segmento específico pero falla en asociar este tráfico al IPG al cual pertenece el tráfico.

Por ejemplo, como en la Figura 1a, en operación normal, siempre existe tráfico que va hacia la primera TESI 7 y la segunda TESI 8, así que el campo del tráfico siempre será establecido por las MAs que monitorizan a esas TESIs. Por lo tanto, la situación de desacuerdo descrita e ilustrada anteriormente en la Fig. 1b no puede ser detectada por las MAs meramente mediante monitorización del campo del tráfico de los CCMs 11 en las TESIs 7 y 8, porque los campos del tráfico de los CCMs 11 en las dos direcciones están siempre definidos. Más específicamente en la Fig. 1b, el campo del tráfico de los CCMs en la primera TESI 7 está siempre definido porque la primera TESI 7 es todavía la TESI de trabajo del grupo de protección de TE B y el campo del tráfico de los CCMs de la segunda TESI 8 está siempre definido porque la segunda TESI 8 es todavía la TESI de trabajo del grupo de protección de TE C.

Las Figs. 4a y 4b ilustran un ejemplo del modo de compartición de carga de la protección de segmento de infraestructura de PBB-TE en operación normal y en una situación de desacuerdo respectivamente. En operación normal tal como se ilustra en la Fig. 4a un IPG D, que incluye las TESIs 24 y 25, atraviesa el segmento 26 que es el segmento de trabajo del IPG D. El IPG D está protegido por su segmento de protección que es el segmento 27. Un IPG E, que incluye las TESIs 41 y 42, atraviesa al segmento 27, que es el segmento de trabajo del IPG E. El IPG E está protegido por el segmento 26, que es el segmento de protección del IPG E. Así, en operación normal, dado que siempre existe tráfico que va a través del segmento 26 y el segmento 27, el campo del tráfico está siempre definido por los MEPs 43a, 43b, 43c y 43d que monitorizan los segmentos 26, 27.

Ahora, asúmase que existe una orden administrativa que dicta que todas las TESIs 24, 25 del IPG D en el segmento 26 deben ser conmutadas al segmento de protección, es decir, al segmento 27. Debido a un error de configuración, sólo la TESI 25 es conmutada al segmento de protección IPG D y la TESI 24 todavía permanece en el segmento de trabajo IPG D, tal como se ilustra en la Fig. 4b. de acuerdo con esto, existe un desacuerdo en este escenario, puesto que existirá tráfico asociado con el IPG D tanto en la TESI de trabajo como en la TESI de protección. No obstante, el campo del tráfico que se monitoriza en las MAs de monitorización de segmento no puede detectar el desacuerdo porque los campos del tráfico de los CCMs en ambas direcciones están siempre definidos.

En la Protección de infraestructura de M:1, ambos extremos tienen el mismo orden de prioridad para que segmentos de protección alternativos eviten posibles desacuerdos. Si hay un error de configuración del orden de prioridad, el error de configuración no puede ser detectado basándose en mecanismos de detección de desacuerdo conocidos previamente tales como el campo del tráfico. Por ejemplo, como en las Figs. 4a y 4b, debe asumirse que los segmentos de protección alternativos 28 y 29 están configurados para el IPG D. Debe asumirse también que el orden de prioridad está configurado como 0 para el segmento 28 y 1 para el segmento 29 en el SEB 22 en un extremo, y en el SEB 22 en el otro extremo, el orden de prioridad está configurado como 1 para el segmento 28 y 0 para el segmento 29. Si hay un fallo de conectividad en el segmento de protección (segmento 27) del IPG D, un extremo SEB 22 tomará el segmento 28 como segmento de protección y el otro extremo SEB 22 tomará el segmento 29 como segmento de protección. Este error de configuración no será detectado hasta que hay un fallo de conectividad en el segmento de trabajo (segmento 26). Cuando un SEB 22 de extremo conmuta las TESIs correspondientes al segmento 28 y el otro SEB 22 de extremo conmuta las TESIs correspondientes al segmento 29, habrá un error de desacuerdo. No obstante, como señalamos en los ejemplos previos, puede no ser posible detectar este desacuerdo si la Protección de Segmento de Infraestructura de PBB-TE está en modo de compartición de carga.

Como se ilustra mediante los ejemplos anteriores el campo del tráfico no es suficiente para la detección del desacuerdo en el modo de compartición de carga para la protección de ruta bidireccional de 1:1 de PBB-TE o la Protección de Segmento de Infraestructura de PBB-TE. Sería por lo tanto deseable tener otro mecanismo, preferiblemente basado en la arquitectura de puentes existente, para monitorizar las entidades de trabajo / protección que permita el reporte de desacuerdos a los operadores.

Las realizaciones que se describen con más detalle a continuación utilizan un bit en un CCM como un bit de indicación, que indica un elemento de información de desacuerdo en el CCM. El bit de indicación puede por ejemplo ser un bit en un campo de marcas del CCM y el elemento de información de desacuerdo puede por ejemplo ser un tipo – longitud – valor (TLV) de desacuerdo. El elemento de información de desacuerdo se define para especificar el estado del tráfico para diferentes grupos de protección de TE para una TESI específica o para diferentes grupos de protección de infraestructura para un segmento específico. Otros parámetros de configuración pueden opcionalmente también ser incluidos para coordinar ambos extremos.

De acuerdo con las realizaciones descritas en esta memoria el bit de indicación es ajustado en respuesta a la ocurrencia de un evento predeterminado y durante un periodo de tiempo configurable (denominado en esta memoria un primer periodo de tiempo) tras la ocurrencia del evento predeterminado. En algunas realizaciones de ejemplo el bit de indicación es establecido solamente cuando existe una nueva transición de estado en una máquina de estados de conmutación de protección y sólo durante un periodo de tiempo limitado (es decir, primer periodo de tiempo) tras la transición de estado para evitar ralentizar el procesamiento normal del CCM.

La Fig. 9a es un diagrama de bloques esquemático de un formato de cabecera de una unidad de datos de protocolo (PDU – Protocol Data Unit, en inglés) de CFM que comprende los campos de nivel de MD, versión, Código de Operación, marcas 91 y primer Desfase de TLV. La Fig. 9b es un diagrama de bloques esquemático del campo de marcas 91 de una PDU de CCM de acuerdo con una realización de ejemplo. En esta realización de ejemplo un bit del campo de marcas 91 se utiliza como el bit de indicación 92 para indicar si el elemento de información de desacuerdo está incluido en el CCM. De acuerdo con el estándar actual existe un número de bits reservados en el campo de marcas 91 y de acuerdo con esta realización de ejemplo uno de esos bits reservados se utiliza como el bit de indicación 92.

Como se ha mencionado anteriormente el elemento de información de desacuerdo debería ser definido para especificar el estado del tráfico para diferentes grupos de protección de TE (TEPGs – TE Protection Groups, en inglés) para un TE – SI específico o diferentes Grupos de Protección de Infraestructura (IPGs – Infrastructure Protection Groups, en inglés) para un Segmento específico. El elemento de información de desacuerdo debería, de acuerdo con ciertas realizaciones, ser añadido al CCM sólo cuando la máquina de estados se inicializa o se produce un evento que activa el cambio del tráfico de una ruta a otra, en otras palabras, en conexión con una transición de estado en la máquina de estados. El elemento de información de desacuerdo puede ser añadido a los CCMs que monitorizan la ruta de red correspondiente durante el periodo de tiempo limitado (es decir, el primer periodo de tiempo) para evitar la ralentización del procesamiento normal del CCM. Existe un conjunto de máquinas de estado de conmutación de protección por grupo de protección en cada puente que termina el grupo de protección. De manera correspondiente la máquina de estados está situada en los nodos / puentes 2, 3 y 22 de las Figs. 1 – 4 descritas anteriormente. En los estándares del IEEE, la máquina de estados normalmente incluye estados como de

Iniciación, de Trabajo, de Fallo de TESI / Segmento, de Protección de Fallo de TESI / Segmento, etc. De acuerdo con esto una transición de estado generalmente implica que algo sucede a la ruta de red o que el operador de la red desea conmutar la ruta del tráfico. Si no hay ningún fallo y ninguna reconfiguración mediante órdenes administrativas, no habrá ninguna transición de estado. Cuando la máquina de estados se inicializa o hay una nueva transición de estado en la máquina de estados, por ejemplo, EMPEZAR -> Trabajo o Trabajo -> Protección, el elemento de información de desacuerdo puede ser añadido a los CCMs y el correspondiente bit de indicación es definido. Las razones son que un error de desacuerdo normalmente tiene lugar cuando hay una transición de estado. Así, no hay generalmente necesidad de monitorizar desacuerdos por medio del elemento de información de desacuerdo todo el tiempo. Por el contrario, generalmente es suficiente comprobar si hay un desacuerdo incompleto de la conmutación de protección o un desacuerdo de configuración tan pronto como se produce una transición de estado. Tampoco necesitamos ejecutar CCMs con el elemento de información de desacuerdo todo el tiempo tras la transición de estado. Puede configurarse un periodo de tiempo limitado (denominado en esta memoria el primer periodo de tiempo), el cual se considera apropiado y suficiente para la detección de cualquier desacuerdo en conexión con la transición de estado. Este primer periodo de tiempo puede, por ejemplo, ser 50 ms o más y puede ser monitorizado mediante un temporizador de información de desacuerdo.

Un formato de una realización de ejemplo de un elemento de información de desacuerdo 93 se ilustra en la Fig. 9c. El elemento de información de desacuerdo 93 de la Fig. 9c es un TLV de desacuerdo definido sobre la base de la estructura de datos en el estándar IEEE Std 802.1 Qay – 2009 ó en el documento de estándar IEEE P802.1Qbf/D0.0 para facilitar la modificación de esos estándares para que cumplan con las realizaciones descritas en esta memoria.

De acuerdo con una versión modificada del estándar IEEE 802.1Qay el TLV del desacuerdo 93 contiene una lista de grupos de protección de ingeniería del tráfico (TEPGs – Traffic Engineering Protection Groups, en inglés) a los cuales se asigna la TESI monitorizada por el CCM. Cada entrada de la lista contiene los siguientes elementos asociados con el TEPG:

- la identidad del TEPG

- el estado del tráfico para la TESI de trabajo del TEPG, en otras palabras, si esta TESI de trabajo está activa con tráfico desde este TEPG. Si está activa, estado del tráfico = 1, si no está activa, estado del tráfico = 0.

- el estado del tráfico para la TESI de protección en el TEPG, en otras palabras, si esta TESI de protección está activa con tráfico desde este TEPG.

Si está activa, estado del tráfico = 1, si no está activa, estado del tráfico = 0.

La identidad de los TEPGs debe ser única dentro de los grupos de protección compartidos y los dos puntos de extremo de la TESI deben compartir la misma comprensión de la identidad de los grupos de protección compartidos. Una posible idea es utilizar la combinación del TE-SID de trabajo y del TE-SID de protección para identificar de manera única un TEPG, pero cualquier otro identificador que satisfaga la condición anterior resulta apropiado.

En la Fig. 1a los elementos de información de desacuerdo 13a, 13b, 13c y 13d se muestran para ilustrar esquemáticamente el contenido de los elementos de información de desacuerdo que serían transmitidos en los CCMs para los respectivos MEPs 9a – d en operación normal de la configuración de ejemplo ilustrada en la Fig. 1a. Por razones de sencillez, las identidades de los TEPGs se representan aquí mediante letras.

De acuerdo con una versión modificada del estándar IEEE 802.1Qbf el TLV del desacuerdo 93 contiene una lista de IPGs a los cuales se asigna el segmento monitorizado por el CCM. Cada entrada de la lista contiene los siguientes elementos asociados con el IPG:

- la identidad del IPG

- el estado del tráfico para el segmento de trabajo en el IPG, en otras palabras, si este segmento de trabajo está activo con tráfico desde este IPG. Si está activo, estado del tráfico = 1, si no está activo = 0.

- el estado del tráfico para el segmento de protección en el IPG, en otras palabras, si este segmento de protección está activo con tráfico desde este IPG.

Si está activo, estado del tráfico = 1, si no está activo, estado del tráfico = 0.

La identidad de los IPGs debe ser única dentro de los grupos de protección compartidos y los dos SEBs deben compartir la misma comprensión acerca de la identidad de los grupos de protección compartidos. Una posible idea es utilizar la combinación de MAID del Segmento de Trabajo y el MAID del Segmento de Protección para identificar de manera única un IPG pero cualquier otro identificador que satisfaga la condición anterior resulta apropiado.

En la Fig. 4a los elementos de información de desacuerdo 44a, 44b, 44c y 44d se muestran para ilustrar esquemáticamente el contenido de los elementos de información de desacuerdo que serían transmitidos en CCMs

desde los respectivos MEPs 43a – d en operación normal de la configuración de ejemplo ilustrada en la Fig. 4a. Por razones de sencillez, las identidades de los IPGs se representan en esta memoria mediante letras.

De acuerdo con ciertas realizaciones de ejemplo, siempre que los MEPs envían CCMs, pueden realizarse las siguientes operaciones:

- El MEP comprueba si hay una transición de la máquina de estados o si un temporizador de TLV de desacuerdo ha expirado para todos los TEPGs compartidos o IPGs compartidos asociados con el MEP. Si hay una transición de estado o el temporizador de TLV de desacuerdo está aún corriendo para alguno de esos TEPGs o IPGs asociados con el MEP, el MEP lleva a cabo lo siguiente:

    a. Ajustar la versión de protocolo en el CMM a la versión 2. (En la versión 1, los bits reservados en el campo de marcas 91 son ignorados.)

    b. Ajustar el “Campo de Indicación” 92 en el CCM a “verdadero”.

    c. Añadir el TLV de desacuerdo con el valor apropiado al CCM.

- El TLV de “Desacuerdo” se construye basándose en información configurada por los operadores. Un desacuerdo se detecta si

- Los dos campos de Estado del Tráfico para Trabajo y Estado del Tráfico para Protección son iguales para un TEPG o IPG específico.

Siempre que los MEPs reciben CCMs, el MEP respectivo puede llevar a cabo la siguiente operación:

- Comparar cualquier TLV de desacuerdo recibido con el propio TLV de desacuerdo actual de los MEPs. Si es diferente durante un periodo de tiempo (denominado en esta memoria un segundo periodo de tiempo, por ejemplo 50 ms, se declara un defecto de desacuerdo.

Por ejemplo, la situación de desacuerdo ilustrada y descrita en conexión con la Fig. 1b puede ser detectada por medio de los elementos de información de desacuerdo 13a – d, que en la Fig. 1b se ilustran con contenidos correspondientes a la situación de desacuerdo. En este caso, el desacuerdo será detectado cuando un MEP reciba elementos de información de desacuerdo y encuentre que los elementos de información de desacuerdo recibidos son diferentes de los propios elementos de información de desacuerdo del MEP transmitidos durante el segundo periodo de tiempo. El MEP 9a puede, por ejemplo, detectar el desacuerdo comparando el elemento de información de desacuerdo 13c recibido en un CCM desde el MEP 9c con el elemento de información de desacuerdo 13a que el MEP 9c transmite en la TESI 7. La comparación muestra estados del tráfico que difieren para los TE-SIs de trabajo y de protección del TEPG A, lo que indica el desacuerdo. El desacuerdo puede también ser detectado mediante comparaciones correspondientes en los MEPs 9b, 9c y 9d.

La situación de desacuerdo de ejemplo ilustrada y descrita en conexión con la Fig. 4b puede ser detectada por medio de los elementos de información de desacuerdo 44a – d, los cuales en la Fig. 4b se ilustran con contenidos correspondientes a la situación de desacuerdo. En este caso, el desacuerdo será detectado en los MEPs 43a – d puesto que para el IPG D, tanto el segmento de trabajo como el segmento de protección están activos con tráfico tal como se indica mediante el estado del tráfico para el IPG D en los elementos de información de desacuerdo 44a – d. Así, esta clase de desacuerdo de configuración puede ser detectada.

Si hay un error de configuración del orden de prioridad para segmentos de protección alternativos en la Protección de Infraestructura de M:1, este desacuerdo puede ser detectado cuando existe un fallo de conexión en el segmento de protección original. Si la identidad del IPG incluye el MAID del segmento de protección, esta identidad de IPG específica será diferente entre el elemento de información de desacuerdo de los dos extremos.

El bit de indicación propuesto puede ser utilizado siempre que el CCM necesite ser comprobado más profundamente. Además de indicar que existe un elemento de información de desacuerdo incluido en el CCM, el bit de indicación puede ser extendido para indicar que existe un elemento de información especial (por ejemplo TLV) unido al CCM para una futura extensión del CCM.

La Fig. 5 es un diagrama de flujo que ilustra una realización de ejemplo de un método para la gestión de instancias de servicios en un nodo de red tal como uno de los puentes / nodos 2, 3 ó 22. El método comprende monitorizar una pluralidad de rutas de red bidireccionales y distintas que contienen un número de instancias de servicios del nodo de red a otro nodo de red. Las rutas de red pueden, por ejemplo ser TESIs que contienen un número de instancias de servicios de red troncal o segmentos de infraestructura que contienen un número de TESIs. Las rutas de red forman uno o varios grupos de protección asociados con una instancia de servicio o grupo de instancias de servicios respectivo o respectivos. La monitorización de las rutas de red incluye la transmisión periódica de CCMs en una ruta de red monitorizada. Más específicamente y como se ilustra en la Fig. 5 se determina en una etapa 51, si es hora de enviar un CCM. Cuando es hora de enviar un CCM se investiga si ha ocurrido un evento predeterminado y si el tiempo desde que tal evento predeterminado ocurrió hace menos de un tiempo predeterminado t ms, etapa 52. El

evento predeterminado puede, por ejemplo ser una transición de estado en la máquina de estados de conmutación de protección y el tiempo t (referido al primer periodo de tiempo anterior) puede por ejemplo ser 50 ms, como se explicó anteriormente. Si la determinación en una etapa 52 es afirmativa el bit de indicación y el elemento de información de desacuerdo debe ser incluido en el CCM, etapa 53, o si no, el CCM debe ser enviado sin el bit de indicación y el elemento de información de desacuerdo en una etapa 56. Como se ha explicado anteriormente el elemento de información de desacuerdo incluye información que especifica, para cada grupo de protección, que la ruta de red monitorizada es un miembro de, estado del tráfico de una ruta de red de trabajo y de una ruta de red de protección. En una etapa 54 opcional el elemento de información de desacuerdo del CCM para ser enviado puede ser examinado para determinar si existe algún estado del tráfico en conflicto de la ruta de trabajo y de la ruta de protección de cualquier grupo de protección incluido en el elemento de información de desacuerdo. Si tal estado del tráfico en conflicto es detectado un operador o NMS es notificado acerca de que un desacuerdo ha sido detectado en una etapa 55. El CCM es enviado en una etapa 56. La etapa 56 puede ser también llevada a cabo antes de las etapas opcionales 54 y 55.

Una realización de ejemplo de un método para la gestión de instancias de servicios en un nodo de red puede, además de la transmisión de CCMs tal como se ilustra en la Fig. 5, incluir también la monitorización de los CCMs recibidos tal como se ilustra en la Fig. 6. En una etapa 61 un CCM es recibido en una ruta de red monitorizada. En una etapa 62 se examina si el CCM recibido incluye un bit de indicación que indica la presencia de un elemento de información de desacuerdo en el CCM. Si el CCM recibido incluye el elemento de información de desacuerdo, el elemento de información de desacuerdo es leído y comparado con el elemento de información de desacuerdo de un CCM correspondiente enviado en la misma ruta de red. El CCM correspondiente enviado puede por ejemplo ser el CCM que fue enviado más recientemente antes de la recepción del CCM recibido o el primer CCM que es enviado tras la recepción del CCM recibido. En una etapa 64 se determina si los elementos de información de desacuerdo comparados difieren, por ejemplo, con respecto al estado del tráfico de cualquier ruta de red de trabajo o de protección o con respecto a una identidad de un grupo de protección (de acuerdo con la explicación anterior relativa a un modo de detección de desacuerdo en una prioridad configurada para alternar segmentos de protección). Si los elementos de información de desacuerdo comparados difieren se notifica a un operador o NMS un desacuerdo detectado en una etapa 65.

La Fig. 7 es un diagrama de bloques esquemático de una realización de ejemplo de un nodo de red 70 en el cual el método ilustrado en la Fig. 5 y 6 puede ser llevado a cabo. El nodo de red 70 comprende circuitos de procesamiento 71 y un número de puertos de red 72 para recibir y transmitir mensajes en un número de rutas de red. Los circuitos de procesamiento 71 incluyen un número de entidades de Operación, Administración y Gestión (OAM – Operation, Administration and Management, en inglés) 73. Los MEPs 9a – d y 43a – d mencionados anteriormente están configurados para llevar a cabo las etapas 51 – 56 de la Fig. 5 y las etapas 61 – 65 de la Fig. 6. Con este propósito las entidades de OAM 73 pueden incluir un submódulo de control de CCM 74 para controlar la generación, transmisión y recepción de CCMs, y un submódulo de comprobación de desacuerdo 75 configurado para detección de desacuerdos mediante un examen de los elementos de información de desacuerdo de los CCMs enviados y/o recibidos.

La Fig. 8 es un diagrama de bloques esquemático de otra realización de ejemplo 80 de un nodo de red en la cual el método ilustrado en la Fig. 5 y 6 puede ser llevado a cabo. La Fig. 8 puede ser una descripción alternativa de la realización de ejemplo mostrada en la Fig. 7. El nodo de red 80 comprende los puertos de red 72 para recibir y transmitir mensajes en un número de rutas de red. El nodo de red 80 también comprende una unidad de entrada 81 que está adaptada para recibir mensajes desde las rutas de red y una unidad de salida para la salida de mensajes en las rutas de red. La unidad de entrada 81 y la unidad de salida 82 pueden estar integradas en el hardware del nodo de red 80. El nodo de red 80 está además provisto de una CPU 83, que puede ser una sola unidad o estar compuesta de varias unidades que están configuradas para llevar a cabo las etapas de los procedimientos descritos en esta memoria. Al menos un producto de programa de ordenador 84 está incluido en el UE 22. El producto de programa de ordenador 84 puede ser realizado en forma de memoria volátil o una memoria no volátil, por ejemplo, una EEPROM, una memoria rápida o una unidad de disco. El producto de programa de ordenador 84 comprende submódulos de programa de ordenador. La Fig. 8 muestra un submódulo de transmisión de CCM 85 para controlar la generación y transmisión de CCMs en rutas de red monitorizadas, un submódulo de elemento de información de desacuerdo 86 para la generación de elementos de información de desacuerdo para la inclusión de elemento de información de desacuerdo en CCMs, un módulo de comprobación de desacuerdo 87 para la detección de desacuerdos mediante la detección de estados de tráfico en conflicto en los elementos de información de desacuerdo de CCMs enviados, y un módulo de comprobación de desacuerdo 88 para la detección de desacuerdos mediante comparaciones de elementos de información de desacuerdo de CCMs recibidos y transmitidos. Los submódulos 85 – 88 esencialmente llevan a cabo las etapas 51 – 56 del diagrama de flujo de la Fig. 5 y las etapas 61 – 65 del diagrama de flujo de la Fig. 6. En otras palabras, cuando los diferentes submódulos 85 – 88 son ejecutados en la CPU 83, el nodo de red lleva a cabo las etapas 51 – 56 de la Fig. 5 y las etapas 61 – 65 de la Fig. 6. Los submódulos 85 – 88 serían generalmente implementados en software, aunque también son factibles implementaciones completa o parcialmente en firmware, hardware o combinaciones de los mismos.

En los dibujos y especificación, se han explicado realizaciones preferidas típicas de la invención y, aunque se emplean términos específicos, son utilizados sólo en un sentido genérico y descriptivo y no con propósitos de limitación, siendo el alcance de la invención establecido en las reivindicaciones siguientes.

REIVINDICACIONES

1. Un método para la gestión de instancias de servicios en un primer nodo de red (2, 3, 22, 70, 80) de una red de comunicación (1), comprendiendo el método

monitorizar una pluralidad de rutas de red (7, 8, 26, 27, 28) bidireccionales y distintas para transportar un número de instancias de servicios (10a, 10b, 10c, 24, 25, 41, 42) desde el primer nodo de red a un segundo nodo de red (2, 3, 22, 70, 80), donde un número de las citadas rutas de red forman un grupo de protección asociado con una respectiva instancia de servicio o grupo de instancias de servicios, incluyendo la citada monitorización:

enviar (56) continua y periódicamente Mensajes de Comprobación de Continuidad, CCMs (Continuity Check Messages, en inglés) (11), en una ruta de red (7, 8, 26, 27, 28) monitorizada hacia el segundo nodo de red (2, 3, 22, 70, 80);

en respuesta a la ocurrencia de un evento predeterminado, incluir (53) un bit de indicación en los CCMs (11), que son enviados en la citada ruta de red monitorizada durante un periodo de tiempo predeterminado tras la ocurrencia del citado evento predeterminado, donde el bit de indicación indica la presencia de un elemento de información de desacuerdo (13a - d, 44a – d) en el CCM que incluye el bit de indicación, donde el elemento de instancia de desacuerdo incluye información que especifica, para cada grupo de protección que la citada ruta de red monitorizada es un miembro de, estado del tráfico de una ruta de red de trabajo y de una ruta de red de protección del grupo de protección.

2. El método de acuerdo con la reivindicación 1, en el que el citado número de instancias de servicios son servicios de red troncal (10a, 10b, 10c) y la citada pluralidad de rutas de red son Instancias de Servicios de Ingeniería del Tráfico, TESIs (Traffic Engineering Service Instances, en inglés) (7, 8).

3. El método de acuerdo con la reivindicación 1, en el que el citado número de instancias de servicios son las TESIs (24, 25, 41, 42) y la citada pluralidad de rutas de red son los Segmentos de Infraestructura (26, 27, 28, 29).

4. El método de acuerdo con cualquiera de las reivindicaciones 1 – 3, en el que el citado evento predeterminado es una transición de estado en una máquina de estados para controlar el estado del tráfico de la citada pluralidad de rutas de red.

5. El método de acuerdo con cualquiera de las reivindicaciones 1 – 4, en el que cada elemento de información de desacuerdo (13a – d, 44a – d) es un elemento de tipo – longitud - valor, TLV, que comprende, para cada grupo de protección el que la citada ruta de red monitorizada es un miembro de, una identidad del grupo de protección, un bit que indica el estado del tráfico para la citada ruta de red de trabajo del grupo de protección y un bit que indica el estado del tráfico para la citada ruta de red del citado grupo de protección.

6. El método de acuerdo con cualquiera de las reivindicaciones 1 – 5, en el que el citado primer nodo es un puente o una central de conmutación de una red de Ethernet.

7. El método de acuerdo con cualquiera de las reivindicaciones 1 – 6, que comprende también

detectar (54) un desacuerdo si al menos uno de los citados elementos de información de desacuerdo (13a – d, 44a – d), que están incluidos en un CCM enviado, especifica estados del tráfico en conflicto de la ruta de red de trabajo y de la ruta de red de protección de al menos un grupo de protección;

y

notificar (55) a un Sistema de Gestión de Red, NMS (Network Management System, en inglés) (12), o un operador del desacuerdo detectado.

8. El método de acuerdo con cualquiera de las reivindicaciones 1 – 7, que comprende también

recibir (61) un número de CCMs (11) desde el segundo nodo de red;

para cada CCM (11) recibido: leer (63) un elemento de información de desacuerdo desde el CCM recibido, si el CCM recibido incluye un bit de indicación que indica la presencia del elemento de información de desacuerdo en el CCM recibido y comparar (63) el elemento de información de desacuerdo del CCM recibido con el elemento de información de desacuerdo incluido en un CCM enviado;

detectar (64) un desacuerdo si los elementos de información de desacuerdo comparados difieren durante un segundo periodo de tiempo predeterminado, y

notificarlo (65) a un Sistema de Gestión de Red, NMS (Network Management System, en inglés) (12), o a un operador el desacuerdo detectado.

9. Un nodo de red (2, 3, 22, 70, 80) para su uso en una red de comunicación (1), comprendiendo el nodo de red un número de entidades de Operación, Administración y Gestión, OAM (Operation, Administración and Management, en inglés) (9a – d, 43a – d, 73) configuradas para monitorizar una pluralidad de rutas de red (7, 8, 26, 28) bidireccionales y distintas para transportar un número de instancias de servicios (10a, 10b, 10c, 24, 25, 41, 42) desde el nodo de red a otro nodo de red, donde un número de las citadas rutas forma un grupo de protección asociado con una respectiva instancia de servicio o grupo de instancias de servicios, donde el citado número de entidades de OAM están también configuradas para continua y periódicamente enviar Mensajes de Comprobación de Continuidad, CCMs (Continuity Check Messages, en inglés) (11), en una ruta de red monitorizada al otro nodo de red;

en respuesta a la ocurrencia de un evento predeterminado, incluir un bit de indicación en los CCMs (11), que son enviados en la citada ruta de red monitorizada durante un primer periodo de tiempo predeterminado tras la ocurrencia del citado evento predeterminado, donde el bit de indicación indica la presencia de un elemento de información de desacuerdo (13a – d, 44a – d) en el CCM que incluye el bit de indicación, donde el elemento de información de desacuerdo incluye información que especifica, para cada grupo de protección que la citada ruta de red monitorizada es un miembro de, estado del tráfico de una ruta de red de trabajo y de una ruta de red de protección del grupo de protección.

10. El nodo de red (2, 3, 70, 80) de acuerdo con la reivindicación 9, donde el citado número de instancias de servicios (10a, 10b, 10c) son servicios de red troncal y la citada pluralidad de rutas de red son Instancias de Servicios de Ingeniería del Tráfico, TESIs (Traffic Engineering Service Instances, en inglés) (7, 8).

11. El nodo de red (22, 70, 80) de acuerdo con la reivindicación 9, en donde el citado número de instancias de servicios son TESIs (24, 25, 41, 42) y la citada pluralidad de rutas de red son Segmentos de Infraestructura (26, 27, 28, 29).

12. El nodo de red de acuerdo con cualquiera de las reivindicaciones 9 – 11, donde el citado evento predeterminado es una transición de estado en una máquina de estados para controlar el estado del tráfico de la citada pluralidad de rutas de red.

13. El nodo de red (2, 3, 22, 70, 80) de acuerdo con cualquiera de las reivindicaciones 9 – 12, donde el citado elemento de información de desacuerdo (13a – d, 44a – d) es un elemento tipo-longitud-valor, TLV, que comprende, para cada grupo de protección del cual es un miembro la citada ruta de red monitorizada, una identidad del grupo de protección, indicando un bit el estado del tráfico para la citada ruta de red de trabajo del grupo de protección y un bit indicando el estado del tráfico para la citada ruta de red de protección del grupo de protección.

14. El nodo de red (2, 3, 22, 70, 80) de acuerdo con cualquiera de las reivindicaciones 9 – 13, en el que el citado nodo de red es un puente o una central de conmutación de una red de Ethernet.

15. El nodo de red (2, 3, 22, 70, 80) de acuerdo con cualquiera de las reivindicaciones 9 – 14, donde el citado número de entidades de OAM están también configuradas para

detectar un desacuerdo si al menos uno de los citados elementos de información de desacuerdo (13a – d, 44a – d), que está incluido en un CCM enviado, especifica un estado del tráfico de la ruta de red de trabajo y de la ruta de red de protección de al menos un grupo de protección en conflicto; y notificarlo a un Sistema de Gestión de Red, NMS (Network Management System, en inglés) (12), o a un operador del desacuerdo detectado.

16. El nodo de red (2, 3, 22, 70, 80) de acuerdo con cualquiera de las reivindicaciones 9 – 15, donde el citado número de entidades de OAM (9a – d, 43a – d, 73) están también configuradas para

recibir un número de CCMs (11) del otro nodo de red;

para cada CCM recibido: leer un elemento de información de desacuerdo (13a – d, 11a – d) del CCM recibido, si el CCM recibido incluye un bit de indicación que indica la presencia del elemento de información de desacuerdo en el CCM recibido y comparar el elemento de información de desacuerdo del CCM recibido con el elemento de información de desacuerdo incluido en un CCM enviado;

detectar un desacuerdo si los elementos de información de desacuerdo comparados difieren durante un segundo periodo de tiempo predeterminado, y

notificar a un Sistema de Gestión de Red, NMS (Network Management System, en inglés) (12), o a un operador el desacuerdo detectado.

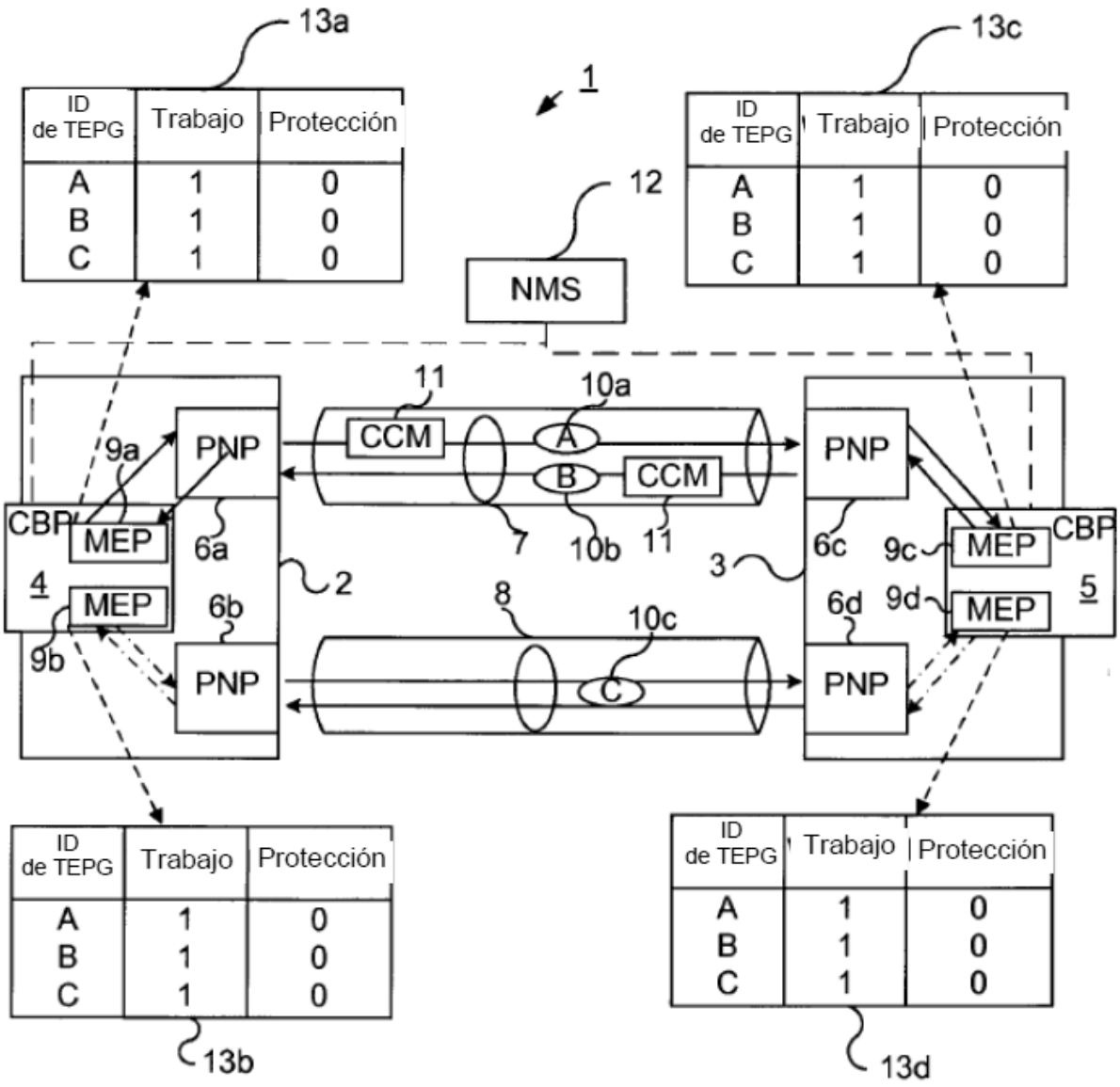
13a
ID de TEPG
Trabajo
Protección
A 1 0
B 1 0
C 1 0
1
13c
ID de TEPG
Trabajo
Protección
A 1 0
B 1 0
C 1 0
12
NMS
11
10a
CCM
A
B
CCM
PNP
9a
CBP
MEP
6a
4
MEP
6b
9b
PNP
7
10b
11
2
8
10c
C
3
6c
9c
MEP
CBP
6d
9d
MEP
5
PNP
ID de TEPG
Trabajo
Protección
A 1 0
B 1 0
C 1 0
13b
ID de TEPG
Trabajo
Protección
A 1 0
B 1 0
C 1 0
13d

Fig. 1a

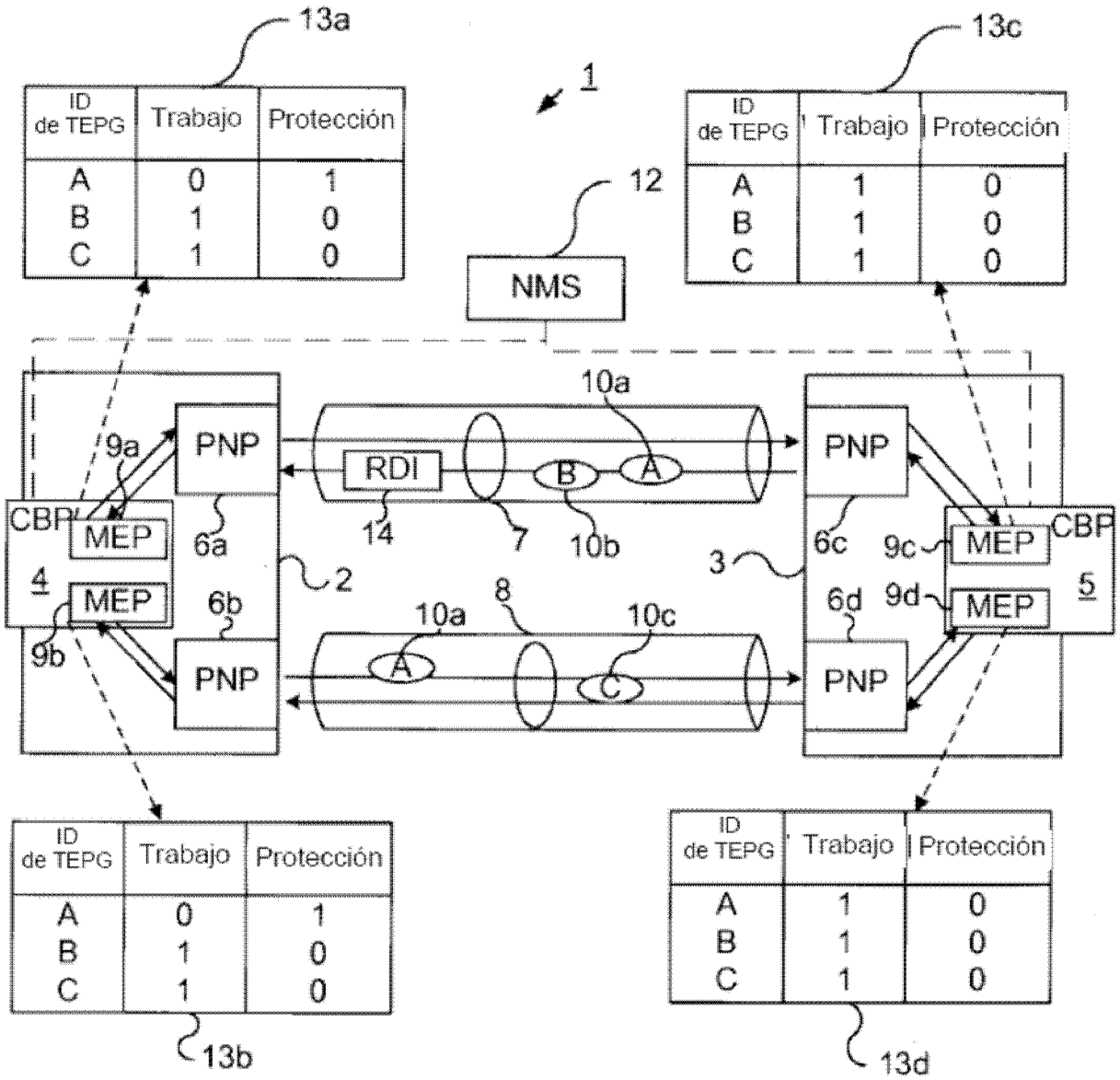
13a
ID de TEPG
Trabajo
Protección
A 0 1
B 1 0
C 1 0
1
12
NMS
13c
ID de TEPG
Trabajo
Protección
A 1 0
B 1 0
C 1 0
10a
9a
PNP
RDI
B
A
PNP
CBP
MEP
6a
14
7
10b
6c
9c
MEP
CBP
4
MEP
2
3
6d
9d
MEP
5
6b
8
10a
10c
9b
PNP
A
C
PNP
ID de TEPG
Trabajo
Protección
A 0 1
B 1 0
C 1 0
13b
ID de TEPG
Trabajo
Protección
A 1 0
B 1 0
C 1 0
13d

Fig. 1b

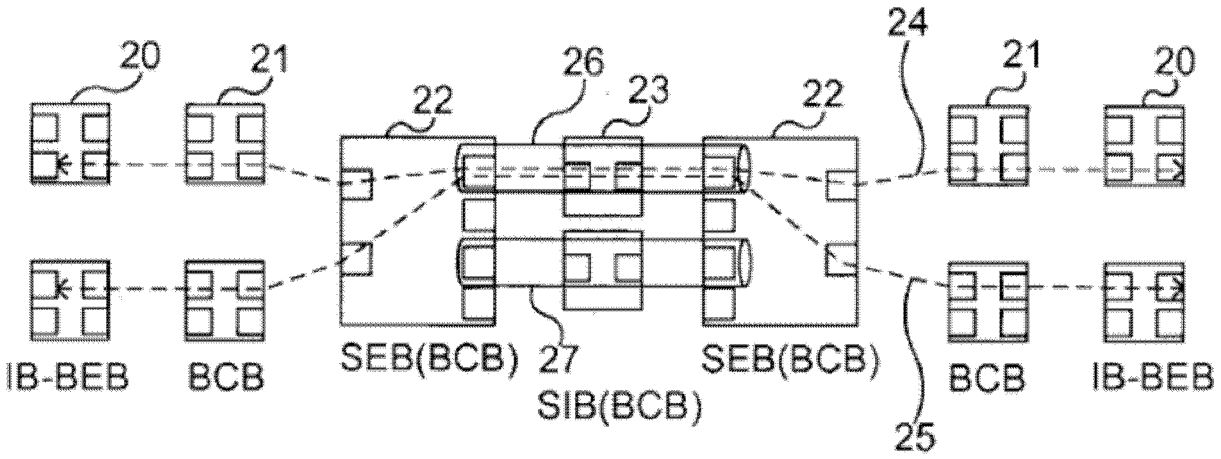

Fig. 2a

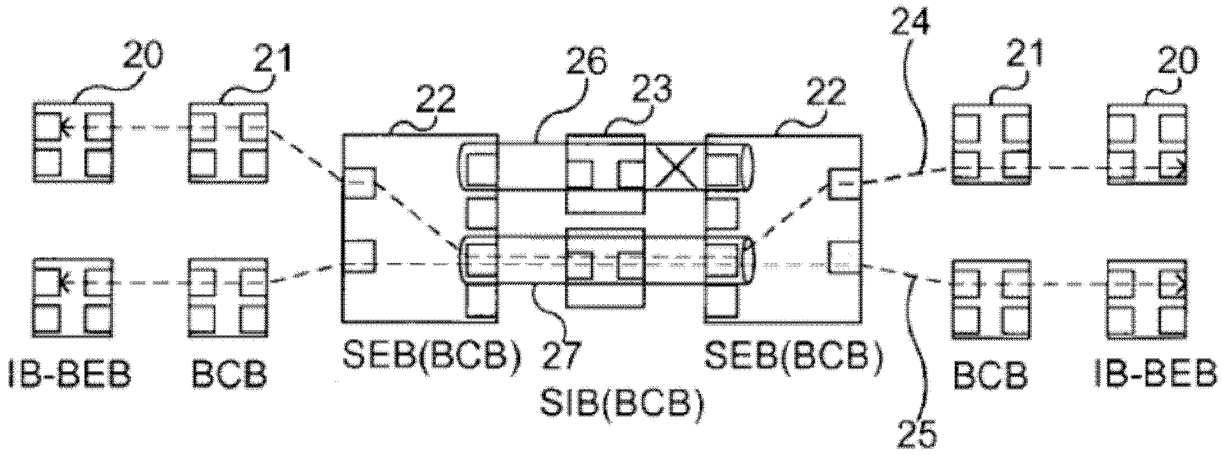

Fig. 2b

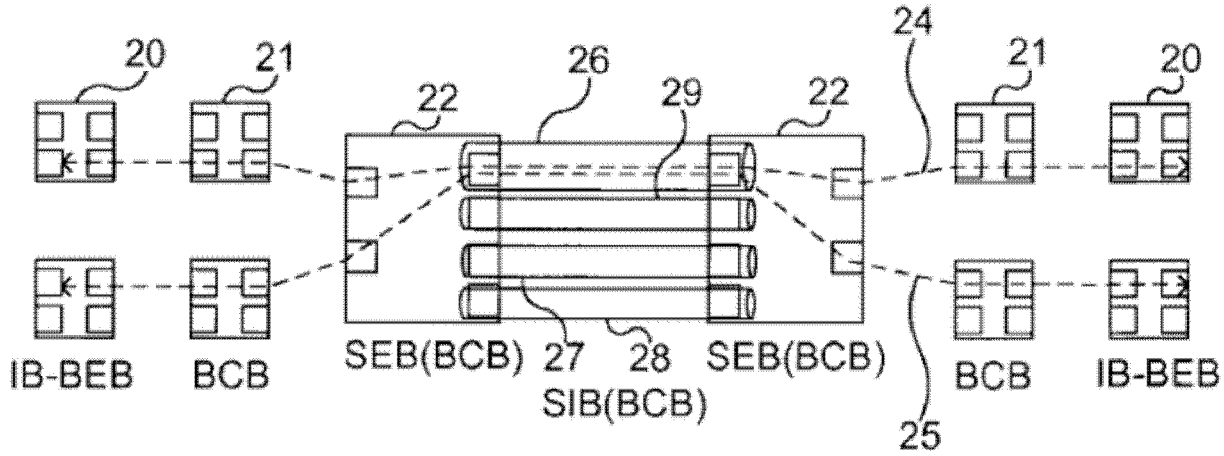

Fig. 3

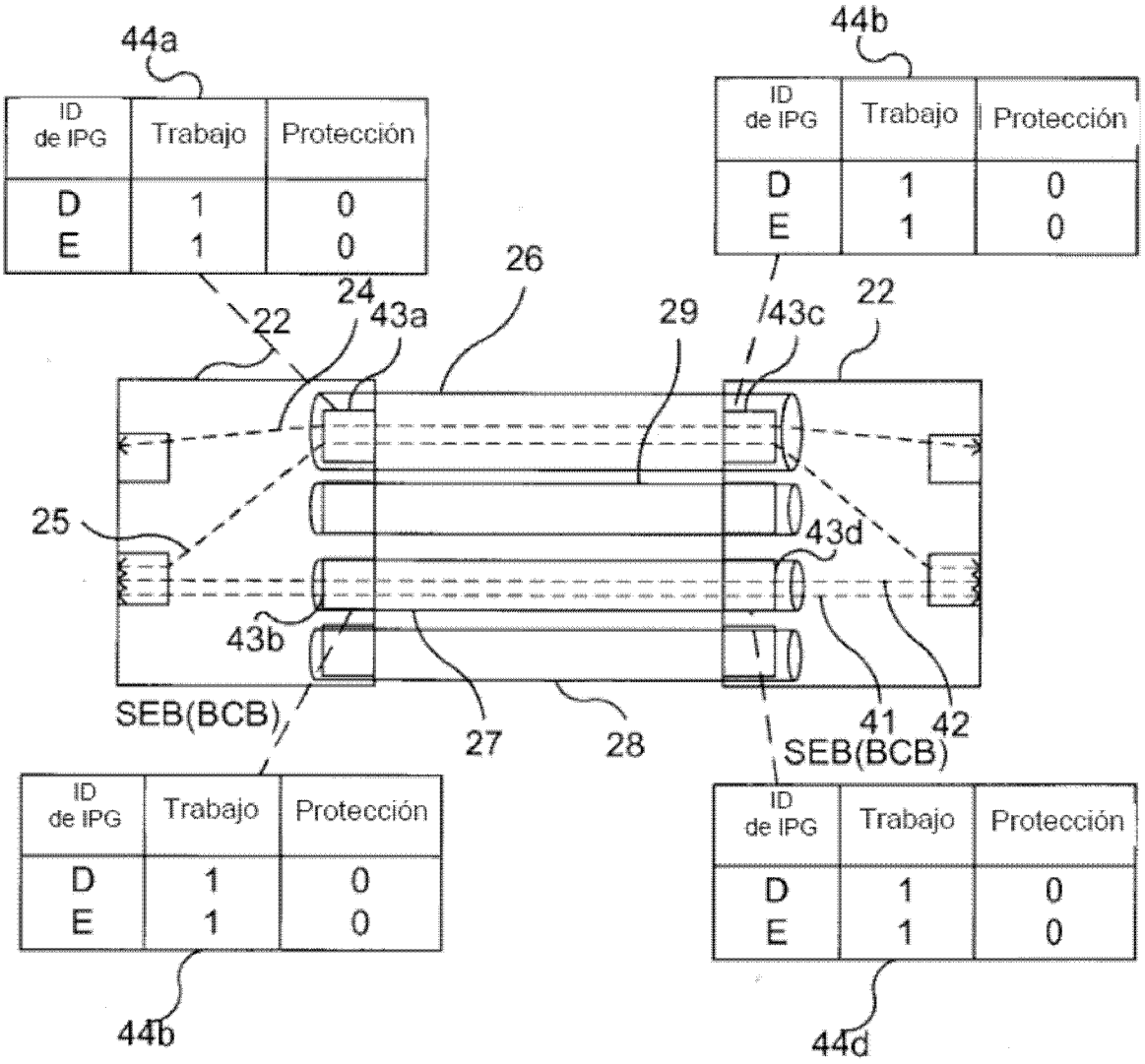
44a
ID de IPG
Trabajo
Protección
D 1 0
E 1 0
44b
ID de IPG
Trabajo
Protección
D 1 0
E 1 0
22
24
43a
26
29
43c
22
25
43d
43b
SEB(BCB)
27
28
41
42
SEB(BCB)
ID de IPG
Trabajo
Protección
D 1 0
E 1 0
44b
ID de IPG
Trabajo
Protección
D 1 0
E 1 0
44d

Fig. 4a

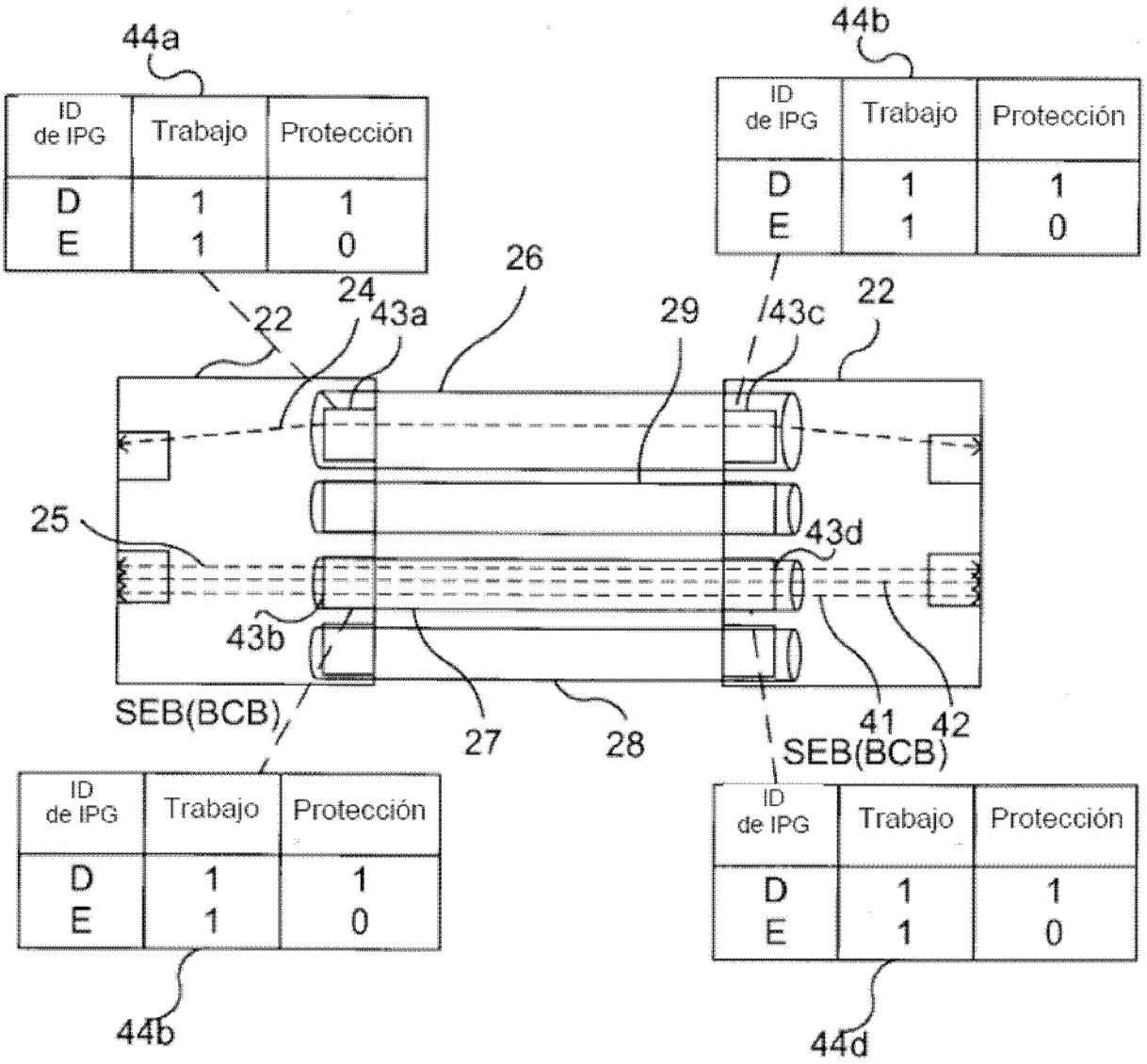
44a
ID de IPG
Trabajo
Protección
D
E
1
1
1
0
44b
ID de IPG
Trabajo
Protección
D
E
1
1
1
0
22
24
43a
26
29
43c
22
25
43d
43b
SEB(BCB)
27
28
41
42
SEB(BCB)
ID de IPG
Trabajo
Protección
D
E
1
1
1
0
44b
ID de IPG
Trabajo
Protección
D
E
1
1
1
0
44d

Fig. 4b

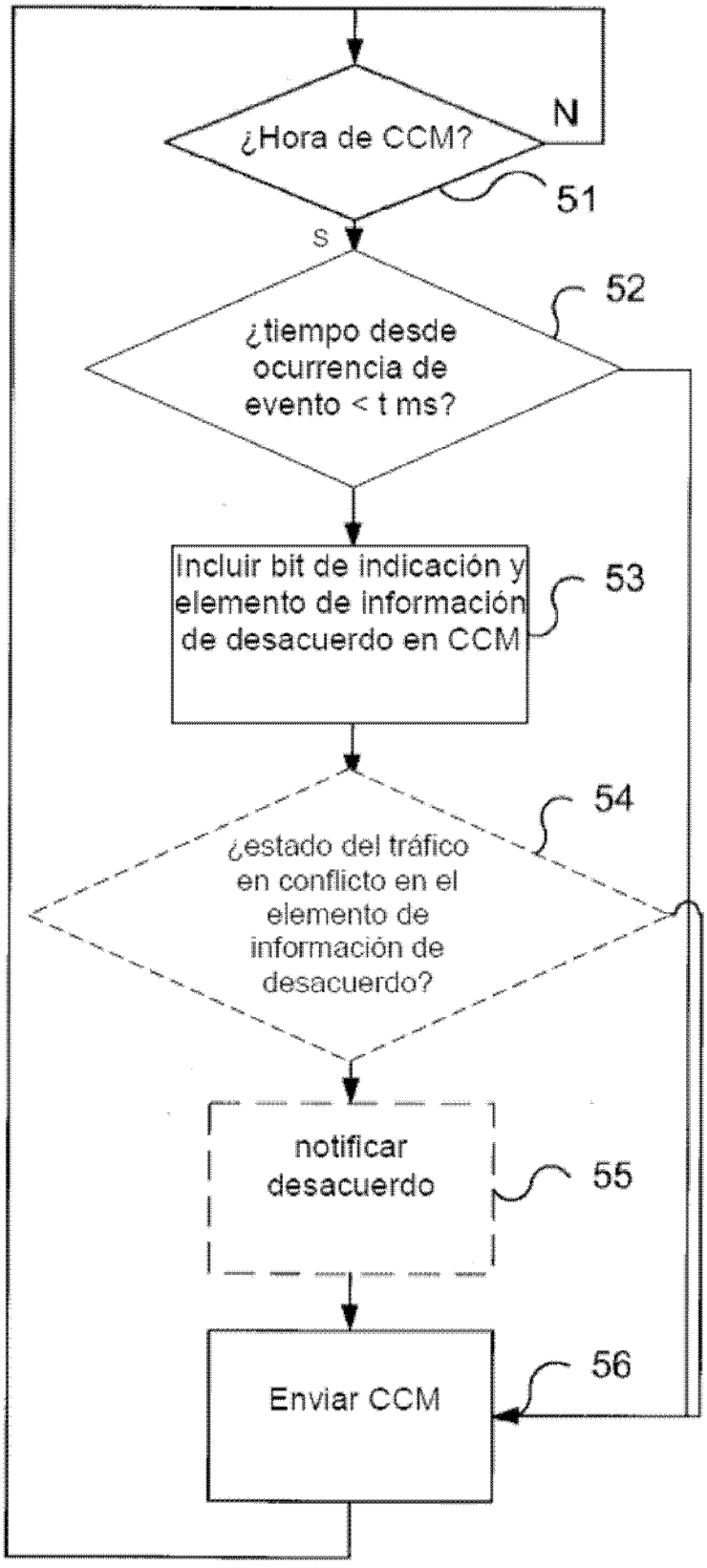
¿Hora de CCM?
N
51
S
¿tiempo desde ocurrencia de evento < t ms?
52
Incluir bit de indicación y elemento de información de desacuerdo en CCM
53
¿estado del tráfico en conflicto en el elemento de información de desacuerdo?
54
notificar desacuerdo
55
Enviar CCM
56

Fig. 5

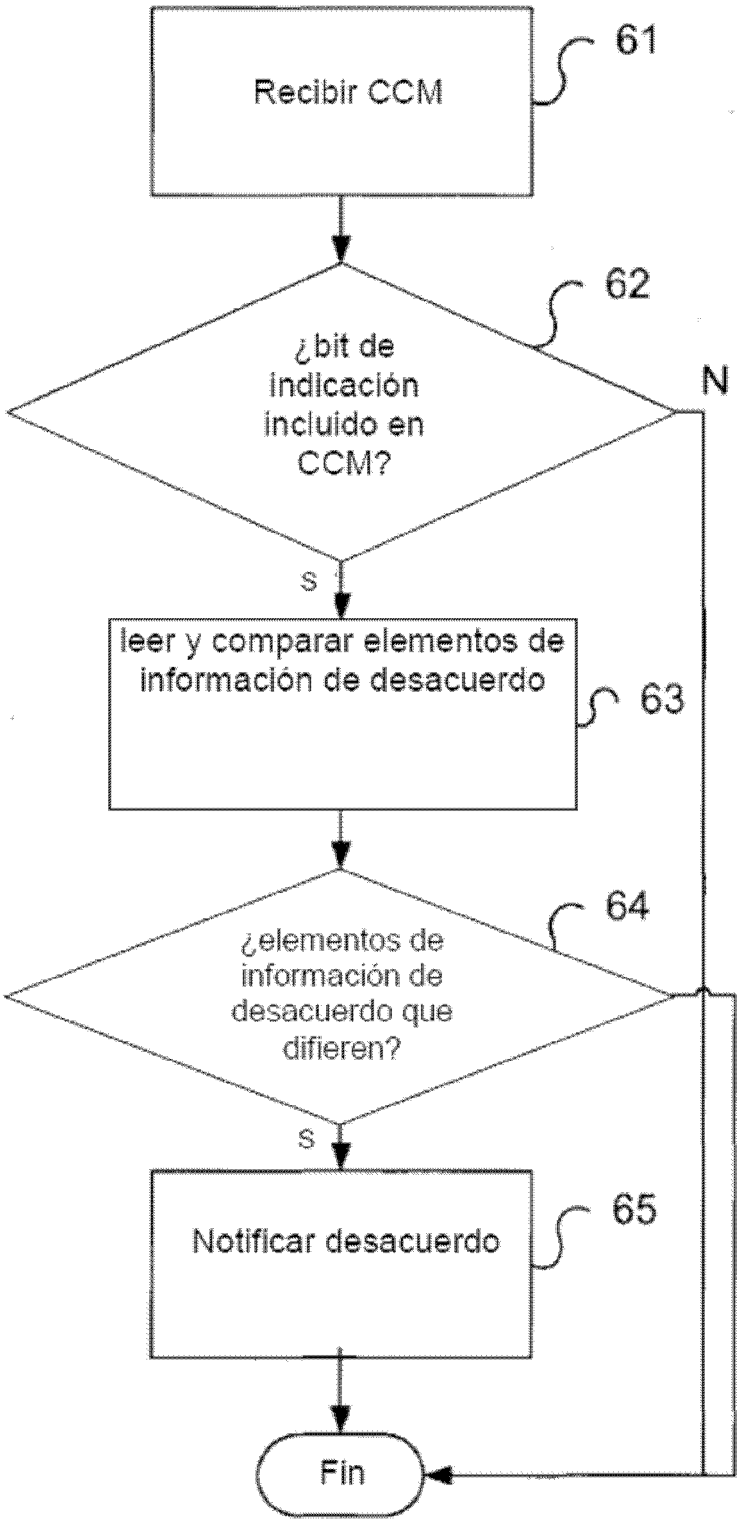
Recibir CCM
61
¿bit de indicación incluido en CCM?
62
N
S
leer y comparar elementos de información de desacuerdo
63
¿elementos de información de desacuerdo que difieren?
64
S
Notificar desacuerdo
65
Fin

Fig. 6

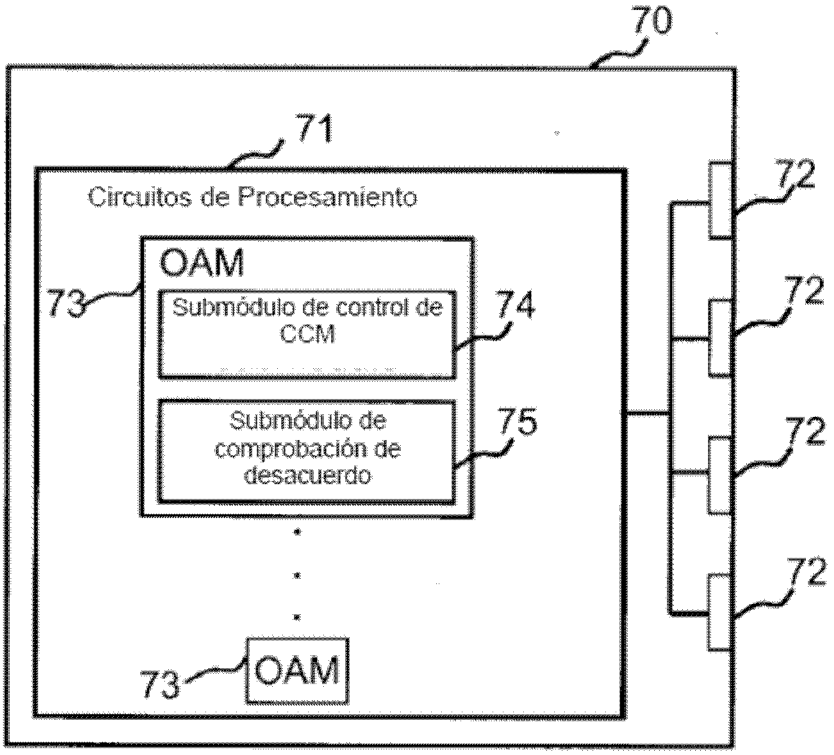
70
71
Circuitos de Procesamiento
OAM
73
Submódulo de control de CCM
74
Submódulo de comprobación de desacuerdo
75
73
OAM
72
72
72
72

Fig. 7

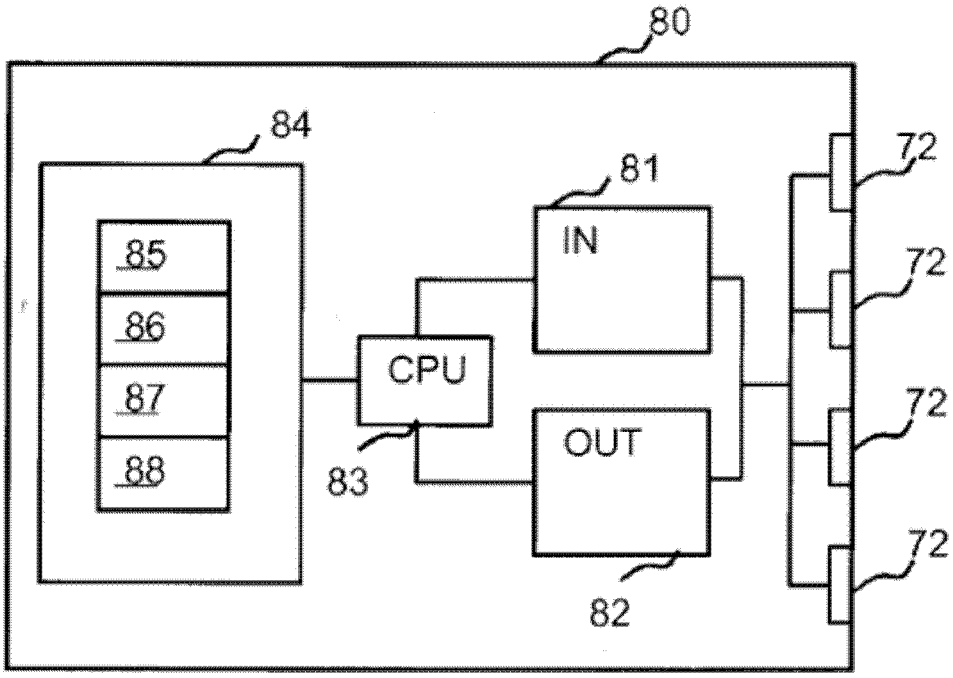
80
84
85
86
87
88
CPU
83
81
IN
OUT
82
72
72
72
72

Fig. 8

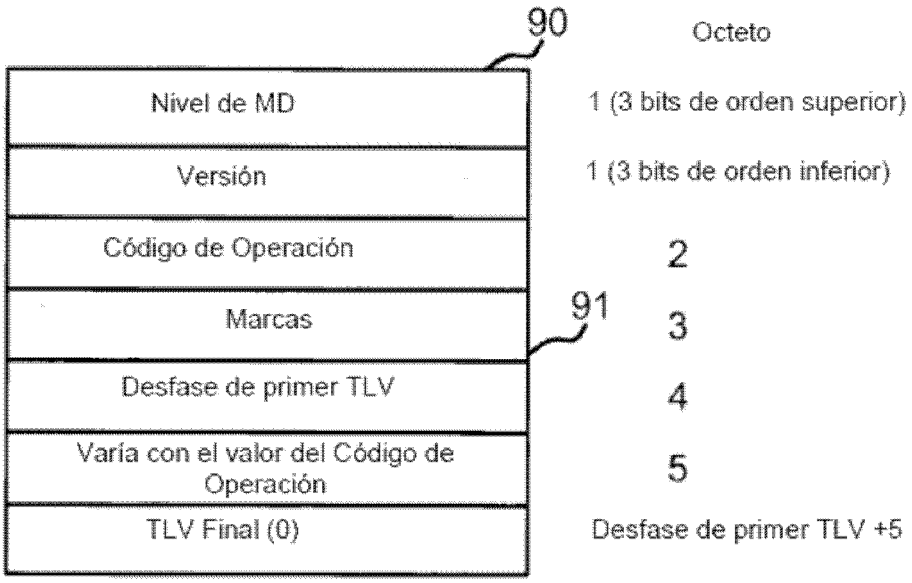

Fig. 9a

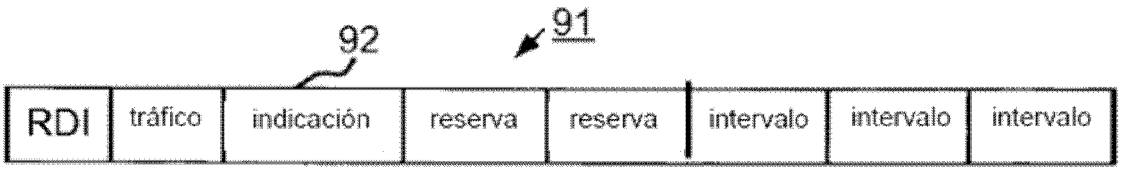

Fig. 9b

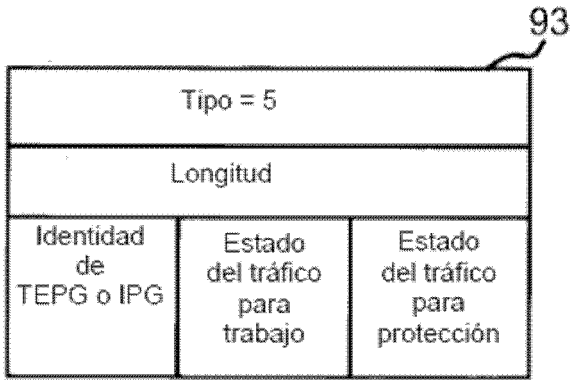

Fig. 9c