(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 364 537**

(51) Int. Cl.:
H04L 12/46 (2006.01)
H04L 12/26 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08832775 .4**
(96) Fecha de presentación : **31.10.2008**
(97) Número de publicación de la solicitud: **2232783**
(97) Fecha de publicación de la solicitud: **29.09.2010**

(54) Título: **Método de conmutación de protección de red Ethernet.**

(30) Prioridad: **02.11.2007 US 984892 P**

(45) Fecha de publicación de la mención BOPI:
06.09.2011

(45) Fecha de la publicación del folleto de la patente:
06.09.2011

(73) Titular/es: **Telefonaktiebolaget LM Ericsson (publ)**
164 83 Stockholm, SE

(72) Inventor/es: **Saltsidis, Panagiotis;**
Julien, Martin y
Monette, Sylvain

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Método de conmutación de protección de red Ethernet.

Campo Técnico

El presente invento se refiere de manera general a redes de comunicaciones y, en particular, a redes de comunicaciones que utilizan sistemas y métodos de conmutación de protección de red Ethernet en un dominio de Puente de Red Troncal de Proveedor - Ingeniería de Tráfico (PBB-TE, del inglés *Provider Backbone Bridging Traffic Engineering*).

Antecedentes

A lo largo de los últimos años, Ethernet se ha convertido en el líder indiscutible de la tecnología de Red de Área Local (LAN, del inglés *Local Area Network*) debido a las características intrínsecas de esta tecnología, tales como su simplicidad para implementarse y utilizarse, su bajo coste para emplearse, su facilidad para gestionarse, y su compatibilidad hacia atrás.

Con los servicios de datos suponiendo hoy día el grueso del tráfico, las operadoras y portadoras de telecomunicaciones están investigando la posibilidad de cosechar los mismos beneficios reemplazando su infraestructura de Jerarquía Digital Síncrona (SDH, del inglés *Synchronous Digital Hierarchy*) o su Red Óptica Síncrona (SONET, del inglés *Synchronous Optical Networking*) por una infraestructura de transporte de paquetes basada en tecnología Ethernet. Sin embargo, las redes metro y las redes troncales tienen requerimientos bastante diferentes a las de las LAN corporativas.

Consecuentemente, la tecnología Ethernet necesita mejoras específicas si pretende cumplir estos requerimientos de calidad de portadora. En el momento actual, en el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, del inglés *Institute of Electrical and Electronics Engineers*) se está trabajando en el concepto de Puente de Red Troncal de Proveedor - Ingeniería de Tráfico (PBB-TE, del inglés *Provider Backbone Bridging Traffic Engineering*), para implementar tecnología Ethernet para uso de portadora. Se está debatiendo una enmienda al estándar IEEE P802.1Q (IEEE P802.1Q-2006/D0.1, Borrador del Estándar IEEE para Redes de Área Local y Metropolitana: Redes de Área Local de Puente Virtual - *Draft IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks*), que pretende proporcionar una verdadera solución para el transporte de paquetes con calidad de portadora basado en Ethernet.

El PBB-TE (véase el documento IEEE 802.1Qay/D0.0, Borrador del Estándar para Redes de Área Local y Metropolitana - Redes de Área Local de Puente Virtual: Puentes de Red Troncal de Proveedor - Ingeniería de Tráfico, *Draft Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks: Provider Backbone Bridges – Traffic Engineering*, Mayo de 2007) propone una solución sencilla y orientada a la conexión. Esta implementación mantienen las ventajas inherentes de Ethernet, ocupándose a la vez de las deficiencias de Ethernet como protocolo de transporte de paquetes con calidad de portadora. Se forja sobre los conceptos establecidos en las enmiendas al estándar IEEE802.1Q y, en particular, la separación de red de PBB (véase el documento IEEE 802.1Qah/D3.8, Borrador del Estándar para Redes de Área Local y Metropolitana - Redes de Área Local de Puente Virtual: Puentes de Red Troncal de Proveedor, *Draft Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks: Provider Backbone Bridges,* Octubre de 2007) para proporcionar una solución escalable.

En contraste con la tecnología de Puente de Red Troncal de Proveedor (PBB), los protocolos de árbol de expansión y los protocolos de emisión/distribución no se utilizan en PBB-TE. Las bases de datos de filtrado se rellenan utilizando un sistema de gestión de red o un plano de control mejorado, permitiendo que las Rutas Conmutadas de Red Ethernet (ESPs, del inglés *Ethernet Switched Paths*) sean creadas y provistas a través de la red. Esto permite controlar el volumen de tráfico a través de la red de transporte de paquetes basada en Ethernet, lo que asegura una asignación óptima de recursos. Cada ESP representa una ruta unidireccional. Una pareja de ESPs que forman una ruta bidireccional a través de la red define un enlace o túnel PBB-TE.

Uno de los puntos clave abordados en PBB-TE se refiere al modo de proporcionar protección lineal de extremo a extremo para enlaces PBB-TE, donde un enlace PBB-TE de protección dedicado se establece para un enlace particular, y el tráfico es conmutado automáticamente del enlace PBB-TE operativo (primario) al enlace PBB-TE de protección (de respaldo) cuando ocurre un fallo en el enlace primario.

La Figura 1 es un diagrama de bloques simplificado que ilustra los elementos esenciales de un esquema 10 de protección lineal de extremo a extremo y su disposición en redes existentes para una entidad 12 de protección. El

esquema utiliza tráfico normal sobre una ESP 14 como entidad operativa y una ESP 16 como entidad de protección entre un componente 18 Oeste y un componente 20 Este. El componente Oeste incluye un proceso 22 de conmutación de protección y el componente Este incluye un proceso 24 de conmutación de protección. En los extremos de envío, el tráfico puede ser dispuesto de dos maneras. En primer lugar, puede ser dispuesto en una disposición 1+1, en la que el tráfico se envía simultáneamente tanto en la ruta operativa como en la ruta de protección (puenteada). En segundo lugar, puede ser dispuesto en una disposición 1:1 ó 1 para 1, en la que el tráfico se envía solamente en una de las rutas en cualquier instante de tiempo (conmutada). En ambas disposiciones de protección, el extremo receptor selecciona tráfico de las entidades operativas o de protección en base a información obtenida de operadores de red o procesos de Operaciones, Administración y Gestión (OAM, del inglés *Operations, Administration and Management*). En el caso 1 para 1, el "puente de protección" que envía y el “selector” que recibe deben estar coordinados.

La Unión Internacional de Telecomunicaciones - sector Telecomunicación (ITU-T, del inglés *International Telecommunication Union – Telecommunication*) define el término "puente" para el conmutador que selecciona una de los dos o ambas rutas de transmisión en el extremo que envía de un dominio de protección. Debe entenderse que esta definición no es la misma que la del término "puente" utilizado en el estándar IEEE 802. Tal como se define en el presente invento, el puente de protección lineal de la ITU-T se refiere a un "puente de protección".

En esquemas de protección lineal unidireccional, los selectores en cada extremo del dominio de protección operan de manera asíncrona. Específicamente, una acción de selección de ruta de tráfico en un extremo no resulta en una acción de selección de tráfico en el otro extremo en el tráfico en la dirección inversa. Consecuentemente, el tráfico en una dirección puede utilizar una ruta diferente que el tráfico en la otra dirección.

Sin embargo, los esquemas de protección lineal bidireccional funcionan de manera síncrona en el sentido de que una acción de selección de tráfico en un extremo también provoca una acción de selección correspondiente en el otro extremo en el tráfico en la dirección inversa. Por consiguiente, el tráfico en ambas direcciones comparte la misma ruta (es decir, bien la ruta operativa o bien la ruta de protección).

La conmutación de protección puede ser disparada por información OAM que surge de la monitorización periódica de las rutas operativa y de protección o bien de una monitorización de capa física, tal como pérdida de señal o errores de trama detectados durante la secuencia de comprobación de trama.

Los esquemas de protección lineal están configurados habitualmente para ser "revertidos" o "no revertidos", donde el tráfico de recepción y de transmisión, según corresponda, se revierte automáticamente a la ruta operativa una vez que OAM indica que el fallo o el defecto han sido eliminados.

La mayoría de los esquemas de protección lineal tienen como objetivo hoy día conmutar completamente (ambos extremos cuando sea apropiado) en menos de 50 ms desde la ocurrencia del fallo, y no sólo desde la indicación de un defecto por parte de OAM. Consecuentemente, la periodicidad de los mensajes de comprobación de continuidad de OAM debe ser casi un orden de magnitud más rápido para detectar el fallo y para transportar la información de sincronización de extremo a extremo.

La mayoría de los esquemas también incorporan temporizadores de tiempo de espera para protección y de tiempo de espera para restauración. Los tiempos de espera para protección aseguran que no se considere como fallo un evento transitorio, que surja de alguna conmutación de protección en algún nivel inferior, mientras que los tiempos de espera para restauración aseguran que el rendimiento de la ruta operativa esté totalmente recuperado antes de conmutar de nuevo a dicha ruta. Obviamente, el tiempo de recuperación total es mayor.

Por consiguiente, se necesita un mecanismo resiliente escalable de extremo a extremo por debajo de 50 ms que ofrezca capacidades de protección lineal bidireccional de extremo a extremo para túneles o enlaces PBB-TE de punto a punto en un dominio PBB-TE.

Hoy en día, se utilizan en las redes Ethernet diferentes mecanismos resilientes de tipo propietario o estándar, tales como el Protocolo de Árbol de Expansión (STP, del inglés *Spanning Tree Protocol*), el Protocolo de Árbol de Expansión Rápido (RSTP, del inglés *Rapid Spanning Tree Protocol*), el Protocolo de Árbol de Expansión Múltiple (MSTP, del inglés *Multiple Spanning Tree Protocol*), el Anillo de Paquete Resiliente (RPR, del inglés *Resilient Packet Ring*), y el Grupo Agregado de Enlaces (LAG, del inglés *Link Aggregation Group*). Sin embargo, estos mecanismos están limitados a fallos del enlace y no están diseñados para ser fácilmente escalados en redes extensas. Más aún, no soportan conmutación de protección por debajo del 50 ms ni en un anillo ni en un entorno lineal. Adicionalmente, debido a que los protocolos de árbol de expansión no se utilizan en PBB-TE, esto también excluye su utilización desde el inicio como una solución potencial para proporcionar resiliencia a un enlace PBB-TE.

En redes SDH/SONET, la función y el protocolo de Conmutación de Protección Automática (APS) proporcionan protección de extremo a extremo del circuito. Esta función y protocolo APS puede soportar conmutación de 50 ms, conmutación unidireccional y bidireccional, conmutación revertida y no revertida, conmutación manual, y/o conmutación automática. La función APS puede también soportar topologías lineales, en anillo, y en malla. La función APS permite la conmutación de circuitos en caso de fallo circuital y se utiliza en la mayor parte de las redes síncronas.

La ITU-IT, a través de la Recomendación G.8031/Y.1342, define el uso de la función y el protocolo APS para la conexión de subredes punto a punto basadas en VLAN en redes de transporte Ethernet. El protocolo APS se utiliza para coordinar los dos extremos de un dominio de protección. Sólo se envían mensajes APS en la ruta de protección. La aplicación directa de los mecanismos G.8031 en un dominio PBB-TE introduce una complejidad adicional ya que la llegada de la Unidad de Datos de Protocolo APS (PDU, del inglés *Protocol Data Unit*) para propósitos de señalización contiene una información redundante sustancial que conduce a una solución que no es eficiente en coste.

Por ejemplo, la Recomendación G.8031 establece que es deseable que se envíen Mensajes de Comprobación de Continuidad (CCMs, *Continuity Check Messages*) con un intervalo de 3,3 ms y de nuevo a continuación con un intervalo de 5 segundos. Esto permite la pérdida de hasta dos mensajes APS debidos a errores u otros fenómenos consiguiéndose todavía un tiempo de conmutación de protección de 50 ms.

La Publicación de Solicitud de Patente de EEUU número 2004/156313 a favor de Hofmeister y otros describe un método para proporcionar conmutación de protección en una red troncal de tal modo que se establecen enlaces operativo y de protección. El enlace operativo es monitorizado por una unidad de control central y se lleva a cabo una conmutación al enlace de protección cuando la unidad de control detecta un fallo. Hofmeister menciona redes Ethernet y VLANs que están conectadas a la red troncal, pero no describe la conmutación de protección de Ethernet, debido a que la red troncal no funciona de acuerdo con tecnología Ethernet, sino que solamente está conectada a una red Ethernet.

La patente de EE.UU. Nº 7.093.027 a favor de Shabtay y otros describe un método para establecer dos enlaces físicos Ethernet entre pares de nodos de una red de tal modo que se utiliza un enlace para cada dirección de comunicación entre los respectivos pares de nodos. Puede establecerse una VLAN en la red, pero la conexión física Ethernet con los dos enlaces Ethernet entre cada par de nodos permanece oculta en la red VLAN. Shabtay no describe una red troncal con conmutación de protección Ethernet entre enlaces.

Resumen

Existe en la técnica una necesidad de funcionalidad APS en un dominio PBB-TE para crear un mecanismo de conmutación de protección lineal bidireccional de extremo a extremo más simple y eficiente. El presente invento tiene por objeto obtener soluciones que atiendan a esta necesidad. En el presente invento se proporciona una solución mucho más simple basada en el intercambio de CCMs y el uso de un Indicador de Defecto Remoto (RDI, del inglés *Remote Defect Indicator*) para señalización APS.

El presente invento proporciona la capacidad de una conmutación de protección lineal bidireccional 1:1 en un dominio PBB-TE que se apoya en el estándar IEEE 802.1Qag Gestión de Fallos de Conectividad (CFM, del inglés *Connectivity Fault Management*), CCMs y RDI. El presente invento también proporciona una solución simplificada y eficiente, que está bien situada para utilizar tecnología Ethernet.

Por consiguiente, en una realización, el presente invento se orienta hacia un método para proporcionar conmutación de protección Ethernet en un Dominio PBB-TE. El método comienza estableciendo dos enlaces PBB-TE entre un primer componente-B y un segundo componente-B. Cada enlace incluye dos Rutas Conmutadas de Red Ethernet (ESPs, del inglés *Ethernet Switching Paths*), cada una de ellas asociada con un Identificador VLAN (VID, del inglés *Virtual Local Area Network Identifier*) posiblemente distinto. El método incluye el mapeo de tráfico de datos al primer enlace PBB-TE, donde el primer enlace PBB-TE corresponde a una entidad operativa y el segundo enlace PBB-TE corresponde a una entidad de protección de respaldo. El tráfico de datos se envía en el primer enlace a través de una ESP asociada con un VID en una dirección y de otra ESP asociada con un VID posiblemente diferente en la dirección opuesta. Los enlaces PBB-TE son monitorizados para detectar fallos. En el momento en que se detecta un fallo en uno de los enlaces PBB-TE, se re-mapea el tráfico de datos al otro enlace PBB-TE a través de una tercera ESP asociada con un tercer VID y una cuarta ESP asociada con un cuarto VID.

En otra realización, el presente invento se orienta hacia un sistema para proporcionar conmutación de protección Ethernet en un Dominio PBB-TE. El sistema incluye un primer enlace PBB-TE entre un primer componente-B y un segundo componente-B, donde el primer enlace PBB-TE tiene una primera ESP para tráfico unidireccional desde el

primer componente-B hacia segundo componente-B y una segunda ESP para tráfico unidireccional desde el segundo componente-B hacia primer componente-B. La primera ESP está asociada con un primer VID y la segunda ESP está asociada con un segundo VID. El sistema también incluye un segundo enlace PBB-TE entre el primer componente-B y el segundo componente-B. El segundo PBB-TE tiene una tercera ESP para tráfico unidireccional desde el primer componente-B hacia el segundo componente-B y una cuarta ESP para tráfico unidireccional desde el segundo componente-B hacia el primer componente-B. La tercera ESP está asociada con un tercer VID y la cuarta ESP está asociada con un cuarto VID. Adicionalmente, el sistema mapea tráfico de datos al primer enlace PBB-TE, donde el primer enlace PBB-TE corresponde a una entidad operativa y el segundo enlace PBB-TE corresponde con una entidad de protección de respaldo. Los dos enlaces PBB-TE son monitorizados para detectar fallos. En el momento en que se detecta un fallo en uno de los enlaces PBB-TE, se re-mapea el tráfico de datos al otro enlace PBB-TE.

En otra realización más, el presente invento se orienta hacia un nodo para proporcionar conmutación de protección Ethernet en un Dominio PBB-TE. El nodo se conecta a un primer enlace PBB-TE entre el nodo y un segundo nodo. El primer enlace PBB-TE tiene una primera ESP para tráfico unidireccional desde el primer nodo hacia el segundo nodo y una segunda ESP para tráfico unidireccional desde el segundo nodo hacia el nodo. La primera ESP está asociada con un primer VID y la segunda ESP está asociada a un segundo VID. El nodo también se conecta con un segundo enlace PBB-TE entre el nodo y el segundo nodo. El segundo enlace PBB-TE tiene una tercera ESP para tráfico unidireccional desde el primer nodo hacia el segundo nodo y una cuarta ESP para tráfico unidireccional desde el segundo nodo hacia el nodo. La tercera ESP está asociada con un tercer VID y la cuarta ESP está asociada a un cuarto VID. El nodo mapea tráfico de datos al primer enlace PBB-TE. El primer enlace PBB-TE corresponde a una entidad operativa y el segundo enlace PBB-TE corresponde a una entidad de protección de respaldo. Los dos enlaces PBB-TE son monitorizados para detectar fallos. En el momento en que se detecta un fallo en uno de los enlaces PBB-TE, el nodo re-mapea el tráfico de datos al otro enlace PBB-TE.

Breve Descripción de los Dibujos

La Figura 1 (técnica anterior) es un diagrama de bloques simplificado que ilustra los elementos esenciales de un esquema de protección lineal de extremo a extremo y su disposición en redes existentes para una entidad de protección;

La Figura 2 es un diagrama de bloques simplificado de una red que ilustra la configuración de enlaces en la realización preferida del presente invento;

La Figura 3 es un diagrama de bloques simplificado que ilustra el mapeo de tráfico de datos específico a una entidad operativa en la red de la Figura 2;

La Figura 4 es un diagrama de bloques simplificado que ilustra un fallo en una entidad operativa de la red de la Figura 2;

La Figura 5 es un diagrama de bloques simplificado de la red que ilustra el re-mapeo de tráfico de datos específico a la entidad de protección; y

La Figura 6 es un diagrama de flujo que ilustra los pasos para el establecimiento y el mapeo de enlaces PBB-TE para proporcionar capacidades de conmutación de protección en un dominio PBB-TE.

Descripción Detallada

El presente invento es un sistema y un método para conmutación de protección Ethernet en un dominio PBB-TE. El presente invento proporciona capacidades de conmutación de protección bidireccional lineal 1:1 en un dominio PBB-TE. En un dominio PBB-TE, los Puentes de Borde de Red Troncal (BEBs, del inglés *Backbone Edge Bridges*) señalan la demarcación entre la Red en Puente de Red Troncal de Proveedor (PBBN, del inglés *Provider Backbone Bridged Network*) de interés y las redes conectadas a ella. Se asume que estos BEBs son B-BEBs o IB-BEBs donde cada uno de ellos contiene un componente-B. Se define el dominio de protección como el área entre los Puertos de Red Troncal de Cliente (CBPs, del inglés *Customer Backbone Ports*) en los diferentes Componentes-B de los BEBs implicados. Se proporcionan ESPs de un BEB a otro, identificado cada uno de ellos mediante la n-upla <B-DA, B-SA, B-VID>. Cada ESP representa una ruta unidireccional y las parejas de ESP que forman la ruta bidireccional definen un enlace PBB-TE. Las ESPs que pertenecen al mismo enlace PBB-TE están co-enrutadas, pero pueden también ser identificadas mediante diferentes B-VIDs.

La Figura 2 es un diagrama de bloques simplificado de una red 100 que ilustra la configuración de enlace PBB-TE en la realización preferida del presente invento. La red 100 incluye al menos dos enlaces PBB-TE, el enlace 102 PBB-TE (Entidad Operativa) y el enlace 104 PBB-TE (Entidad de Protección), entre un BEB 106 que tiene un Componen-

te-B 108 Oeste y un BEB 110 que tiene un Componente-B 112 Este. El enlace 102 PBB-TE incluye una ESP 114 de Oeste a Este y una ESP 116 de Este a Oeste. Cada ESP puede corresponder al mismo o a diferentes ajustes B-VID para las dos direcciones diferentes. El enlace 104 PBB-TE incluye una ESP 118 de Oeste a Este y una ESP 120 de Este a Oeste.

Las ESPs 114, 116, 118 y 120 se establecen configurando entradas en las bases de datos de filtrado (FDBs, del inglés *Filtering Databases*) en todos los puentes que esas ESPs necesitan atravesar y debe ser establecida la afiliación de cada puerto participante a una VLAN. Existen dos Componentes-B en los extremos de las ESPs. Como se muestra en la Figura 2, el Componente-B 108 Oeste incluye un Puerto 126 de Red Troncal de Cliente (CBP, del inglés *Customer Backbone Port*) y un cierto número de Puertos de Red de Proveedor (PNPs, del inglés *Provider Network Ports*), el PNP 122, y el PNP 124. El Componente-B 112 Este incluye un CBP 164, y un número de PNPs, el PNP 160 y el PNP 162. La ESP 114 asociada con el VID 128 es parte de la Entidad Operativa 102 y se configura entre el CBP 126 y el CBP 164. Adicionalmente, hay otra ESP 118, asociada con el VID 130, que forma parte de la Entidad de Protección 104 y se configura entre el CBP 126 y el CBP 164. Debido a que la ESP 114 está asociada con el VID 128, los puertos CBP 126 y PNP 122 en el componente-B 108 Oeste y los puertos PNP 160 y CBP 164 en el Componente-B 112 Este se configuran para ser miembros del conjunto de miembros del VID 128. Debido a que la ESP 118 está asociada con el VID 130, los puertos CBP 126 y PNP 124 en el componente-B 108 Oeste y los puertos PNP 162 y CBP 164 en el Componente-B 112 Este se configuran para ser miembros del conjunto de miembros del VID 130. En la dirección opuesta del componente-B 112 Este al componente-B 108 Oeste, está situada la ESP 116 asociada con el VID 166 que forma parte de la Entidad Operativa 102 y se configura entre el CBP 164 y el CBP 126 y una cuarta ESP 120, asociada con el VID 168, que forma parte de la Entidad de Protección 104 y se configura entre el CBP 164 y el CBP 126. Debido a que la ESP 116 está asociada con el VID 166, los puertos CBP 126 y PNP 122 en el componente-B 108 Oeste y los puertos PNP 160 y CBP 164 en el Componente-B 112 Este se configuran para ser miembros del conjunto de miembros del VID 166. Debido a que la ESP 120 está asociada con el VID 168, los puertos CBP 126 y PNP 124 en el componente-B 108 Oeste y los puertos PNP 162 y CBP 164 en el Componente-B 112 Este se configuran para ser miembros del conjunto de miembros del VID 168. Las tramas están etiquetadas para un VID específico y sólo pueden salir o entrar a través de puertos asociados.

Configurar los enlaces PBB-TE significa que también se configuran las Asociaciones de Mantenimiento (MAs, del inglés *Maintenance Associations*). Se establece una MA para monitorizar el enlace PBB-TE superior (enlace-1) y se establece una segunda MA para monitorizar el enlace PBB-TE inferior (enlace-2). Cada una de estas dos MAs puede asociarse con una pareja de Identificadores de Red de Área Local Virtual (VIDs, del inglés *Virtual LAN Identifiers*), donde cada VID corresponde a una ESP unidireccional. La MA que monitorizada el enlace-1 PBB-TE puede entonces contener ambos VIDs en su lista de VID. Los Puntos Extremos de Mantenimiento (MEPs, del inglés *Maintenance End Points*), asociados con esta MA son MEPs Up, configurados en los CBPs que demarcan el enlace PBB-TE asociado. Por ejemplo, cuando se utilizan dos VIDs para un enlace PBB-TE, cada uno de los MEPs tiene su propio VID primario (por ejemplo, VID 128 para el MEP en el componente-B Oeste asociado con el enlace 102 PBB-TE, y VID 166 para el MEP en el componente-B Este). En esta configuración, cada MEP puede recibir tramas que están etiquetadas con cualquiera de los VIDs en la lista de MA, pero pueden enviar tramas que están etiquetadas sólo con el VID primario de ese MEP. En particular, en el ejemplo descrito, el MEP para la entidad operativa en el componente-B Oeste puede enviar sólo Mensajes de Comprobación de Continuidad (CCMs, del inglés *Continuity Checked Messages*) especificados etiquetados con el VID 128 mientras que el MEP correspondiente en el componente Este puede enviar sólo tramas etiquetadas con el VID 166. Ambos MEPs pueden recibir tramas CCM que están etiquetadas para el VID 166 ó el VID 128.

El tráfico de datos se mapea a un enlace PBB-TE configurando los parámetros de la CBP. En particular, el identificador de servicio de instancia de red troncal CBP se utiliza para que solamente se permita el transporte de instancias de servicio específicas por parte del enlace PBB-TE y la columna B-VID en la tabla de Instancia de Servicio de Red Troncal o, si esto no es soportado, el parámetro del Puerto VID (PVID, del inglés *Port VLAN Identifier*) del CBP puede utilizarse para mapear las instancias de servicio identificadas a una ESP específica. La Figura 3 es un diagrama de bloques simplificado que ilustra el mapeo de tráfico de datos específico a una entidad operativa en la red 100 de la Figura 2. El valor PVID del CBP para el CBP 126 está asociado con el VID 128, mientras que en el CBP 164 está asociada con el VID 166. Tal y como se representa, la red incluye un MEP 200 asociado con el VID 128 en el Componente-B 108 Oeste y un MEP 202 que está asociado con el VID 166 en el Componente-B 112 Este.

Como resultado de esta configuración, tramas con un valor de Identificador de Instancia de Servicio de Red Troncal (I-SID, del inglés *Backbone Service Instance Identifier*) específico que alcanzan el CBP en el componente-B 108 Oeste se mapean a la ESP 114, mientras que tramas específicas que alcanzan el CBP en el componente-B 112 Este se mapean a la ESP 116. Por consiguiente, el enlace 102 PBB-TE corresponde a la entidad operativa y el enlace 104 PBB-TE corresponde a una entidad de protección en espera. Sin tener en cuenta cómo se mapea el tráfico de

datos a los enlaces PBB-TE, las tramas CCM se intercambian en las entidades operativa y protegida con el fin de comprobar regularmente la conectividad proporcionada.

La Figura 4 es un diagrama de bloques simplificado que ilustra un fallo en una entidad operativa de la red 100 de la Figura 2. Si ocurre un fallo en alguna de las ESPs, el MEP en el extremo receptor es notificado. Por ejemplo, si ocurre un fallo 300 en la ESP 114, el MEP 202 en el componente-B 112 Este declara un defecto en el MEP remoto poniendo a 1 un parámetro rMEPCCMdefect. El contador del temporizador para el vencimiento de temporización de CCMs tiene una granularidad más fina o igual a 1/4 del tiempo representado por la variable CCMinterval (el tiempo configurado entre transmisiones CCM). Un Puente no pone a 1 el parámetro rMEPCCMdefect en menos de (3,25 * CCMinterval) segundos desde la recepción de un CCM, y pone a 1 el parámetro rMEPCCMdefect en menos de (3,25 * CCMinterval) segundos después de la recepción del último CCM. La puesta a 1 del parámetro rMEPCCMdefect resulta en un cambio del parámetro PVID del CBP al VID 168, que es el BVID de la ESP asociada provista en el enlace 104 PBB-TE de protección (el parámetro PVID también cambia cuando se ponen a 1 los parámetros xConCCMdefect o errorCCMdefect ya que estos indican un problema muy serio de mala configuración). Todos los CCMs subsiguientes enviados a través del MEP asociado con el VID 166 tienen sus campos RDI puestos a 1 (mientras el MEP no reciba los CCMs correctos).

La Figura 5 es un diagrama de bloques simplificado de la red 100 que ilustra el re-mapeo de tráfico de datos específico a la entidad de protección. La recepción de una trama CCM con el campo RDI puesto a 1 (o un evento que cause la puesta a 1 del parámetro someRMEPCCMdefect, el parámetro xConCCMdefect o el parámetro errorCCMdefect) provoca que la entrada asociada B-VID en la tabla de Instancia de Servicio de Red Troncal cambie al valor pre-configurado de la ESP de protección (es decir, asociándose con la ESP 118 y el correspondiente VID 130). De manera alternativa, si la columna B-VID no está soportada, el parámetro PVID de la CBP 126 en el componente-B 108 Oeste cambia al valor pre-configurado de la ESP de protección. Esto resulta en el traslado de la instancia de servicio específico al enlace 104 de protección PBB-TE tal y como se muestra en la Figura 5.

La Figura 6 es un diagrama de flujo que ilustra los pasos para el establecimiento y el mapeo de enlaces PBB-TE para proporcionar capacidades de conmutación de protección en un dominio PBB-TE. A continuación se explicará el método con referencia a las Figuras 2-6. En el paso 400, se establecen los enlaces PBB-TE. El enlace 102 PBB-TE se establece como entidad operativa e incluye la ESP 114 asociada con el VID 128 en una dirección (es decir, oeste a este) y la ESP 116 asociada con el VID 166 en otra dirección (es decir, este a oeste). El enlace 104 PBB-TE se establece como la entidad de protección e incluye la ESP 118 asociada con el VID 130 en una dirección (es decir, oeste a este) y la ESP 120 asociada con el VID 168 en otra dirección (es decir, este a oeste). A continuación, en el paso 402, el tráfico de datos se mapea al enlace PBB-TE especificado (es decir, el enlace 102 PBB-TE) configurando los parámetros del CBP. En particular, el identificador de servicio de instancia de red troncal CBP se utiliza para que solamente se permita el transporte de instancias de servicio específicas por parte del enlace PBB-TE y la columna B-VID del CBP en sus tablas de Instancia de Servicio de Red Troncal. Alternativamente, si esto no es soportado, el parámetro del Puerto VID (PVID, del inglés *Port VLAN Identifier*) puede utilizarse para mapear las instancias de servicio identificadas a una ESP específica. El valor del B-VID o del PVID del CBP para el CBP 126 está asociado con el VID 128 mientras que el CBP 164 está asociado con el VID 166. Como resultado de esta configuración, tramas con un valor de I-SID específico que alcanzan el CBP en el componente-B 108 Oeste se mapean a la ESP 114, mientras que tramas específicas que alcanzan el CBP en el componente-B 112 Este se mapean en la ESP 116. Por consiguiente, el enlace 102 PBB-TE corresponde a la entidad operativa y el enlace 104 PBB-TE corresponde a una entidad de protección en espera. Sin tener en cuenta cómo se mapea el tráfico de datos a los enlaces PBB-TE, las tramas CCM se intercambian en las entidades operativa y protegida con el fin de comprobar regularmente la conectividad proporcionada.

A continuación el método continúa con el paso 404 en el que se monitorizar los enlaces buscando fallos. A continuación, en el paso 406, se determina si se detecta un fallo. Si no se detecta un fallo, el método continúa monitorizando los enlaces en el paso 404. Sin embargo, en el paso 406, si se determina la detección de un fallo en la entidad operativa, el método continúa en el paso 408 en el que se re-mapea el tráfico de datos a la entidad de protección. Si ocurre un fallo en alguna de las ESPs, el MEP en el extremo receptor es notificado. Por ejemplo, si ocurre un fallo 300 en la ESP 114, el MEP 202 en el componente-B 112 Este declara un defecto en el MEP remoto poniendo a 1 un parámetro rMEPCCMdefect. El contador del temporizador para el vencimiento de temporización de CCMs tiene una granularidad más fina o igual a 1/4 del tiempo representado por la variable CCMinterval (el tiempo configurado entre transmisiones CCM). Un Puente no pone a 1 el parámetro rMEPCCMdefect en menos de (3,25 * CCMinterval) segundos desde la recepción de un CCM, y pone a 1 el parámetro rMEPCCMdefect en menos de (3,25 * CCMinterval) segundos después de la recepción del último CCM. La puesta a 1 del parámetro rMEPCCMdefect resulta en un cambio del parámetro PVID del CBP a VID 168, que es el BVID de la ESP asociada provista en el enlace 104 PBB-TE de protección. Todos los CCMs subsiguientes enviados a través del MEP asociado con el VID 166 tienen sus campos RDI puestos a 1 (mientras el MEP no reciba los CCMs correctos). Una recepción de una

trama CCM con el campo RDI puesto a 1 (o un evento que cause la puesta a 1 del parámetro someRMEPCCMdefect, el parámetro xConCCMdefect o el parámetro errorCCMdefect) provoca un cambio en el valor de B-VID en la columna de la tabla de Instancia de Servicio de Red Troncal o en el parámetro PVID del CBP 126 en el componente-B 108 Oeste, al valor pre-configurado de la ESP de protección (es decir, asociándose con la ESP 118 y el correspondiente VID 130). Esto resulta en el traslado de la instancia de servicio específico al enlace 104 de protección PBB-TE.

El presente invento proporciona un sistema y un método que ofrece capacidad de conmutación de protección bidireccional lineal 1:1 en un dominio PBB-TE que se apoya en el estándar IEEE 802.1Qag Gestión de Fallos de Conectividad (CFM, del inglés *Connectivity Fault Management*), CCMs y RDI. El presente invento también proporciona una solución simplificada y eficiente, que está bien alineada con las características intrínsecas de la tecnología Ethernet.

El presente invento puede por supuesto ser llevado a cabo de otras maneras específicas a las descritas en la presente memoria sin apartarse de las características esenciales del invento. Las realizaciones presentes, por lo tanto, deben ser consideradas a todos los efectos como ilustrativas y no restrictivas y se pretende que todos los cambios que se lleven a cabo dentro del significado y el rango de equivalencia de las reivindicaciones adjuntas estén contenidos en su seno.

REIVINDICACIONES

1.- Un método para proporcionar conmutación de protección Ethernet en un Dominio de Puente de Red Troncal de Proveedor - Ingeniería de Tráfico (*Provider Backbone Bridging Traffic Engineering*), PBB-TE, donde el método comprende los pasos de: establecer (400) un primer enlace (102) PBB-TE entre un primer componente-B (108) y un segundo componente-B (112), donde el primer enlace PBB-TE tiene una primera ruta de conmutación Ethernet, ESP, (114) para tráfico unidireccional desde el primer componente-B hacia segundo componente-B y una segunda ESP (116) para tráfico unidireccional desde el segundo componente-B hacia el primer componente-B, en el que la primera ESP está asociada con un primer Identificador VLAN, VID, (128) y la segunda ESP está asociada con un segundo VID (166); establecer (400) un segundo enlace (104) PBB-TE entre el primer componente-B (108) y el segundo componente-B (112), donde el segundo enlace PBB-TE tiene una tercera ESP (118) para tráfico unidireccional desde el primer componente-B hacia el segundo componente-B y una cuarta ESP (120) para tráfico unidireccional desde el segundo componente-B hacia el primer componente-B, en el que la tercera ESP está asociada con un tercer VID (130) y la cuarta ESP está asociada con un cuarto VID (168); mapear (402) tráfico de datos al primer enlace (102) PBB-TE, donde el primer enlace PBB-TE corresponde a una entidad operativa y el segundo enlace (104) PBB-TE corresponde a una entidad de protección de respaldo; monitorizar (404) el primer enlace PBB-TE para detectar fallos; y en el momento (406) de detectar un fallo en el primer enlace (102) PBB-TE, re-mapear (408) tráfico de datos al segundo enlace (104) PBB-TE.

2.- El método de acuerdo con la reivindicación 1ª, en el que el paso de monitorización también incluye monitorizar el segundo enlace PBB-TE para detectar fallos, en el que el tráfico de datos se re-mapea al primer enlace PBB-TE cuando se detecta un fallo en el segundo enlace PBB-TE.

3.- El método de acuerdo con la reivindicación 1ª, en el que: el primer componente-B (108) incluye un primer puerto (122) de entrada asociado con el segundo VID (166) y un primer puerto (122) de salida asociado con el primer VID (128), donde el primer puerto de entrada recibe tráfico de datos a través de la segunda ESP (116) y el primer puerto de salida envía tráfico de datos a través de la primera ESP (114) al segundo componente-B; y el segundo componente-B (112) incluye un segundo puerto (160) de entrada asociado con el primer VID (128) y un segundo puerto (160) de salida asociado con el segundo VID (166), donde el segundo puerto de entrada recibe tráfico de datos a través de la primera ESP (114) y el segundo puerto de salida envía tráfico de datos a través de la segunda ESP (116) al primer componente-B.

4.- El método de acuerdo con la reivindicación 3ª, en el que el paso de re-mapear datos al segundo enlace PBB-TE incluye reconfigurar los puertos en el primer componente-B y el segundo componente-B para enviar y recibir tráfico a través de la tercera y la cuarta ESPs.

5.- El método de acuerdo con la reivindicación 1ª, en el que una primera Asociación de Mantenimiento (*Maintenance Associations*), MA, monitoriza el primer enlace PBB-TE y una segunda MA monitoriza el segundo enlace PBB-TE para detectar fallos.

6.- El método de acuerdo con la reivindicación 5ª, en el que la primera MA está asociada con el primer VID y el segundo VID y la segunda MA está asociada con el tercer VID y el cuarto VID.

7.- El método de acuerdo con la reivindicación 6ª, en el que: el primer componente-B (108) incluye un primer Punto Extremo de Mantenimiento (*Maintenance End Point*), MEP, (200) para monitorizar la primera ESP (114), donde el primer MEP está asociado con el primer VID (128); el segundo componente-B (112) incluye un segundo MEP (202) para monitorizar la segunda ESP (116), donde el segundo MEP está asociado con el segundo VID (166); el primer MEP envía Mensajes de Comprobación de Continuidad (*Continuity Check Messages*), CCMs, al segundo componente-B a través de la primera ESP (114) y el segundo MEP envía CCMs a través de la segunda ESP (116).

8.- El método de acuerdo con la reivindicación 7ª, en el que, en el momento de detectar un fallo, el primer o el segundo MEP detecta la fallo y pone a 1 un parámetro de establecimientos de defecto, activando de esta manera el paso de re-mapear tráfico de datos al segundo enlace PBB-TE.

9.- El método de acuerdo con la reivindicación 6ª, en el que: el primer componente-B (108) incluye un tercer Punto Extremo de Mantenimiento, MEP, para monitorizar la tercera ESP (118), donde el tercer MEP está asociado con el tercer VID (130); el segundo componente-B (112) incluye un cuarto MEP para monitorizar la cuarta ESP (120), donde el cuarto MEP está asociado con el cuarto VID (168); el tercer MEP envía Mensajes de Comprobación de Continuidad, CCMs, al segundo componente-B a través de la tercera ESP (118) y el cuarto MEP envía CCMs al primer componente-B a través de la cuarta ESP (120).

10.- El método de acuerdo con la reivindicación 1ª, que incluye adicionalmente el paso de enviar Mensajes de

Comprobación de Continuidad, CCMs, a través del primer (102) y el segundo (104) enlace PBB-TE para comprobar la conectividad de los enlaces.

11.- Un sistema para proporcionar conmutación de protección Ethernet en un Dominio de Puente de Red Troncal de Proveedor - Ingeniería de Tráfico (*Provider Backbone Bridging Traffic Engineering*), PBB-TE, donde el sistema comprende: un primer enlace (102) PBB-TE entre un primer componente-B (108) y un segundo componente-B (112), donde el primer enlace PBB-TE tiene una primera ruta de conmutación Ethernet, ESP, (114) para tráfico unidireccional desde el primer componente-B hacia segundo componente-B y una segunda ESP (116) para tráfico unidireccional desde el segundo componente-B hacia el primer componente-B, en el que la primera ESP está asociada con un primer Identificador VLAN, VID, (128) y la segunda ESP está asociada con un segundo VID (166); un segundo enlace (104) PBB-TE entre el primer componente-B y el segundo componente-B, donde el segundo enlace PBB-TE tiene una tercera ESP (118) para tráfico unidireccional desde el primer componente-B hacia el segundo componente-B y una cuarta ESP (120) para tráfico unidireccional desde el segundo componente-B hacia el primer componente-B, en el que la tercera ESP está asociada con un tercer VID (130) y la cuarta ESP está asociada con un cuarto VID (168); medios (126) para mapear (402) tráfico de datos al primer enlace (102) PBB-TE, donde el primer enlace PBB-TE corresponde a una entidad operativa y el segundo enlace PBB-TE corresponde a una entidad de protección de respaldo; medios (200, 202) para monitorizar el primer enlace (102) PBB-TE para detectar fallos; y medios (126) para re-mapear tráfico de datos al segundo enlace PBB-TE en respuesta a la detección de un fallo en el primer enlace PBB-TE.

12.- El sistema de acuerdo con la reivindicación 11ª, que comprende adicionalmente una primera Asociación de Mantenimiento, MA, para monitorizar el primer enlace PBB-TE y una segunda MA para monitorizar el segundo enlace PBB-TE.

13.- El sistema de acuerdo con la reivindicación 12ª, en el que la primera MA está asociada con el primer VID y el segundo VID y la segunda MA está asociada con el tercer VID y el cuarto VID.

14.- El sistema de acuerdo con la reivindicación 13ª, en el que: el primer componente-B (108) incluye un primer Punto Extremo de Mantenimiento, MEP, (200) para monitorizar la primera ESP (114), donde el primer MEP está asociado con el primer VID (128); el segundo componente-B (112) incluye un segundo MEP (202) para monitorizar la segunda ESP (116), donde el segundo MEP está asociado con el segundo VID (166); el primer MEP envía Mensajes de Comprobación de Continuidad, CCMs, al segundo componente-B a través de la primera ESP (114) y el segundo MEP envía CCMs al primer componente-B a través de la segunda ESP (116).

15.- El sistema de acuerdo con la reivindicación 14ª, en el que: el primer componente-B (108) incluye un tercer MEP para monitorizar la tercera ESP (118), donde el tercer MEP está asociado con el tercer VID (130); el segundo componente-B (112) incluye un cuarto MEP para monitorizar la cuarta ESP (120), donde el cuarto MEP está asociado con el cuarto VID (168); el tercer MEP envía CCMs al segundo componente-B a través de la tercera ESP (118) y el cuarto MEP envía CCMs al primer componente-B a través de la cuarta ESP (120).

16.- El sistema de acuerdo con la reivindicación 14ª, en el que, en el momento de detectar un fallo, el primer o el segundo MEP detecta la fallo y pone a 1 un parámetro de establecimientos de defecto, activando de esta manera el paso de re-mapear tráfico de datos al segundo enlace PBB-TE.

17.- Un nodo (108) para proporcionar conmutación de protección Ethernet en un Dominio de Puente de Red Troncal de Proveedor - Ingeniería de Tráfico (*Provider Backbone Bridging Traffic Engineering*), PBB-TE, donde el nodo comprende: medios (122) para conectarse a un primer enlace (102) PBB-TE entre el nodo y un segundo nodo (112), donde el primer enlace PBB-TE tiene una primera ruta de conmutación Ethernet, ESP, (114) para tráfico unidireccional desde el nodo hacia el segundo nodo y una segunda ESP (116) para tráfico unidireccional desde el segundo nodo hacia el nodo, en el que la primera ESP está asociada con un primer Identificador VLAN, VID, (128) y la segunda ESP está asociada con un segundo VID (166); medios (124) para conectarse a un segundo enlace (104) PBB-TE entre el nodo y el segundo nodo, donde el segundo enlace PBB-TE tiene una tercera ESP (118) para tráfico unidireccional desde el nodo hacia el segundo nodo y una cuarta ESP (120) para tráfico unidireccional desde el segundo nodo hacia el nodo, en el que la tercera ESP está asociada con un tercer VID (130), y la cuarta ESP está asociada con un cuarto VID (168); medios (126) para mapear tráfico de datos al primer enlace PBB-TE, donde el primer enlace PBB-TE corresponde a una entidad operativa y el segundo enlace PBB-TE corresponde a una entidad de protección de respaldo; medios (200) para monitorizar el primer enlace PBB-TE para detectar fallos; y medios (126) para re-mapear tráfico de datos al segundo enlace (104) PBB-TE en el momento de detectar un fallo en el primer enlace (102) PBB-TE.

18.- El nodo de acuerdo con la reivindicación 17ª, en el que los medios de monitorización también incluyen medios para monitorizar el segundo enlace (104) PBB-TE para detectar fallos, en el que cuando se detecta un fallo en el

segundo enlace PBB-TE, los medios de re-mapeo re-mapean tráfico de datos al primer enlace (102) PBB-TE.

19.- El nodo de acuerdo con la reivindicación 17ª, en el que el nodo incluye un primer puerto (122) de entrada asociado con el segundo VID (166) y un primer puerto (122) de salida asociado con el primer VID (128), donde el primer puerto de entrada recibe tráfico de datos a través de la segunda ESP (116) y el primer puerto de salida envía tráfico de datos a través de la primera ESP (114) al segundo componente-B.

20.- El nodo de acuerdo con la reivindicación 19ª, en el que el tráfico de datos se re-mapea al segundo enlace PBB-TE reconfigurando los puertos en el nodo para enviar y recibir tráfico a través de la tercera ESP y la cuarta ESP.

21.- El nodo de acuerdo con la reivindicación 17ª, que comprende adicionalmente una primera Asociación de Mantenimiento, MA, para monitorizar el primer enlace PBB-TE y una segunda MA para monitorizar el segundo enlace PBB-TE.

22.- El nodo de acuerdo con la reivindicación 21ª, en el que la primera MA está asociada con el primer VID y el segundo VID, y la segunda MA está asociada con el tercer VID y el cuarto VID.

23.- El nodo de acuerdo con la reivindicación 17ª, que comprende adicionalmente medios para enviar Mensajes de Comprobación de Continuidad, CCMs, a través del primer y el segundo enlace PBB-TE para comprobar la conectividad de los enlaces.

24.- El nodo de acuerdo con la reivindicación 17ª, en el que el nodo es un Componente-B de un Puente de Borde de Red Troncal (*Backbone Edge Bridge*).

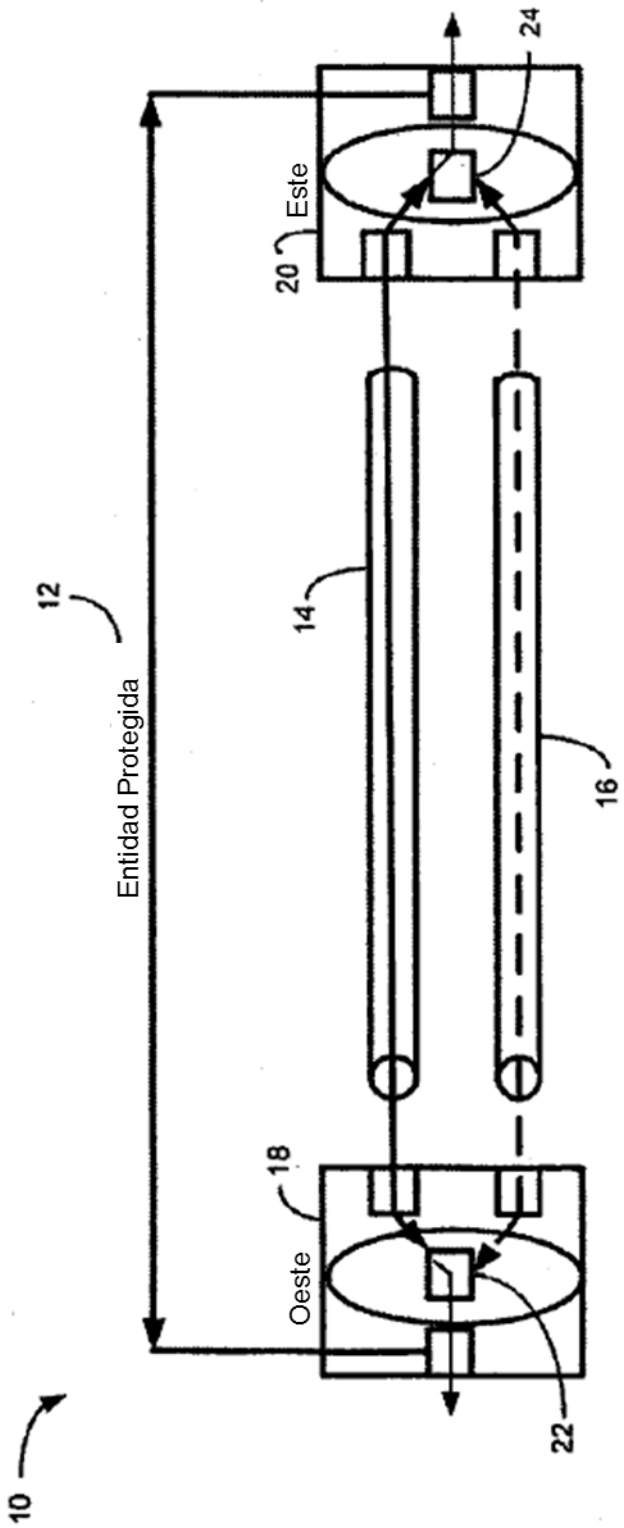


FIG. 1
(Técnica Anterior)

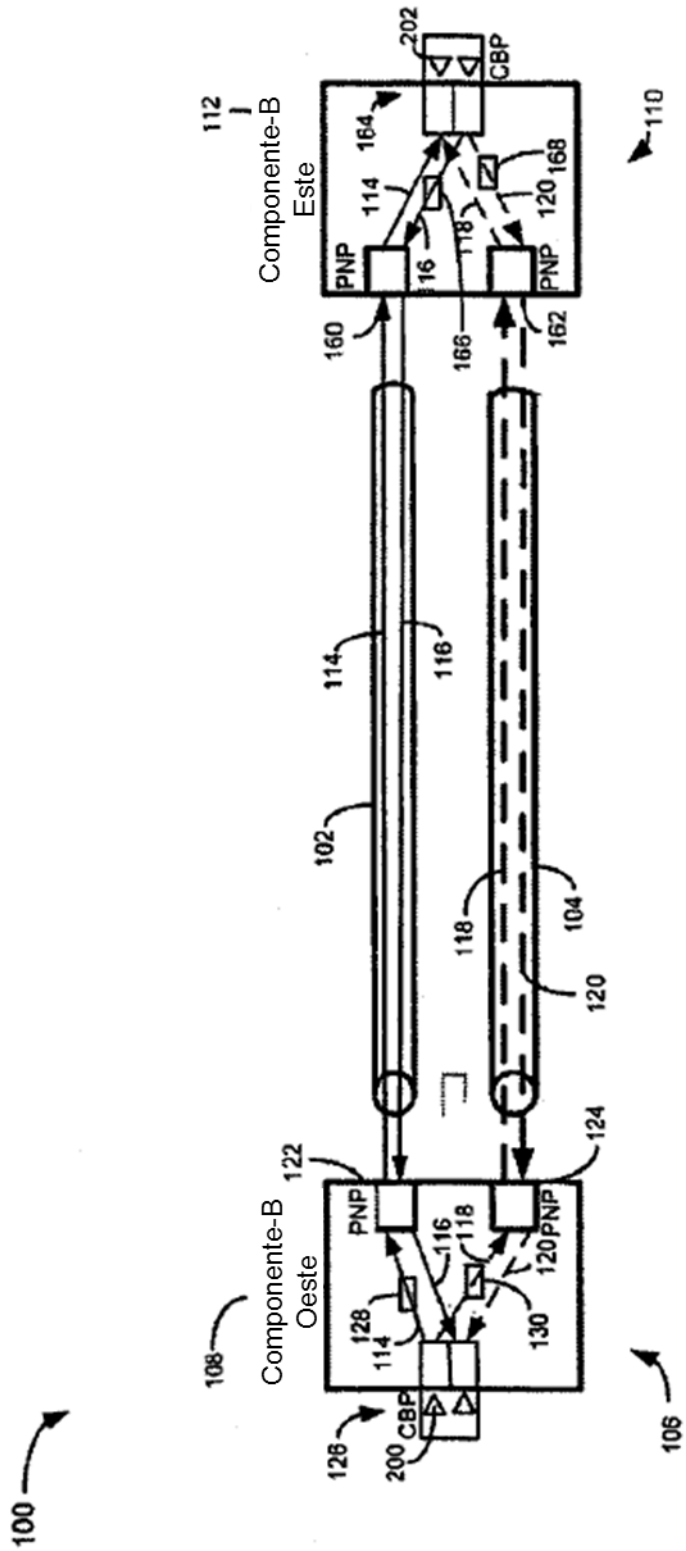

100
112
Componente-B
Este
110
202
CBP
164
114
168
120
118
16
PNP
PNP
160
166
162
114
116
102
104
118
120
122
124
Componente-B
Oeste
108
106
PNP
PNP
116
118
120
128
114
130
126
200
CBP

FIG. 2

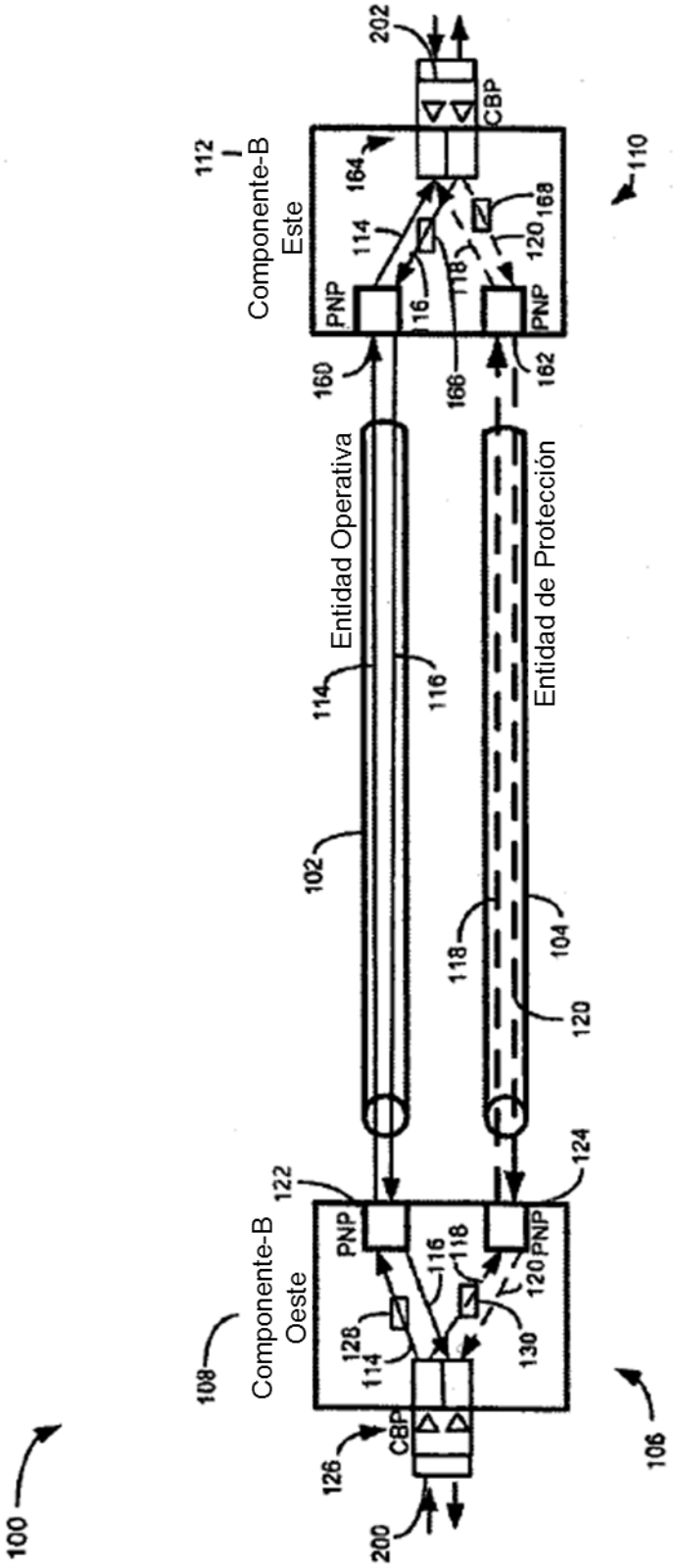

100
112
Componente-B Este
110
202
CBP
164
168
120
114
118
116
PNP
PNP
160
166
162
Entidad Operativa
Entidad de Protección
102
104
118
120
114
116
124
122
PNP
PNP
116
118
120
128
114
130
108
Componente-B Oeste
106
126
CBP
200

FIG. 3

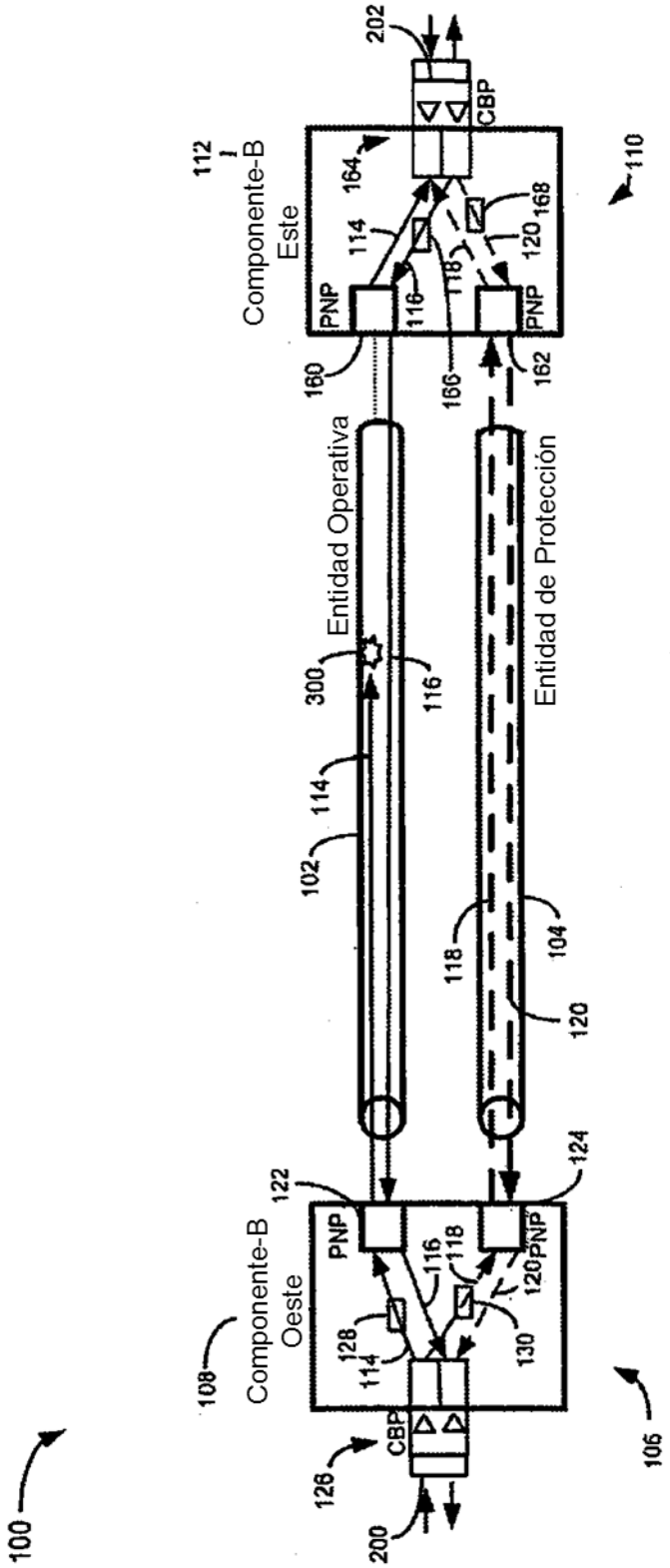

100
112
Componente-B
Este
110
202
CBP
164
114
120
168
118
116
PNP
PNP
160
166
162
Entidad Operativa
Entidad de Protección
300
116
114
102
118
104
120
122
124
108
Componente-B
Oeste
106
128
130
126
200

FIG. 4

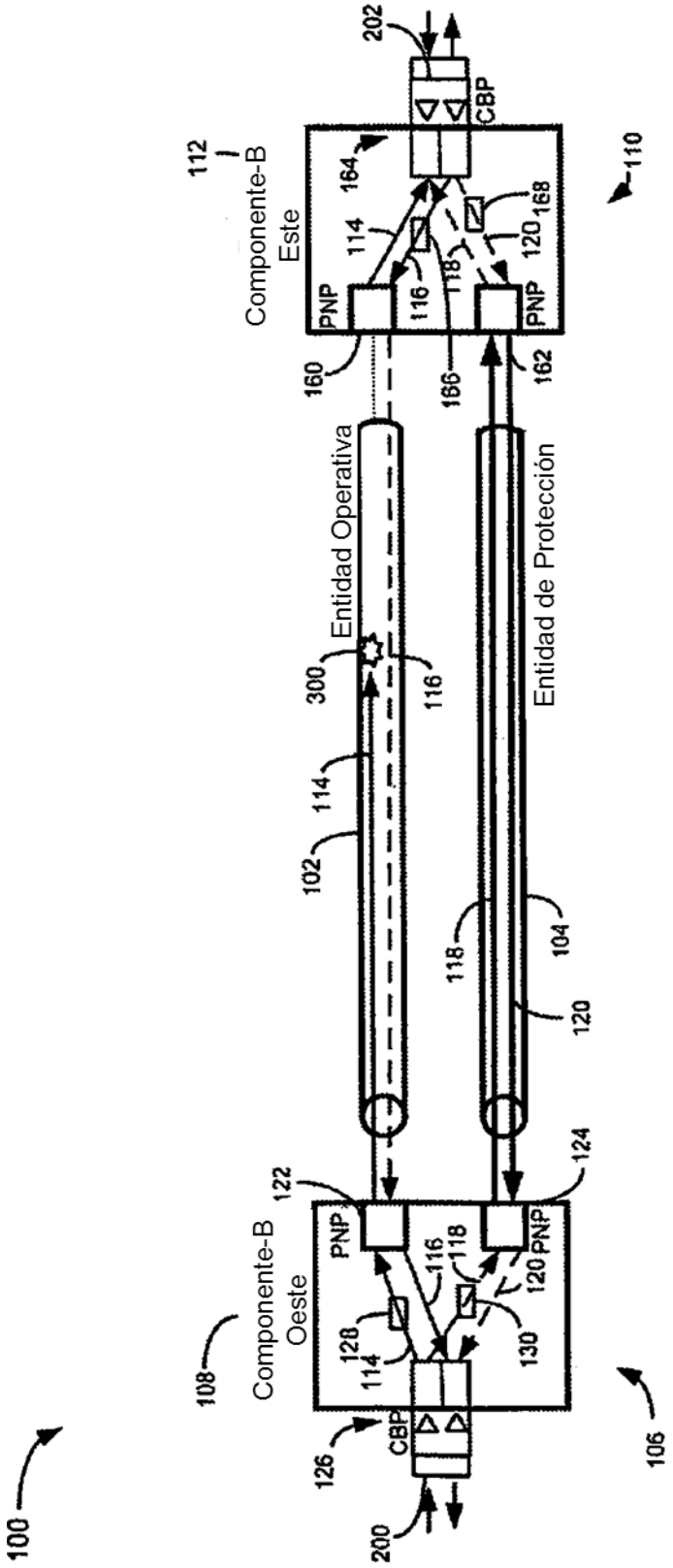
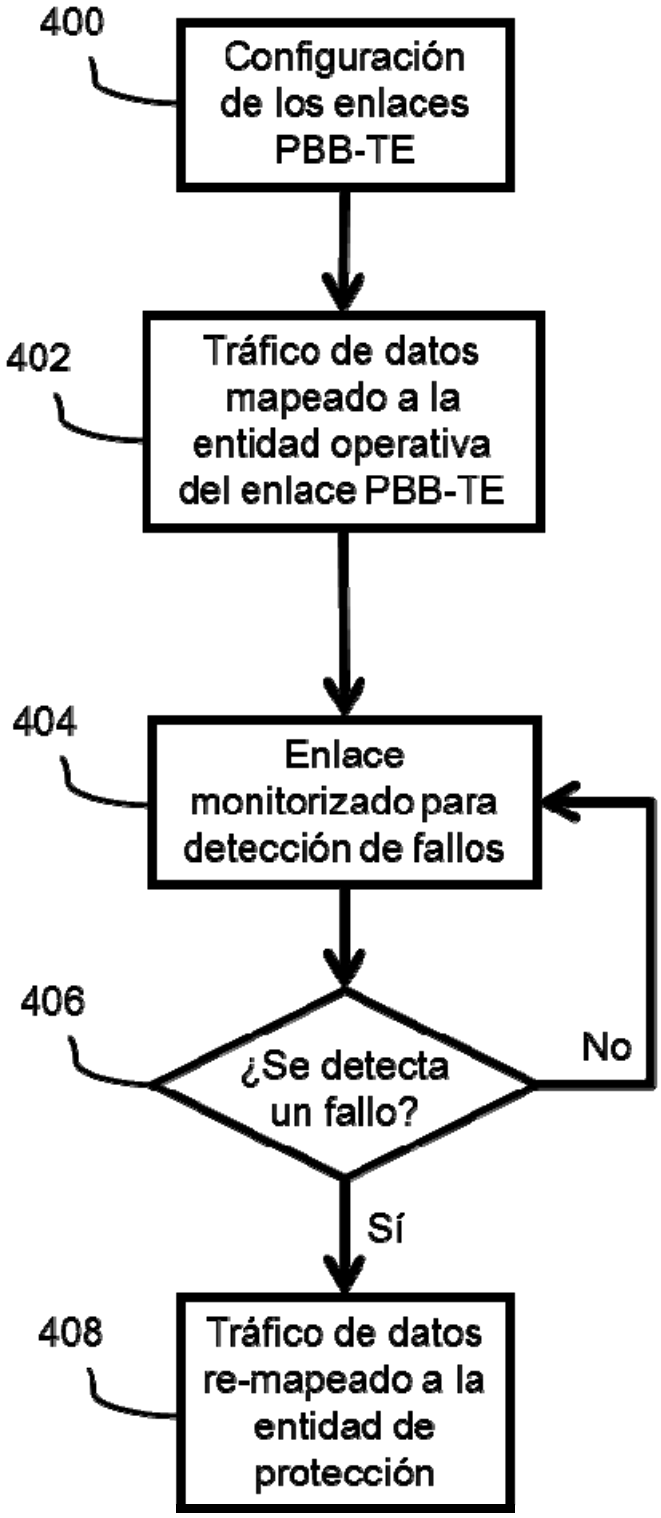

100
202
CBP
112
Componente-B
Este
110
164
114
168
120
118
116
PNP
PNP
160
166
162
Entidad Operativa
Entidad de Protección
300
116
114
102
118
104
120
122
124
PNP
PNP
116
118
120
108
Componente-B
Oeste
128
114
130
106
CBP
126
200

FIG. 5

FIG. 6


400
Configuración de los enlaces PBB-TE
402
Tráfico de datos mapeado a la entidad operativa del enlace PBB-TE
404
Enlace monitorizado para detección de fallos
406
¿Se detecta un fallo?
No
Sí
408
Tráfico de datos re-mapeado a la entidad de protección