(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 641 226**

(51) Int. CI.:

H04L 12/723 (2013.01)
H04L 12/24 (2006.01)
H04L 12/707 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **18.06.2014 PCT/CN2014/080218**

(87) Fecha y número de publicación internacional: **24.12.2014 WO14202004**

(96) Fecha de presentación y número de la solicitud europea: **18.06.2014 E 14813784 (7)**

(97) Fecha y número de publicación de la concesión europea: **09.08.2017 EP 2965475**

(54) Título: **Protección de ingreso de salto siguiente de trayectos conmutados por etiquetas**

(30) Prioridad:

18.06.2013 US 201361836514 P
17.06.2014 US 201414306855

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.11.2017

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian Longgang District , Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

CHEN, HUAIMO

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Protección de ingreso de salto siguiente de trayectos conmutados por etiquetas.

Campo de la invención

La presente invención se refiere al campo de las comunicaciones de redes y, en realizaciones particulares, a la protección de ingreso de salto siguiente de trayectos conmutados por etiquetas.

Antecedentes

En un sistema de trayecto de conmutación por etiquetas (LSP, por sus siglas en inglés) de ingeniería de tráfico (TE, por sus siglas en inglés) de multiprotocolo de conmutación por etiquetas (MPLS, por sus siglas en inglés) convencional, se puede emplear un segundo LSP como un LSP de seguridad para un LSP primario para proteger el LSP primario en caso de fallo del nodo de ingreso primario. El segundo LSP puede consumir recursos porque el segundo LSP puede usar un ancho de banda de red adicional que puede ser comparable con el ancho de banda reservado del primer LSP. Además, el segundo LSP puede reencaminar el tráfico de datos que provoca un retardo en la entrega de tráfico. Dicho retardo puede no ser aceptable en algunos sistemas (p.ej., para servicios en tiempo real como, por ejemplo, televisión de protocolo de internet (IP, por sus siglas en inglés)). Los sistemas convencionales también pueden detectar, de forma incorrecta, un fallo del nodo de ingreso primario para el LSP primario. Una detección de fallo incorrecta del nodo de ingreso primario puede resultar en que el nodo de ingreso primario del LSP primario y un nodo de ingreso de seguridad del segundo LSP entreguen el mismo tráfico de datos a un nodo de salto siguiente del nodo de ingreso primario. El tráfico duplicado que se entrega al nodo de salto siguiente del nodo de ingreso primario puede provocar interrupciones de servicio. Además, la ubicación de un nodo de ingreso de seguridad dentro de un segundo LSP puede ser limitada. Por ejemplo, un nodo de ingreso de seguridad puede no ser un salto siguiente de un nodo de ingreso primario a lo largo de un LSP primario.

Por ejemplo, el documento EP 2 301 205 A0 se refiere a la protección del ingreso y egreso de un trayecto conmutado por etiquetas.

Además, el documento US 2011/0199891A1 se refiere a un sistema y método para proteger el ingreso y egreso de un trayecto conmutado por etiquetas punto a multipunto.

El documento EP 2 540 041A0 se refiere a un sistema y método para computar un ingreso de seguridad de un trayecto conmutado por etiquetas punto a multipunto.

El documento US 7,626,925B1 se refiere a métodos para encontrar un reencaminamiento rápido MPLS del nodo de punto de fusión.

El documento XP015052690 se refiere a métodos de protección para RSVP-TE P2MP LSP.

Compendio

En un aspecto, la presente invención se refiere a un método para proveer protección de fallo de ingreso en un nodo de red, en una red conmutada por etiquetas, el método comprende:

recibir información de trayecto que identifica uno o más de otros nodos de red a lo largo de un trayecto primario conmutado por etiquetas, LSP;

crear un LSP de seguridad para los otros nodos de red;

generar una o más entradas de reenvío a lo largo del LSP de seguridad, en donde las entradas de reenvío a lo largo del LSP de seguridad comprenden un identificador de estado que indica un estado activo cuando el tráfico de datos se envía usando el LSP de seguridad y un estado inactivo cuando el tráfico de datos no se envía usando el LSP de seguridad;

comunicar el tráfico de datos de un primer trayecto de origen a uno o más de los otros nodos de red;

recibir el tráfico de datos de un segundo trayecto de origen en respuesta a un fallo de nodo de ingreso del primer trayecto de origen; y

enviar el tráfico de datos del segundo trayecto de origen usando las entradas de reenvío y el LSP de seguridad,

en donde el nodo de red es un miembro del LSP primario.

En otro aspecto, la presente invención se refiere a un aparato que comprende:

un receptor configurado para recibir un mensaje de protección de ingreso que identifica el aparato como un nodo de ingreso de seguridad e identifica uno o más nodos de red a lo largo de un trayecto primario conmutado por etiquetas, LSP, y para recibir el tráfico de datos de un segundo trayecto de origen en respuesta a un fallo de nodo de ingreso de un primer trayecto de origen;

un procesador acoplado a un dispositivo de memoria y al receptor, en donde el dispositivo de memoria comprende instrucciones ejecutables por ordenador almacenadas en un medio legible por ordenador no transitorio de modo que, cuando se ejecutan por el procesador, hacen que el procesador:

cree un LSP de seguridad; y

genere una tabla de reenvío que comprende una o más entradas de reenvío para los nodos de red a lo largo del LSP primario y una o más entradas de reenvío para los nodos de red a lo largo del LSP de seguridad, en donde las entradas de reenvío a lo largo del LSP de seguridad comprenden un identificador de estado que indica un estado activo cuando el tráfico de datos se transmite usando el LSP de seguridad y un estado inactivo cuando el tráfico de datos no se transmite usando el LSP de seguridad; y

un transmisor acoplado al procesador, en donde el transmisor se configura para enviar el tráfico de datos desde el segundo trayecto de origen usando las entradas de reenvío y el LSP de seguridad, y

en donde el aparato es un miembro del LSP primario.

Estas y otras características se comprenderán con mayor claridad a partir de la descripción detallada tomada en conjunto con los dibujos anexos y las reivindicaciones.

Breve descripción de los dibujos

Para una comprensión más completa de la presente descripción, a continuación se hace referencia a la siguiente descripción breve, tomada en relación con los dibujos anexos y la descripción detallada, en donde numerales de referencia iguales representan partes iguales.

La Figura 1 es un diagrama esquemático de una realización a modo de ejemplo de un sistema conmutado por etiquetas donde las realizaciones de la presente descripción pueden funcionar.

La Figura 2 es un diagrama esquemático de una realización a modo de ejemplo de un elemento de red.

La Figura 3 es un diagrama esquemático de una realización a modo de ejemplo de un sistema conmutado por etiquetas que emplea la protección de nodo de ingreso.

La Figura 4 es un diagrama esquemático de otra realización a modo de ejemplo de un sistema conmutado por etiquetas que emplea la protección de nodo de ingreso.

La Figura 5 es un diagrama esquemático de otra realización a modo de ejemplo de un sistema conmutado por etiquetas que emplea la protección de nodo de ingreso.

La Figura 6 es un diagrama esquemático de otra realización a modo de ejemplo de un sistema conmutado por etiquetas que emplea la protección de nodo de ingreso.

La Figura 7 es una realización a modo de ejemplo de un objeto de mensaje.

La Figura 8 es una realización a modo de ejemplo de un subobjeto de mensaje.

La Figura 9 es otra realización a modo de ejemplo de un subobjeto de mensaje.

La Figura 10 es otra realización a modo de ejemplo de un subobjeto de mensaje.

La Figura 11 es un diagrama de flujo de una realización a modo de ejemplo de un método de protección de nodo de ingreso.

Descripción detallada

Se debe comprender desde el comienzo que a pesar de que a continuación se provee una implementación ilustrativa de una o más realizaciones, los sistemas y/o métodos descritos pueden implementarse utilizando cualquier cantidad de técnicas, ya sean conocidas o existentes en la actualidad. De ningún modo la descripción estará limitada a las implementaciones ilustrativas, dibujos y técnicas ilustradas más abajo, incluidos los diseños e implementaciones a modo de ejemplo ilustradas y descritas en la presente memoria, pero se podrá modificar dentro del alcance de las reivindicaciones adjuntas junto con su total alcance de equivalentes.

En la presente memoria se describen varias realizaciones a modo de ejemplo para establecer un LSP de seguridad, detectar un fallo que implica un nodo de ingreso primario de un LSP, generar una o más entradas de reenvío para el LSP de seguridad, y controlar la entrega del tráfico de datos de un nodo de origen a uno o más nodos de salto siguiente del nodo de ingreso primario mediante un nodo de ingreso de seguridad y el LSP de seguridad. El tráfico de datos se puede entregar de una red y/o nodo de origen a uno o más nodos de salto siguiente del nodo de ingreso primario mediante el nodo de ingreso de seguridad y el LSP de seguridad. Una red, un nodo de origen y/o un nodo de ingreso de seguridad pueden detectar un fallo de un nodo de ingreso primario de un LSP primario y pueden reencaminar el tráfico de datos a los nodos de salto siguiente del nodo de ingreso primario mediante el nodo de ingreso de seguridad y un LSP de seguridad. El fallo del nodo de ingreso primario se puede determinar empleando uno o más enlaces de detección de fallo con el fin de reducir detecciones de fallo falsas positivas de un nodo de ingreso primario. Tras determinar que ha ocurrido un fallo de nodo de ingreso primario (p.ej., no un fallo de enlace), el nodo de ingreso de seguridad puede activar el LSP de seguridad y entregar el tráfico al nodo de salto siguiente del nodo de ingreso primario mediante el LSP de seguridad. El nodo de ingreso de seguridad puede evitar que el tráfico duplicado se entregue en respuesta a una detección falsa positiva de un nodo de ingreso primario. Algunos ejemplos de protección contra fallos que implican el nodo de ingreso primario de un MPLS TE LSP se describen en la Solicitud de Patente de Estados Unidos No. de Serie 12/683,968, titulada "*Protecting Ingress and Egress of a Label Switched Path*" y Solicitud de Estados Unidos No. de Serie 12/983,587, titulada "*System and Method for Protecting Ingress and Egress of a Point-To-Multipoint Label Switched Path*".

La Figura 1 es un diagrama esquemático de una realización a modo de ejemplo de un sistema conmutado por etiquetas 100, donde las realizaciones de la presente descripción pueden funcionar. El sistema conmutado por etiquetas 100 comprende múltiples nodos de origen 140 en comunicación de datos con múltiples nodos cliente 150 mediante una red conmutada por etiquetas 101 (p.ej., una red conmutada por paquetes) que comprende múltiples nodos de red. La red conmutada por etiquetas 101 se puede configurar para encaminar o conmutar el tráfico de datos (p.ej., paquetes de datos o tramas) a lo largo de trayectos que se establecen usando un protocolo de conmutación por etiquetas, por ejemplo, usando MPLS o multiprotocolo generalizado de conmutación por etiquetas (GMPLS, por sus siglas en inglés). De manera alternativa, los paquetes se pueden encaminar o conmutar mediante trayectos establecidos usando cualquier otro protocolo apropiado como apreciará una persona con experiencia ordinaria en la técnica tras estudiar la presente descripción. La red conmutada por etiquetas 101 se puede configurar para establecer múltiples LSP entre al menos algunos de los nodos de red y/o entre el nodo de origen 140 y al menos algunos de los nodos de red. Un LSP puede ser un LSP punto a punto (P2P, por sus siglas en inglés) o un LSP punto a multipunto (P2MP, por sus siglas en inglés) y se puede usar para transportar el tráfico de datos (p.ej., usando paquetes y etiquetas de paquetes para el encaminamiento).

Los múltiples nodos de red pueden ser múltiples nodos de egreso 121, 122 y múltiples nodos internos 130. Los nodos de egreso 121, 122 y nodos internos 130 pueden ser cualquier dispositivo o componente que admita el transporte del tráfico de datos (p.ej., paquetes de datos) a través de la red conmutada por etiquetas 101. Por ejemplo, los nodos de red pueden incluir conmutaciones, enrutadores y cualquier otro dispositivo de red apropiado para comunicar paquetes como apreciará una persona con experiencia ordinaria en la técnica tras estudiar la presente descripción, o combinaciones de ellos. Los nodos de red se pueden configurar para recibir datos de otros nodos de red, para determinar a qué nodos de red enviar los datos (p.ej., mediante circuitos lógicos o una tabla de reenvío) y/o para transmitir los datos a otros nodos de red. En algunas realizaciones a modo de ejemplo, al menos algunos de los nodos de red pueden ser enrutadores conmutados por etiquetas (LSR, por sus siglas en inglés) y se pueden configurar para modificar o actualizar las etiquetas de los paquetes transportados en la red conmutada por etiquetas 101. Además, al menos algunos de los nodos de red pueden ser enrutadores de borde de etiqueta (LER, por sus siglas en inglés) y se pueden configurar para insertar o eliminar las etiquetas de los paquetes transportados entre la red conmutada por etiquetas 101 y un nodo de origen 140 y/o un nodo cliente 150.

Un nodo de origen 140 y/o un nodo cliente 150 pueden ser una red o nodo de red que es externo o distinto de la red conmutada por etiquetas 101. De manera alternativa, un nodo de origen 140 y/o un nodo cliente 150 pueden ser una porción de y/o incorporarse a la red conmutada por etiquetas 101. La red conmutada por etiquetas 101 comprende un primer nodo de ingreso (p.ej., un nodo de ingreso primario) 111, un segundo nodo de ingreso (p.ej., un nodo de ingreso de seguridad) 112, múltiples nodos internos 130, múltiples primeros nodos de egreso (p.ej., un nodo de egreso primario) 121 y múltiples segundos nodos de egreso (p.ej., un nodo de egreso de seguridad) 122. Aunque la red conmutada por etiquetas 101 se ilustra como una red que comprende un primer nodo de ingreso 111, un segundo nodo de ingreso 112, múltiples nodos internos 130, múltiples primeros nodos de egreso 121 y múltiples segundos nodos de egreso 122, en una o más realizaciones a modo de ejemplo, cualquier otra configuración apropiada y/o combinaciones de ellos se puede incorporar, de forma adicional o alternativa, a la red conmutada por etiquetas 101 como apreciará una persona con experiencia ordinaria en la técnica tras estudiar la presente descripción.

La red conmutada por etiquetas 101 se puede configurar de modo que múltiples LSP (p.ej., LSP P2P y/o LSP P2MP) se pueden establecer entre los nodos de red y/o entre las redes y al menos algunos de los nodos de red. La red conmutada por etiquetas 101 puede comprender un LSP primario (p.ej., un LSP P2P) configurado para transportar el tráfico de datos de un nodo de origen 140 a un nodo cliente 150. El LSP primario puede comprender el primer nodo

de ingreso 111, uno o más nodos internos 130 y un primer nodo de egreso 121. La red conmutada por etiquetas 101 comprende además un LSP de seguridad (p.ej., un LSP P2P de seguridad). El LSP de seguridad puede comprender uno o más LSP P2P de desvío y/o LSP P2MP.

El LSP de seguridad puede ser un túnel de desvío P2P. El LSP de seguridad se puede crear computando un trayecto del segundo nodo de ingreso 112 a uno o más nodos de salto siguiente del primer nodo de ingreso 111, estableciendo el LSP de seguridad a lo largo del trayecto computado, enviando un mensaje de trayecto (TRAYECTO) al segundo nodo de ingreso 112 que comprende un objeto de mensaje de protección de fallo de ingreso, recibiendo un mensaje de reserva (RESV) en respuesta al mensaje TRAYECTO y creando uno o más estados de reenvío (p.ej., tabla de reenvío) para el LSP de seguridad. El objeto de mensaje de protección de fallo de ingreso puede ser como se describe en la Figura 7. En una realización a modo de ejemplo, el LSP de seguridad se puede establecer como se describe en la Solicitud de Patente de Estados Unidos No. de Serie 12/683,968, titulada "*Protecting Ingress and Egress of a Label Switched Path*". Los mensajes TRAYECTO y RESV pueden ser similares a los mensajes TRAYECTO y RESV definidos por la Solicitud de Comentarios (RFC, por sus siglas en inglés) 6510 del Grupo de Trabajo de Ingeniería de Internet (IETF, por sus siglas en inglés).

La Figura 2 es un diagrama esquemático de una realización a modo de ejemplo de un elemento de red 200 que se puede usar para transportar y procesar el tráfico a través de al menos una porción de una red 100 que se muestra en la Figura 1. Al menos algunas de las características/métodos descritos en la descripción se pueden implementar en el elemento de red 200. Por ejemplo, las características/métodos de la descripción se pueden implementar en hardware, firmware y/o software instalado para ejecutarse en hardware. El elemento de red 200 puede ser cualquier dispositivo (p.ej., un punto de acceso, una estación de punto de acceso, un servidor, un cliente, un equipo de usuario, un dispositivo de comunicaciones móviles, etc.) que transporta datos a través de una red, sistema y/o dominio. Además, los términos "elemento" de red, "nodo" de red, "componente" de red, "módulo" de red y/o términos similares se pueden usar, de forma intercambiable, para describir, en general, un dispositivo de red y no tienen un significado particular o especial a menos que se establezca y/o indique específicamente lo contrario en la descripción. En una realización a modo de ejemplo, el elemento de red 200 puede ser un aparato configurado para implementar la protección de fallo de ingreso. Por ejemplo, el elemento de red 200 puede encontrarse en o incorporarse a un segundo nodo de ingreso 112 o nodo interno 130 según se describe en la Figura 1.

El elemento de red 200 puede comprender uno más puertos descendentes 210 acoplados a un transceptor (Tx/Rx) 220, que pueden ser transmisores, receptores o combinaciones de ellos. El Tx/Rx 220 puede transmitir y/o recibir tramas de otros nodos de red mediante los puertos descendentes 210. De manera similar, el elemento de red 200 puede comprender otro Tx/Rx 220 acoplado a múltiples puertos ascendentes 240, en donde el Tx/Rx 220 puede transmitir y/o recibir tramas de otros nodos mediante los puertos ascendentes 240. Los puertos descendentes 210 y/o puertos ascendentes 240 pueden incluir componentes de transmisión y/o recepción eléctricos y/u ópticos. En otra realización a modo de ejemplo, el elemento de red 200 puede comprender una o más antenas acopladas al Tx/Rx 220. El Tx/Rx 220 puede transmitir y/o recibir datos (p.ej., paquetes) de otros elementos de red de forma inalámbrica mediante una o más antenas.

Se puede acoplar un procesador 230 al Tx/Rx 220 y se puede configurar para procesar las tramas y/o determinar los nodos a los cuales enviar (p.ej., transmitir) los paquetes. En una realización a modo de ejemplo, el procesador 230 puede comprender uno o más procesadores de núcleos múltiples y/o módulos de memoria 250, que pueden funcionar como almacenes de datos, búferes, etc. El procesador 230 puede implementarse como un procesador general o puede ser parte de uno o más circuitos integrados de aplicación específica (ASIC, por sus siglas en inglés), disposiciones de puertos programables en campo (FPGA, por sus siglas en inglés) y/o procesadores de señales digitales (DSP, por sus siglas en inglés). Aunque se ilustra como un solo procesador, el procesador 230 no se encuentra limitado y puede comprender múltiples procesadores. El procesador 230 se puede configurar para generar un LSP de seguridad, generar una o más entradas de reenvío para el LSP de seguridad, detectar un fallo de un nodo de ingreso primario, activar las entradas de reenvío y enviar el tráfico de datos usando el LSP de seguridad y las entradas de reenvío.

La Figura 2 ilustra que un módulo de memoria 250 se puede acoplar al procesador 230 y puede ser un medio no transitorio configurado para almacenar varios tipos de datos. El módulo de memoria 250 puede comprender dispositivos de memoria que incluyen almacenamiento secundario, memoria de solo lectura (ROM, por sus siglas en inglés) y memoria de acceso aleatorio (RAM, por sus siglas en inglés). El almacenamiento secundario se compone, normalmente, de una o más unidades de disco, unidades de disco óptico, unidades de estado sólido (SSD, por sus siglas en inglés) y/o unidades de cinta y se usa para el almacenamiento permanente de datos y como un dispositivo de almacenamiento de desbordamiento si la RAM no es lo suficientemente grande para contener todos los datos de trabajo. El almacenamiento secundario se puede usar para almacenar programas que se cargan en la RAM cuando dichos programas se seleccionan para su ejecución. La ROM se usa para almacenar instrucciones y, quizás, datos que se leen durante la ejecución del programa. La ROM es un dispositivo de memoria permanente que tiene, normalmente, una pequeña capacidad de memoria respecto a la mayor capacidad de memoria del almacenamiento secundario. La RAM se usa para almacenar datos no permanentes y, quizás, para almacenar instrucciones. El acceso tanto a la ROM como a la RAM es, en general, más rápido que al almacenamiento secundario.

El módulo de memoria 250 se puede usar para alojar las instrucciones para llevar a cabo las diferentes realizaciones a modo de ejemplo descritas en la presente memoria. En una realización a modo de ejemplo, el módulo de memoria 250 puede comprender un módulo de protección de ingreso 260 que se puede implementar en el procesador 230. En una realización a modo de ejemplo, el módulo de protección de ingreso 260 se puede implementar en un nodo de ingreso de seguridad (p.ej., un segundo nodo de ingreso 112 o un nodo interno 130 según se describe en la Figura 1) para implementar un esquema de protección de nodo de ingreso como, por ejemplo, el método 1100 según se describe en la Figura 11. Por ejemplo, el nodo de ingreso de seguridad puede usar el módulo de protección de ingreso 260 para generar una o más entradas de reenvío para otros nodos de red de un LSP primario usando un LSP de seguridad y puede enviar el tráfico de datos a los otros nodos de red usando el LSP de seguridad cuando ocurre un fallo de nodo de ingreso primario.

Se entiende que, mediante la programación y/o carga de instrucciones ejecutables en el elemento de red 200, se modifica al menos uno del procesador 230, la memoria caché y el almacenamiento a largo plazo, transformando el elemento de red 200 en parte en una máquina o aparato particular, por ejemplo, una arquitectura de reenvío de núcleos múltiples, quedando la funcionalidad novedosa expuesta en la presente descripción. Es fundamental para las técnicas de ingeniería de software e ingeniería eléctrica que la funcionalidad que se puede implementar cargando software ejecutable en un ordenador se pueda convertir en una implementación de hardware mediante normas de diseño conocidas en la técnica. Las decisiones entre implementar un concepto en software versus hardware normalmente dependen de las consideraciones de estabilidad del diseño y cantidad de unidades que se producirán, más que de cualquier problema relacionado con la conversión del dominio de software al dominio de hardware. En general, un diseño que está aún sujeto a cambios frecuentes se puede preferir para implementarse en software, debido a que reestructurar una implementación de hardware es más costoso que reestructurar un diseño de software. En general, se puede preferir implementar en hardware un diseño que sea estable y que se producirá en grandes volúmenes (p.ej., en un ASIC) puesto que para grandes ejecuciones de producción la implementación de hardware puede ser menos costosa que las implementaciones de software. Con frecuencia, un diseño puede desarrollarse y probarse en forma de software y posteriormente transformarse, mediante normas de diseño conocidas en la técnica, en una implementación de hardware equivalente en un ASIC que cablea las instrucciones del software. De la misma forma que una máquina controlada por un nuevo ASIC es una máquina o aparato particular, un ordenador que se ha programado y/o cargado con instrucciones ejecutables puede verse como una máquina o aparato particular.

Cualquier procesamiento de la presente descripción se puede implementar haciendo que un procesador (p.ej., un procesador de núcleos múltiples con propósito general) ejecute un programa de ordenador. En el presente caso, un producto de programa de ordenador se puede proveer a un ordenador o a un dispositivo de red usando cualquier tipo de medio legible por ordenador no transitorio. El producto de programa de ordenador se puede almacenar en un medio legible por ordenador no transitorio en el ordenador o dispositivo de red. Los medios legibles por ordenador no transitorios incluyen cualquier tipo de medios de almacenamiento tangibles. Ejemplos de medios legibles por ordenador no transitorios incluyen medios de almacenamiento magnético (como, por ejemplo, discos flexibles, cintas magnéticas, unidades de disco duro, etc.), medios de almacenamiento magnético óptico (p.ej., discos magneto-ópticos), disco compacto con memoria de solo lectura (CD-ROM, por sus siglas en inglés), disco compacto grabable (CD-R, por sus siglas en inglés), disco compacto reescribible (CD-R/W, por sus siglas en inglés), disco versátil digital (DVD), disco Blu-ray (marca registrada) (BD) y memorias con semiconductores (como, por ejemplo, ROM con máscara, ROM programable (PROM), PROM borrable), ROM flash y RAM). El producto de programa de ordenador se puede proveer también a un ordenador o a un dispositivo de red usando cualquier tipo de medio legible por ordenador transitorio. Ejemplos de medios legibles por ordenador transitorios incluyen señales eléctricas, señales ópticas y ondas electromagnéticas. Los medios legibles por ordenador transitorios pueden proveer el programa a un ordenador mediante una línea de comunicación cableada (p.ej., cables eléctricos y fibras ópticas) o una línea de comunicación inalámbrica.

La Figura 3 es un diagrama esquemático de una realización a modo de ejemplo de un sistema conmutado por etiquetas 300 que emplea la protección de nodo de ingreso. El sistema conmutado por etiquetas 300 comprende una red conmutada por etiquetas 302 que comprende múltiples nodos de red 306A-306L. En particular, un nodo de ingreso primario 306A, un nodo de ingreso de seguridad 306B, múltiples nodos internos 306C-306K, y un nodo de egreso 306L. El nodo de ingreso primario 306A puede ser sustancialmente similar al primer nodo de ingreso 111 descrito en la Figura 1, el nodo de ingreso de seguridad 306B puede ser sustancialmente similar al segundo nodo de ingreso 112 descrito en la Figura 1, los múltiples nodos internos 306C-306K pueden ser sustancialmente similares a los nodos internos 130 descritos en la Figura 1, y el nodo de egreso 306L puede ser sustancialmente similar al primer nodo de egreso 121 o al segundo nodo de egreso 122 descritos en la Figura 1. El nodo de ingreso de seguridad 306B puede ser un nodo de ingreso o un nodo interno. Aunque la red conmutada por etiquetas 302 se ilustra como una red que comprende el nodo de ingreso primario 306A, el nodo de ingreso de seguridad 306B, los múltiples nodos internos 306C-306K, y el nodo de egreso 306L, en una o más realizaciones a modo de ejemplo, cualquier otra configuración apropiada y/o combinaciones de ellas se puede incorporar, de forma adicional o alternativa, a la red conmutada por etiquetas 302 como apreciará una persona con experiencia ordinaria en la técnica tras estudiar la presente descripción. La red conmutada por etiquetas 302 puede estar en comunicación de

datos con un nodo de origen 304 y un nodo cliente 308. El nodo de origen 304 y/o el nodo cliente 308 pueden ser una red o un nodo de red que es externo o distinto de la red conmutada por etiquetas 302. De manera alternativa, el nodo de origen 304 y/o el nodo cliente 308 pueden ser una porción de y/o incorporarse a la red conmutada por etiquetas 302.

El sistema conmutado por etiquetas 300 se puede configurar para emplear uno o más LSP (p.ej., uno o más LSP P2P y/o LSP P2MP) para comunicar el tráfico de datos del nodo de origen 304 al nodo cliente 308. En la Figura 3, la red conmutada por etiquetas 302 se puede configurar para emplear un LSP primario P2P. El LSP primario puede comprender el nodo de ingreso primario 306A, el nodo de ingreso de seguridad 306B, los nodos internos 306D y 306G y el nodo de egreso 306L. El LSP primario se muestra usando líneas continuas en forma de flecha en la Figura 3. El sistema conmutado por etiquetas 300 puede además comprender uno o más LSP de seguridad configurados para proteger el nodo de ingreso primario 306A del LSP primario y para reenviar el tráfico de datos del nodo de origen 304 al nodo cliente 308 cuando el nodo de ingreso primario 306A del LSP primario falla. Un LSP de seguridad puede comprender uno o más LSP P2P y/o LSP P2MP. El LSP de seguridad puede comprender el nodo de ingreso de seguridad 306B y uno o más nodos de salto siguiente para el nodo de ingreso primario 306A. Por ejemplo, el LSP de seguridad puede comprender el nodo de ingreso de seguridad 306B y el nodo interno 306D.

En una realización a modo de ejemplo, el nodo de origen 304 se puede configurar para comunicar, simultáneamente, el tráfico de datos al nodo de ingreso primario 306A y al nodo de ingreso de seguridad 306B. En otra realización a modo de ejemplo, el nodo de origen 304 se puede configurar para enviar el tráfico de datos al nodo de ingreso primario 306A durante el funcionamiento típico y puede conmutar el tráfico de datos del nodo de ingreso primario 306A al nodo de ingreso de seguridad 306B cuando se detecta un fallo en el nodo de ingreso primario 306A. El nodo de ingreso primario 306A se puede configurar como un nodo de ingreso primario para un LSP (p.ej., un LSP primario). El nodo de ingreso primario 306A se puede configurar para comunicar el tráfico de datos del nodo de origen 304 al nodo cliente 308 usando uno o más LSP. El nodo de ingreso primario 306A se puede configurar también para comunicarse con el nodo de ingreso de seguridad 306B para señalizar un LSP de seguridad. El nodo de ingreso primario 306A se puede configurar para comunicar un objeto de mensaje de protección de ingreso (p.ej., un objeto de mensaje como se describe en la Figura 7) al nodo de ingreso de seguridad 306B para establecer uno o más LSP de seguridad.

En una realización a modo de ejemplo, el nodo de ingreso de seguridad 306B se puede predeterminar por un operador de red. De manera alternativa, el nodo de ingreso de seguridad 306B se puede configurar para seleccionarse de forma automática (p.ej., mediante el uso de un elemento de cálculo de trayecto (PCE, por sus siglas en inglés)) según la información de topología de red. Por ejemplo, un PCE se puede configurar para informar a otros nodos de red sobre el nodo de ingreso de seguridad 306B seleccionado. En la Figura 3, el nodo de ingreso de seguridad 306B puede ser un nodo de salto siguiente del nodo de ingreso primario 306A y puede ser un miembro del LSP primario. El nodo de ingreso de seguridad 306B se puede configurar para establecer uno o más LSP de seguridad para uno o más nodos de salto siguiente del nodo de ingreso primario 306A y para entregar el tráfico de datos al nodo cliente 308 cuando el nodo de ingreso primario 306A falla.

En respuesta a la recepción de un objeto de mensaje del nodo de ingreso primario 306A, el nodo de ingreso de seguridad 306B se puede configurar para generar una o más entradas de reenvío para un LSP primario y/o una o más entradas de reenvío para un LSP de seguridad en una tabla de reenvío. La tabla de reenvío se puede almacenar y mantener dentro del nodo de ingreso de seguridad 306B. El nodo de ingreso de seguridad 306B se puede configurar para recibir el tráfico de datos del nodo de origen 304 y para comunicar el tráfico de datos a uno o más nodos de red (p.ej., nodos de salto siguiente del nodo de ingreso primario 306A) a lo largo de uno o más LSP primarios usando uno o más LSP de seguridad. En una realización a modo de ejemplo, el nodo de ingreso de seguridad 306B se puede configurar para extraer el tráfico de datos del nodo de origen 304 cuando no se ha detectado un fallo en el nodo de ingreso primario 306A.

La Tabla 1 es una realización a modo de ejemplo de una tabla de reenvío que comprende una entrada de reenvío para un LSP primario y una entrada de reenvío para un LSP de seguridad. La tabla de reenvío se puede configurar para mantener múltiples etiquetas entrantes, múltiples etiquetas salientes, múltiples interfaces para identificadores de salto siguiente, un identificador de estado, cualquier otra información de encaminamiento apropiada como apreciará una persona con experiencia ordinaria en la técnica tras estudiar la presente descripción, o combinaciones de ellos. Las etiquetas entrantes pueden indicar el emisor de un paquete de datos. Una Clase de Equivalencia de Reenvío (FEC, por sus siglas en inglés) puede indicar que el tráfico proviene de un nodo de origen (p.ej., nodo de origen 140 como se describe en la Figura 1) y que se enviará por el LSP. Las etiquetas salientes se pueden asignar por un nodo de red de salto siguiente y pueden indicar un salto siguiente para un paquete de datos. La interfaz para los identificadores de salto siguiente puede identificar una interfaz (p.ej., un puerto) asociada al salto siguiente correspondiente a una etiqueta saliente. El identificador de estado puede indicar si una entrada de reenvío se encuentra en un estado activo o en un estado inactivo. Un estado activo puede indicar que la entrada de reenvío se puede usar para reenviar el tráfico de datos. Un estado inactivo puede indicar que la entrada de reenvío no se puede usar para reenviar el tráfico de datos.

Tabla 1 - Una realización a modo de ejemplo de una tabla de reenvío

Entrada Etiqueta/FEC	Salida Etiqueta	Interfaz para salto siguiente	Estado
E1	E2	a Nodo 306D	Activo
FEC1	E2	a Nodo 306D	Inactivo

La red conmutada por etiquetas 302 se puede configurar para emplear un LSP P2P para comunicar el tráfico de datos del nodo de origen 304 al nodo cliente 308. El nodo de ingreso de seguridad 306B puede ser un nodo de salto siguiente del nodo de ingreso primario 306A a lo largo del LSP primario. En una realización a modo de ejemplo, el nodo de ingreso de seguridad 306B se puede configurar, normalmente, para recibir el tráfico de datos de un primer trayecto de origen del nodo de ingreso primario 306A con una etiqueta entrante E1 y enviar el tráfico de datos usando la entrada de reenvío para el LSP primario. El nodo de ingreso de seguridad 306B puede enviar el tráfico de datos al salto siguiente usando una etiqueta saliente E2 mediante la interfaz para el salto siguiente correspondiente a la etiqueta saliente. Cuando el nodo de origen 304 y/o el nodo de ingreso de seguridad 306B detectan un fallo del nodo de ingreso primario 306A, el estado de la entrada de reenvío para el LSP primario puede cambiar de activo a inactivo y el estado de la entrada de reenvío para el LSP de seguridad puede cambiar de inactivo a activo. En una realización a modo de ejemplo, el estado de la entrada de reenvío para el LSP primario y el estado de la entrada de reenvío para el LSP de seguridad pueden cambiar simultáneamente. Luego de detectar un fallo del nodo de ingreso primario 306A, el nodo de ingreso de seguridad 306B se puede configurar para recibir datos de un segundo trayecto de origen del nodo de origen 304 y para enviar el tráfico de datos al nodo interno 306D mediante el uso de la entrada de reenvío para el LSP de seguridad.

El sistema conmutado por etiquetas 300 puede comprender uno o más enlaces de detección de fallo. Los enlaces de detección de fallo usados por el sistema conmutado por etiquetas 300 pueden incluir una sesión de detección de fallo bidireccional (BFD, por sus siglas en inglés), un LSP P2P, y/o cualquier otro enlace de detección de fallo apropiado. El enlace de detección de fallo puede comprender un enlace entre dos nodos de red o un enlace de múltiples saltos entre múltiples nodos de red. En una realización a modo de ejemplo, el enlace de detección de fallo puede comprender una sesión BFD 350 entre el nodo de ingreso primario 306A y el nodo de ingreso de seguridad 306B, una sesión BFD 352 entre el nodo de origen 304 y el nodo de ingreso primario 306A y/o una sesión BFD 354 entre el nodo de origen 304 y el nodo de ingreso de seguridad 306B mediante el nodo de ingreso primario 306A.

El nodo de ingreso de seguridad 306B se puede configurar para detectar un fallo que implica el nodo de ingreso primario 306A mediante el uso de uno o más de los enlaces de detección de fallo (p.ej., sesión BFD 350 y/o sesión BFD 354). Como tal, el nodo de ingreso de seguridad 306B se puede configurar en un modo de detección de seguridad de origen (p.ej., la detección de fallo se lleva a cabo en conjunto con el nodo de origen 304) o un modo de detección de seguridad (p.ej., la detección de fallo se lleva a cabo por el nodo de ingreso de seguridad 306B). Cuando el nodo de ingreso de seguridad 306B detecta un fallo en el nodo de ingreso primario 306A, el nodo de ingreso de seguridad 306B se puede configurar para recibir el tráfico de datos destinado al LSP primario del nodo de origen 304. Después de recibir el tráfico de datos, el nodo de ingreso de seguridad 306B puede importar el tráfico de datos al LSP de seguridad y/o a los nodos de salto siguiente del nodo de ingreso primario 306A, de modo que el tráfico de datos se fusiona con el LSP primario. En una realización a modo de ejemplo, el nodo de ingreso de seguridad 306B puede detectar un fallo de conexión entre el nodo de ingreso de seguridad 306B y el nodo de ingreso primario 306A determinando que la sesión BFD 350 está fuera de servicio (p.ej., no está funcionando). En otra realización a modo de ejemplo donde el enlace de detección de fallo usa tanto la sesión BFD 350 como la sesión BFD 354, el nodo de ingreso de seguridad 306B se puede configurar para detectar un fallo de conexión entre el nodo de ingreso primario 306A y el nodo de origen 304 determinando que la sesión BFD 354 está fuera de servicio y que la sesión BFD 350 está en servicio (p.ej., funcionando). Además, el nodo de ingreso de seguridad 306B se puede configurar para detectar un fallo en el nodo de ingreso primario 306A determinando que la sesión BFD 354 y la sesión BFD 350 se encuentran ambas fuera de servicio. En respuesta a la detección de un fallo de conexión entre el nodo de ingreso primario 306A y el nodo de origen 304 o la detección de un fallo en el nodo de ingreso primario 306A, el nodo de ingreso de seguridad 306B se puede configurar para recibir el tráfico de datos para el LSP primario del nodo de origen 304 y para importar el tráfico de datos a un LSP de seguridad y/o los nodos de salto siguiente del nodo de ingreso primario 306A de modo que el tráfico de datos se fusiona con el LSP primario.

El nodo de origen 304 se puede configurar para detectar un fallo que implica el nodo de ingreso primario 306A mediante el uso de uno o más de los enlaces de detección de fallo (p.ej., sesión BFD 352 y/o sesión BFD 354). Como tal, el nodo de origen 304 se puede configurar en un modo de detección de origen (p.ej., la detección de fallo se lleva a cabo por el nodo de origen) o un modo de detección de seguridad de origen. El nodo de origen 304 se puede configurar para detectar un fallo que implica el nodo de ingreso primario 306A determinando que la sesión

BFD 352 se encuentra fuera de servicio. En respuesta a la detección de un fallo que implica el nodo de ingreso primario 306A, el nodo de origen 304 se puede configurar para enviar el tráfico destinado para el LSP primario al nodo de ingreso de seguridad 306B y para detener el envío de tráfico al nodo de ingreso primario 306A. Como tal, el nodo de origen 304 conmuta el flujo de tráfico del nodo de ingreso primario 306A al nodo de ingreso de seguridad 306B cuando la sesión BFD 352 se encuentra fuera de servicio.

La Figura 4 es un diagrama esquemático de otra realización a modo de ejemplo de un sistema conmutado por etiquetas 400 que emplea la protección de nodo de ingreso. El sistema conmutado por etiquetas 400 comprende una red conmutada por etiquetas 402 que comprende múltiples nodos de red 406A-406N. En particular, un nodo de ingreso primario 406A, un nodo de ingreso de seguridad 406B, múltiples nodos internos 406C-406J y nodos de egreso 406K-406N. El nodo de ingreso primario 406A puede ser sustancialmente similar al primer nodo de ingreso 111 descrito en la Figura 1, el nodo de ingreso de seguridad 406B puede ser sustancialmente similar al segundo nodo de ingreso 112 descrito en la Figura 1, los múltiples nodos internos 406C-406J pueden ser sustancialmente similares a los nodos internos 130 descritos en la Figura 1, y los nodos de egreso 406K-406N pueden ser sustancialmente similares al primer nodo de egreso 121 o al segundo nodo de egreso 122 descritos en la Figura 1.

La red conmutada por etiquetas 402 se puede configurar para emplear uno o más LSP para comunicar el tráfico de datos del nodo de origen 404 a los nodos cliente 408A y 408B y/o a otros nodos cliente conectados a los nodos de egreso 406M y 406N (no se muestran en la Figura 4). El único o más LSP pueden ser como se describe en la Figura 1. En la Figura 4, la red conmutada por etiquetas 402 se puede configurar para emplear un LSP primario P2MP que comprende un primer subLSP primario, un segundo subLSP primario, un tercer subLSP primario y un cuarto subLSP. El primer subLSP primario puede comprender el nodo de ingreso primario 406A, nodos internos 406D-406F y el nodo de egreso 406K. El segundo subLSP primario puede comprender el nodo de ingreso primario 406A, el nodo de ingreso de seguridad 406B, el nodo interno 406H y el nodo de egreso 406L. El tercer subLSP primario puede comprender el nodo de ingreso primario 406A y el nodo de egreso 406M. El cuarto subLSP primario puede comprender el nodo de ingreso primario 406A, el nodo de ingreso de seguridad 406B, el nodo interno 406I y el nodo de egreso 406N. Los subLSP primarios se muestran usando líneas continuas en forma de flecha en la Figura 4. La red conmutada por etiquetas 402 además comprende uno o más LSP de seguridad configurados para proteger el nodo de ingreso primario 406A de los LSP primarios y para reenviar el tráfico de datos del nodo de origen 404 a los nodos cliente 408A y 408B y/u otros nodos cliente (no se muestran en la Figura 4) cuando el nodo de ingreso primario 406A de los LSP primarios falla. Los LSP de seguridad pueden comprender el nodo de ingreso de seguridad 406B, los nodos de salto siguiente del nodo de ingreso de seguridad 406B y uno o más nodos de salto siguiente para el nodo de ingreso primario 406A diferentes del nodo de ingreso de seguridad 406B.

El nodo de origen 404, el nodo de ingreso primario 406A y/o el nodo de ingreso de seguridad 406B se pueden configurar de forma sustancialmente similar al nodo de origen 304, nodo de ingreso primario 306A y nodo de ingreso de seguridad 306B según se describe en la Figura 3, respectivamente. El sistema conmutado por etiquetas 400 puede comprender una o más sesiones BFD para detectar un fallo de nodo de ingreso primario según se describe en la Figura 3. El nodo de ingreso de seguridad 406B se puede configurar para crear un LSP de seguridad y/o para generar una o más entradas de reenvío para un LSP primario y/o una o más entradas de reenvío para un LSP de seguridad en una tabla de reenvío en respuesta a la recepción de un objeto de mensaje (p.ej., un objeto de mensaje según se describe en la Figura 7) del nodo de ingreso primario 406A. El LSP de seguridad puede ser del nodo de ingreso de seguridad 406B a un primer conjunto de nodos y un segundo conjunto de nodos. El primer conjunto de nodos puede comprender los nodos de salto siguiente (p.ej., nodos 406H y 406I) del nodo de ingreso de seguridad 406B. El segundo conjunto de nodos puede comprender los nodos de salto siguiente (p.ej., nodos 406M y 406D) del nodo de ingreso primario 406A diferente del nodo de ingreso de seguridad 406B. En una realización a modo de ejemplo, los subLSP del nodo de ingreso de seguridad 406B al primer conjunto de nodos pueden no señalizarse y las entradas de reenvío para los subLSP se pueden crear usando la información del LSP primario cuando se crea el LSP de seguridad. Por ejemplo, una o más etiquetas se pueden asignar por los nodos para el LSP primario. Los subLSP del nodo de ingreso de seguridad 406B al segundo conjunto de nodos pueden señalizarse y las entradas de reenvío para los subLSP se pueden crear según la señalización. La Tabla 2 es una realización a modo de ejemplo de una tabla de reenvío que comprende múltiples entradas de reenvío para un LSP primario y múltiples entradas de reenvío para un LSP de seguridad. Las múltiples entradas de reenvío para el LSP de seguridad pueden comprender una o más entradas de reenvío para los nodos de salto siguiente del nodo de ingreso de seguridad 406B y/o una o más entradas de reenvío para los nodos de salto siguiente del nodo de ingreso primario 406A. La tabla de reenvío se puede configurar de forma sustancialmente similar a la tabla de reenvío según se describe en la Figura 3.

Tabla 2 - Una realización a modo de ejemplo de una tabla de reenvío

Entrada Etiqueta/FEC	Salida Etiqueta	Interfaz para salto siguiente	Estado
E3	E7	a Nodo 406H	Activo
	E9	a Nodo 406I	
FEC1	E7	a Nodo 406H	Inactivo
	E9	a Nodo 406I	
FEC1	E10	a Nodo 406M	Inactivo
	E11	a Nodo 406D	

La red conmutada por etiquetas 402 se puede configurar para emplear un LSP P2MP para comunicar el tráfico de datos del nodo de origen 404 a los nodos cliente 408A y 408B y/o a otros nodos cliente (no se muestran en la Figura 4). El nodo de ingreso de seguridad 406B puede ser un nodo de salto siguiente del nodo de ingreso primario 406A a lo largo del LSP primario. En un funcionamiento típico, el nodo de ingreso de seguridad 406B se puede configurar para recibir el tráfico de datos de un primer trayecto de origen del nodo de ingreso primario 406A con una etiqueta entrante E3 y para enviar el tráfico de datos usando las entradas de reenvío para el LSP primario (p.ej., LSP P2MP). El nodo de ingreso de seguridad 406B puede enviar el tráfico de datos a uno o más saltos siguientes con etiquetas salientes asociadas a los nodos de salto siguiente. El nodo de ingreso de seguridad 406B puede enviar el tráfico de datos al nodo interno 406H usando una etiqueta saliente E7 y al nodo interno 406I usando una etiqueta saliente E9. Las etiquetas E7 y E9 pueden ser etiquetas asignadas por los nodos 406H y 406I para el LSP primario, respectivamente. Cuando el nodo de origen 404 y/o el nodo de ingreso de seguridad 406B detectan un fallo del nodo de ingreso primario 406A, el estado de las entradas de reenvío para el LSP primario puede cambiar de activo a inactivo y el estado de las entradas de reenvío para el LSP de seguridad puede cambiar de inactivo a activo. En una realización a modo de ejemplo, el estado de la entrada de reenvío para el LSP primario y el estado de la entrada de reenvío para el LSP de seguridad pueden cambiar simultáneamente. Luego de detectar un fallo del nodo de ingreso primario 406A, el nodo de ingreso de seguridad 406B se puede configurar para recibir el tráfico de datos de un segundo trayecto de origen del nodo de origen 404 y para enviar el tráfico de datos usando las entradas de reenvío para los LSP de seguridad. El nodo de ingreso de seguridad 406B se puede configurar para enviar el tráfico de datos del nodo de origen 404 a los nodos 406H, 406I, 406M y 406D. Las etiquetas E1-E9 pueden ser etiquetas asociadas y/o asignadas al flujo de tráfico de datos entre nodos de red adyacentes (p.ej., de salto siguiente). Por ejemplo, la etiqueta E3 puede ser una etiqueta asociada al flujo de tráfico de datos del nodo de ingreso primario 406A al nodo de ingreso de seguridad 406B y se puede asignar por el nodo de ingreso de seguridad 406B.

La Figura 5 es un diagrama esquemático de otra realización a modo de ejemplo de un sistema conmutado por etiquetas 500 que emplea la protección de nodo de ingreso. El sistema conmutado por etiquetas 500 comprende una red conmutada por etiquetas 502 que comprende múltiples nodos de red 506A-506N y 506P. En particular, un nodo de ingreso primario 506A, un nodo de ingreso de seguridad 506B, múltiples nodos internos 506C-506J y nodos de egreso 506K-506N y 506P. El nodo de ingreso primario 506A puede ser sustancialmente similar al primer nodo de ingreso 111 descrito en la Figura 1, el nodo de ingreso de seguridad 506B puede ser sustancialmente similar al segundo nodo de ingreso 112 descrito en la Figura 1, los múltiples nodos internos 506C-506J pueden ser sustancialmente similares a los nodos internos 130 descritos en la Figura 1, y los nodos de egreso 506K-506N y 506P pueden ser sustancialmente similares al primer nodo de egreso 121 o al segundo nodo de egreso 122 descritos en la Figura 1.

La red conmutada por etiquetas 502 se puede configurar para emplear uno o más LSP para comunicar el tráfico de datos del nodo de origen 504 a los nodos cliente 508A y 508B y/o a otros nodos cliente (no se muestran en la Figura 5). El único o más LSP pueden ser como se describe en la Figura 1. Un LSP primario del nodo de ingreso primario 506A a los nodos de egreso 506K-506N y 506P se muestra mediante el uso de líneas continuas en forma de flecha en la Figura 5. La red conmutada por etiquetas 502 además comprende uno o más LSP de seguridad configurados para proteger el nodo de ingreso primario 506A y para reenviar el tráfico de datos del nodo de origen 504 a los nodos cliente 508A y 508B y/u otros nodos cliente (no se muestran en la Figura 5) cuando el nodo de ingreso primario 506A del LSP primario falla. Los LSP de seguridad pueden ser del nodo de ingreso de seguridad 506B a los nodos de salto siguiente del nodo de ingreso de seguridad 506B y los nodos de salto siguiente de cada nodo de salto previo (p.ej., el nodo de ingreso primario 506A y el nodo 506G) del nodo de ingreso de seguridad 506B

diferente de un nodo del nodo de ingreso primario 506A al nodo de ingreso de seguridad 506B a lo largo del LSP primario.

El nodo de origen 504, el nodo de ingreso primario 506A y/o el nodo de ingreso de seguridad 506B se pueden configurar de forma sustancialmente similar al nodo de origen 304, nodo de ingreso primario 306A y nodo de ingreso de seguridad 306B según se describe en la Figura 3, respectivamente. El sistema conmutado por etiquetas 500 puede comprender una o más sesiones BFD para detectar un fallo de nodo de ingreso primario según se describe en la Figura 3. El nodo de ingreso de seguridad 506B se puede configurar para crear uno o más LSP de seguridad y/o para generar una o más entradas de reenvío para un LSP primario y/o una o más entradas de reenvío para los LSP de seguridad en una tabla de reenvío en respuesta a la recepción de un objeto de mensaje (p.ej., un objeto de mensaje según se describe en la Figura 7) del nodo de ingreso primario 506A. En una realización a modo de ejemplo, se puede crear un LSP de seguridad del nodo de ingreso de seguridad 506B a un primer conjunto de nodos y un segundo conjunto de nodos. El primer conjunto de nodos puede comprender los nodos de salto siguiente (p.ej., nodos 506H y 506M) del nodo de ingreso de seguridad 506B. El segundo conjunto de nodos puede comprender los nodos de salto siguiente (p.ej., nodo 506K y 506C) del nodo de ingreso primario 506A diferente del nodo de salto anterior del nodo de ingreso de seguridad 506B (p.ej., nodo 506G) y el nodo de salto siguiente del nodo de salto anterior del nodo de ingreso de seguridad 506B (p.ej., nodo 506I). En una realización a modo de ejemplo, los subLSP del nodo de ingreso de seguridad 506B al primer conjunto de nodos pueden no señalizarse y las entradas de reenvío para los subLSP se pueden crear usando la información del LSP primario cuando se crea el LSP de seguridad. Por ejemplo, una o más etiquetas se pueden asignar por los nodos para el LSP primario. Los subLSP del nodo de ingreso de seguridad 506B al segundo conjunto de nodos pueden señalizarse y las entradas de reenvío para los subLSP se pueden crear según la señalización. La Tabla 3 es una realización a modo de ejemplo de una tabla de reenvío que comprende múltiples entradas de reenvío para un LSP primario y múltiples entradas de reenvío para un LSP de seguridad. Las múltiples entradas de reenvío para el LSP de seguridad pueden comprender una o más entradas de reenvío para los nodos de salto siguiente del nodo de ingreso de seguridad 506B y/o una o más entradas de reenvío para los nodos de salto siguiente de cada nodo de salto anterior (p.ej., el nodo de ingreso primario 506A y el nodo 506G) del nodo de ingreso de seguridad 506B diferente de un nodo del nodo de ingreso primario 506A al nodo de ingreso de seguridad 506B (p.ej., nodos 506G y 506B) a lo largo del LSP primario. La tabla de reenvío se puede configurar de forma sustancialmente similar a la tabla de reenvío descrita en la Figura 3.

Tabla 3 - Una realización a modo de ejemplo de una tabla de reenvío

Entrada Etiqueta/FEC	Salida Etiqueta	Interfaz para salto siguiente	Estado
E7	E4	a Nodo 506H	Activo
	E5	a Nodo 506M	
FEC1	E4	a Nodo 506H	Inactivo
	E5	a Nodo 506M	
FEC1	E8	a Nodo 506K	Inactivo
	E9	a Nodo 506C	
	E10	a Nodo 506I	

La red conmutada por etiquetas 502 se puede configurar para emplear un LSP P2MP para comunicar el tráfico de datos del nodo de origen 504 a los nodos cliente 508A y 508B y/o a otros nodos cliente (no se muestran en la Figura 5). El nodo de ingreso de seguridad 506B puede encontrarse a lo largo del LSP primario, pero puede no ser un salto siguiente directo del nodo de ingreso primario 506A. En un funcionamiento típico, el nodo de ingreso de seguridad 506B se puede configurar para recibir el tráfico de datos de un primer trayecto de origen del nodo de ingreso primario 506A mediante el nodo interno 506G con una etiqueta entrante E7 y para enviar el tráfico de datos usando las entradas de reenvío para el LSP primario. El nodo de ingreso de seguridad 506B puede enviar el tráfico de datos a uno o más nodos de salto siguiente con etiquetas salientes asociadas a los nodos de salto siguiente. El nodo de ingreso de seguridad 506B se puede configurar para enviar el tráfico de datos a nodos internos 506H usando una etiqueta saliente E4 y al nodo de egreso 506M usando una etiqueta saliente E5. Cuando el nodo de origen 504 y/o el nodo de ingreso de seguridad 506B detectan un fallo del nodo de ingreso primario 506A, el estado de las entradas

de reenvío para el LSP primario puede cambiar de activo a inactivo y el estado de las entradas de reenvío para el LSP de seguridad puede cambiar de inactivo a activo. En una realización a modo de ejemplo, el estado de la entrada de reenvío para el LSP primario y el estado de la entrada de reenvío para el LSP de seguridad pueden cambiar de forma sustancialmente simultánea. Luego de detectar un fallo del nodo de ingreso primario 506A, el nodo de ingreso de seguridad 506B se puede configurar para recibir el tráfico de datos de un segundo trayecto de origen del nodo de origen 504 y para enviar el tráfico de datos usando las entradas de reenvío para los LSP de seguridad. El nodo de ingreso de seguridad 506B se puede configurar para enviar el tráfico de datos del nodo de origen 504 a los nodos 506K, 506C, 506I, 506H y 506M.

La Figura 6 es un diagrama esquemático de otra realización a modo de ejemplo de un sistema conmutado por etiquetas 600 que emplea la protección de nodo de ingreso. El sistema conmutado por etiquetas 600 comprende una red conmutada por etiquetas 602 que comprende múltiples nodos de red 606A-606M y 606N-606T. En particular, un nodo de ingreso primario 606A, un nodo de ingreso de seguridad 606B, múltiples nodos internos 606C-606M y nodos de egreso 606N-606T. El nodo de ingreso primario 606A puede ser sustancialmente similar al primer nodo de ingreso 111 descrito en la Figura 1, el nodo de ingreso de seguridad 606B puede ser sustancialmente similar al segundo nodo de ingreso 112 descrito en la Figura 1, los múltiples nodos internos 606C-606M pueden ser sustancialmente similares a los nodos internos 130 descritos en la Figura 1, y los nodos de egreso 606N-606T pueden ser sustancialmente similares al primer nodo de egreso 121 o al segundo nodo de egreso 122 descritos en la Figura 1.

La red conmutada por etiquetas 602 se puede configurar para emplear uno o más LSP para comunicar el tráfico de datos del nodo de origen 604 a los nodos cliente 608A y 608B y/o a otros nodos cliente (no se muestran en la Figura 6). El único o más LSP pueden ser como se describe en la Figura 1. Un LSP primario del nodo de ingreso primario 606A se muestra mediante el uso de líneas continuas en forma de flecha en la Figura 6. La red conmutada por etiquetas 602 además comprende uno o más LSP de seguridad configurados para proteger el nodo de ingreso primario 606A y para reenviar el tráfico de datos del nodo de origen 604 a nodos cliente 608A y 608B y/u otros nodos cliente (no se muestran en la Figura 6) cuando el nodo de ingreso primario 606A del LSP primario falla. Los LSP de seguridad pueden comprender el nodo de ingreso de seguridad 606B, los nodos de salto siguiente del nodo de ingreso de seguridad 606B y los nodos de salto siguiente del nodo de salto anterior (p.ej., el nodo de ingreso primario 606A y los nodos 606G y 606H) del nodo de ingreso de seguridad 606B diferente de un nodo del nodo de ingreso primario 606A al nodo de ingreso de seguridad 606B a lo largo del LSP primario.

El nodo de origen 604, el nodo de ingreso primario 606A y/o el nodo de ingreso de seguridad 606B se pueden configurar de forma sustancialmente similar al nodo de origen 304, nodo de ingreso primario 306A y nodo de ingreso de seguridad 306B según se describe en la Figura 3, respectivamente. El sistema conmutado por etiquetas 600 puede comprender una o más sesiones BFD para detectar un fallo de nodo de ingreso primario según se describe en la Figura 3. El nodo de ingreso de seguridad 606B se puede configurar para crear uno o más LSP de seguridad y/o para generar una o más entradas de reenvío para un LSP primario y/o una o más entradas de reenvío para los LSP de seguridad en una tabla de reenvío en respuesta a la recepción de un objeto de mensaje (p.ej., un objeto de mensaje según se describe en la Figura 7) del nodo de ingreso primario 606A. En una realización a modo de ejemplo, se puede crear un LSP de seguridad del nodo de ingreso de seguridad 606B a un primer conjunto de nodos y un segundo conjunto de nodos. El primer conjunto de nodos puede comprender los nodos de salto siguiente (p.ej., nodos 606K y 606P) del nodo de ingreso de seguridad 606B. El segundo conjunto de nodos puede comprender los nodos de salto siguiente de los nodos del nodo de ingreso primario 606A al nodo de ingreso de seguridad 606B, excluido el nodo de ingreso de seguridad 606B a lo largo del LSP primario diferente de los nodos del nodo de ingreso primario 606A al nodo de ingreso de seguridad 606B a lo largo del LSP primario. El segundo conjunto de nodos puede comprender los nodos de salto siguiente (p.ej., nodos 606N y 606C) del nodo de ingreso primario 606A diferente del nodo 606G, los nodos de salto siguiente (p.ej., nodo 606I) del nodo 606G diferente del nodo 606H, y los nodos de salto siguiente (p.ej., nodo 606J) del nodo 606H diferente del nodo de ingreso de seguridad 606B. En una realización a modo de ejemplo, los subLSP del nodo de ingreso de seguridad 606B al primer conjunto de nodos pueden no señalizarse y las entradas de reenvío para los subLSP se pueden crear usando la información del LSP primario. Por ejemplo, una o más etiquetas se pueden asignar por los nodos para el LSP primario. Los subLSP del nodo de ingreso de seguridad 606B al segundo conjunto de nodos pueden señalizarse y las entradas de reenvío para los subLSP se pueden crear según la señalización. La Tabla 4 es una realización a modo de ejemplo de una tabla de reenvío que comprende múltiples entradas de reenvío para un LSP primario y múltiples entradas de reenvío para un LSP de seguridad. Las múltiples entradas de reenvío para el LSP de seguridad pueden comprender una o más entradas de reenvío para los nodos de salto siguiente del nodo de ingreso de seguridad 606B y/o una o más entradas de reenvío para el segundo conjunto de nodos. La tabla de reenvío se puede configurar de forma sustancialmente similar a la tabla de reenvío según se describe en la Figura 3.

Tabla 4 - Una realización a modo de ejemplo de una tabla de reenvío

Entrada Etiqueta/FEC	Salida Etiqueta	Interfaz para salto siguiente	Estado
E5	E15	a Nodo 606K	Activo
	E16	a Nodo 606P	
FEC1	E15	a Nodo 606K	Inactivo
	E16	a Nodo 606P	
FEC1	E8	a Nodo 606N	Inactivo
	E9	a Nodo 606C	
	E10	a Nodo 606I	
	E11	a Nodo 606J	

La red conmutada por etiquetas 602 se puede configurar para emplear un LSP P2MP para comunicar el tráfico de datos del nodo de origen 604 a los nodos cliente 608A y 608B y/o a otros nodos cliente (no se muestran en la Figura 6). El nodo de ingreso de seguridad 606B puede encontrarse a lo largo del LSP primario, pero puede encontrarse a más de un salto de distancia del nodo de ingreso primario 606A (p.ej., tres saltos de distancia). En un funcionamiento típico, el nodo de ingreso de seguridad 606B se puede configurar para recibir el tráfico de datos de un primer trayecto de origen del nodo de ingreso primario 606A mediante nodos internos 606G y 606H y para enviar el tráfico de datos usando las entradas de reenvío para el LSP primario. El nodo de ingreso de seguridad 606B puede enviar el tráfico de datos a uno o más nodos de salto siguiente con etiquetas salientes asociadas a los nodos de salto siguiente. El nodo de ingreso de seguridad 606B se puede configurar para enviar el tráfico de datos al nodo 606K usando una etiqueta saliente E15 y al nodo 606P usando una etiqueta saliente E16. Cuando el nodo de origen 604 y/o el nodo de ingreso de seguridad 606B detectan un fallo del nodo de ingreso primario 606A, el estado de las entradas de reenvío para el LSP primario puede cambiar de activo a inactivo y el estado de las entradas de reenvío para el LSP de seguridad puede cambiar de inactivo a activo. En una realización a modo de ejemplo, el estado de las entradas de reenvío para el LSP primario y el estado de las entradas de reenvío para el LSP de seguridad pueden cambiar de forma sustancialmente simultánea. Luego de detectar un fallo del nodo de ingreso primario 606A, el nodo de ingreso de seguridad 606B se puede configurar para recibir el tráfico de datos de un segundo trayecto de origen del nodo de origen 604 y para enviar el tráfico de datos usando las entradas de reenvío para los LSP de seguridad. El nodo de ingreso de seguridad 606B se puede configurar para enviar el tráfico de datos del nodo de origen 604 a los nodos de salto siguiente del nodo de ingreso de seguridad 606B (p.ej., nodos 606K y 606P), los nodos de salto siguiente del nodo de ingreso primario 606A diferentes del nodo 606G (p.ej., nodos 606N y 606C), los cuales se encuentran a lo largo del LSP primario del nodo de ingreso primario 606A al nodo de ingreso de seguridad 606B, el nodo de salto siguiente del nodo 606G diferente del nodo 606H (p.ej., nodo 606I), el cual se encuentra a lo largo del LSP primario del nodo de ingreso primario 606A al nodo de ingreso de seguridad 606B, y el nodo de salto siguiente del nodo 606H diferente del nodo 606B (p.ej., nodo 606J), el cual se encuentra a lo largo del LSP primario del nodo de ingreso primario 606A al nodo de ingreso de seguridad 606B.

La Figura 7 es una realización a modo de ejemplo de un objeto de mensaje 700 que se puede emplear para señalizar la detección de fallo de ingreso y/o para proveer información de control a un nodo de ingreso de seguridad para proveer la detección de fallo de ingreso. En una realización, un nodo de ingreso primario (p.ej., nodo de ingreso primario 306A según se describe en la Figura 3) de un LSP primario puede transmitir un objeto de mensaje 700 a un nodo de ingreso de seguridad (p.ej., nodo de ingreso de seguridad 306B según se describe en la Figura 3). También se puede hacer referencia al objeto de mensaje 700 como un objeto de protección de ingreso. El objeto de mensaje 700 se puede configurar para que sea un mensaje independiente o incorporado dentro de otro mensaje. Por ejemplo, el objeto de mensaje 700 puede ser un objeto de protección de ingreso y se puede insertar en un mensaje TRAYECTO que se comunica entre un nodo de ingreso primario y un nodo de ingreso de seguridad.

El objeto de mensaje 700 comprende un campo de longitud 702, un campo de número de clase 704, un campo de tipo de clase (tipo c) 706, un identificador LSP secundario (ID) 708, un campo de bandera 710, un campo de opciones 712, un campo de modo de detección (DM, por sus siglas en inglés) 714 y un campo de subobjetos 716. El

campo de longitud 702 puede ser de alrededor de dos bytes de largo y puede indicar la longitud total (p.ej., en bytes) del objeto de mensaje 700. El campo de número de clase 704 puede ser de alrededor de un byte de largo y puede identificar un objeto de mensaje. El campo de tipo de clase 706 puede ser de alrededor de un byte de largo y puede identificar un tipo de objeto de mensaje. El campo ID LSP secundario 708 puede ser de alrededor de dos bytes de largo y puede comprender un ID, el cual se puede usar por un nodo de ingreso de seguridad para establecer un LSP de seguridad de modo que los recursos se pueden compartir entre el LSP de seguridad y un LSP existente. El campo de bandera 710 puede ser de alrededor de un byte de largo y puede comunicar información de estado del ingreso de seguridad al ingreso primario. Por ejemplo, el campo de bandera 710 puede indicar si la protección de fallo de ingreso se encuentra disponible o en uso. El campo de opciones 712 puede ser de alrededor de cinco bits de largo y puede indicar un comportamiento deseado a un nodo de ingreso de seguridad y/o un nodo de salto siguiente. Por ejemplo, el campo de opción 712 puede indicar usar un LSP de seguridad P2MP para proteger el nodo de ingreso primario. El campo de modo de detección 714 puede ser de alrededor de tres bits de largo y puede indicar un modo de detección de fallo deseado. Por ejemplo, el campo de modo de detección 714 puede indicar que un nodo de ingreso de seguridad y/o un nodo de origen pueden ser responsables de la detección de un fallo de nodo de ingreso y/o de la redirección del tráfico de datos. El campo de subobjetos 716 puede comprender uno o más subobjetos que pueden comprender información para establecer un LSP de seguridad y/o para controlar un LSP de seguridad, como se describirá en la presente memoria. En una realización a modo de ejemplo, el campo de subobjetos 716 puede ser de alrededor de ocho bytes de largo.

La Figura 8 es una realización a modo de ejemplo de un subobjeto de mensaje 800 usado para comunicar una dirección IP de nodo de ingreso de seguridad o una dirección IP de nodo de ingreso primario. En una realización, un nodo de ingreso primario (p.ej., nodo de ingreso primario 306A según se describe en la Figura 3) de un LSP primario puede transmitir un objeto de mensaje (p.ej., objeto de mensaje 700 según se describe en la Figura 7) que comprende un subobjeto 800 a un nodo de ingreso de seguridad (p.ej., nodo de ingreso de seguridad 306B según se describe en la Figura 3). El subobjeto 800 puede comprender un campo de tipo 802, un campo de longitud 804, un campo reservado 806 y un campo de dirección IP 808. El campo de tipo 802 puede ser de alrededor de un byte de largo y puede indicar que el subobjeto 800 comprende una dirección IP de nodo de ingreso de seguridad o una dirección IP de nodo de ingreso primario (p.ej., una dirección IP versión 4 (IPv4) o IP versión 6 (IPv6)). El campo de longitud 804 puede ser de alrededor de un byte de largo y puede indicar la longitud total (p.ej., en bytes) del subobjeto 800. El campo reservado 806 puede ser de alrededor de dos bytes de largo y se puede completar con ceros. El campo de dirección IP 808 puede ser de alrededor de cuatro bytes de largo para una dirección IPv4 y de alrededor de ocho bytes de largo para una dirección IPv6. El campo de dirección IP 808 puede indicar la dirección IP del nodo de ingreso de seguridad o del nodo de ingreso primario. Por ejemplo, el campo de dirección IP 808 puede comprender una dirección unidifusión IPv4 de 32 bits o una dirección unidifusión IPv6 de 128 bits.

La Figura 9 es otra realización a modo de ejemplo de un subobjeto de mensaje 900 empleado para describir el tráfico de datos que se mapeará o encaminará al LSP de seguridad en el nodo de ingreso de seguridad. En una realización, un nodo de ingreso primario (p.ej., nodo de ingreso primario 306A según se describe en la Figura 3) de un LSP primario puede transmitir un objeto de mensaje (p.ej., objeto de mensaje 700 según se describe en la Figura 7) que comprende un subobjeto 900 a un nodo de ingreso de seguridad (p.ej., nodo de ingreso de seguridad 306B según se describe en la Figura 3). El subobjeto 900 comprende un campo de tipo 902, un campo de longitud 904, un campo reservado 906 y uno o más elementos de tráfico 908. El campo de tipo 902 puede ser de alrededor de un byte de largo y puede indicar que el subobjeto 900 comprende uno o más elementos de tráfico. El campo de longitud 904 puede ser de alrededor de un byte de largo y puede indicar la longitud total (p.ej., en bytes) del subobjeto 900. El campo reservado 906 puede ser de alrededor de dos bytes de largo y se puede completar con ceros. Cada elemento de tráfico 908 puede ser de alrededor de cuatro bytes de largo y puede indicar un tipo de tráfico. Por ejemplo, un elemento de tráfico 908 puede indicar un tipo de tráfico como tráfico de interfaz y puede comprender un índice de una interfaz desde la cual el tráfico se importa en el LSP de seguridad. De manera alternativa, el elemento de tráfico 908 puede indicar un tipo de tráfico como el tráfico de prefijo IPv4/IPv6 y puede comprender una longitud de prefijo y un prefijo de dirección IPv4/IPv6.

La Figura 10 es otra realización a modo de ejemplo de un subobjeto de mensaje 1000 empleado para comunicar las etiquetas y trayectos de los saltos siguientes para un nodo de ingreso primario. El subobjeto 1000 comprende un campo de tipo 1002, un campo de longitud 1004, un campo reservado 1006 y un campo de subobjeto 1008. El campo de tipo 1002 puede ser de alrededor de un byte de largo y puede indicar que el subobjeto 1000 comprende una o más etiquetas y/o trayectos para los saltos siguientes para un nodo de ingreso primario. El campo de longitud 1004 puede ser de alrededor de un byte de largo y puede indicar la longitud total (p.ej., en bytes) del subobjeto 1000. El campo reservado 1006 puede ser de alrededor de dos bytes de largo y se puede completar con ceros. El campo de subobjeto 1008 puede comprender una o más etiquetas y/o trayectos para los saltos siguientes para un nodo de ingreso primario. Por ejemplo, el campo de subobjeto 1008 puede ser de alrededor de ocho bytes de largo y puede comprender los primeros saltos de un LSP y una etiqueta emparejada con cada salto. Con respecto a las Figuras 7-10, se advierte que cualquier campo de datos puede tener cualquier tamaño apropiado como apreciará una persona con experiencia ordinaria en la técnica tras estudiar la presente descripción.

La Figura 11 es un diagrama de flujo de una realización a modo de ejemplo de un método de protección de nodo de ingreso 1100. En una realización a modo de ejemplo, el método 1100 se puede implementar en un nodo de red (p.ej., un nodo de ingreso de seguridad 306B según se describe en la Figura 3). El método 1100 se puede emplear para comunicar el tráfico de datos de un nodo de origen a un nodo cliente mediante un LSP de seguridad en caso de que un nodo de ingreso primario del LSP primario falle. En la etapa 1102, el método 1100 puede recibir información de trayecto para un LSP primario. En una realización a modo de ejemplo, el método 1100 puede recibir un mensaje de solicitud de protección de ingreso (p.ej., un mensaje TRAYECTO) que comprende un objeto de protección de ingreso (p.ej., el objeto de mensaje 700 según se describe en la Figura 7) y/o información de trayecto. La información de trayecto puede incluir, pero sin limitación, información de encaminamiento para uno o más LSP, identificadores para uno o más nodos de red a lo largo de uno o más LSP, identificador para uno o más encaminamientos e información de etiquetado. El mensaje de solicitud de protección de ingreso puede comprender también un identificador (p.ej., una dirección IP o una dirección de control de acceso al medio (MAC, por sus siglas en inglés) que indica un nodo de ingreso de seguridad para un nodo de ingreso primario y/o un modo de detección de fallo.

En la etapa 1104, el método 1100 puede generar una o más entradas de reenvío para un LSP de seguridad en una tabla de reenvío. Una entrada de reenvío puede comprender una etiqueta entrante, una etiqueta saliente, un identificador para una interfaz para un nodo de salto siguiente (p.ej., una asignación de puerto) y un identificador de estado. El método 1100 puede usar la información de trayecto para generar una o más entradas de reenvío para los nodos de salto siguiente del nodo de ingreso de seguridad, una o más entradas de reenvío para los nodos de salto siguiente del nodo de ingreso primario y/o una o más entradas de reenvío para los nodos de salto siguiente de nodos de red a lo largo de un trayecto entre el nodo de ingreso primario y el nodo de ingreso de seguridad. En una realización a modo de ejemplo, una entrada de reenvío puede no generarse para uno o más nodos de red a lo largo de un trayecto entre el nodo de ingreso primario y el nodo de ingreso de seguridad. El método 1100 puede enviar un mensaje de confirmación al nodo de ingreso primario en respuesta al mensaje de solicitud de protección de ingreso. El mensaje de confirmación puede indicar que la protección de ingreso para el nodo de ingreso primario está disponible. Por ejemplo, el mensaje de confirmación puede ser un mensaje RESV que comprende un objeto de protección de ingreso (p.ej., objeto de mensaje 700 según se describe en la Figura 7) con una o más banderas (p.ej., campo de bandera 710 según se describe en la Figura 7) configuradas para indicar que la protección local de ingreso se encuentra disponible.

En la etapa 1106, el método 1100 puede recibir el tráfico de datos en respuesta a un fallo de nodo de ingreso primario. Un fallo de nodo de ingreso primario se puede detectar por el nodo de ingreso de seguridad y/o el nodo de origen. Por ejemplo, el fallo de nodo de ingreso primario se puede detectar según se describe en la Figura 3. En una realización a modo de ejemplo, el método 1100 puede recibir el tráfico de datos de un nodo de origen (p.ej., un nodo de origen 304 según se describe en la Figura 3) en respuesta al fallo de nodo de ingreso primario. En otra realización a modo de ejemplo, el método 1100 puede recibir el tráfico de datos del nodo de origen, pero puede extraer el tráfico de datos cuando no se ha detectado fallo de nodo de ingreso primario alguno. Cuando se ha detectado un fallo de nodo de ingreso primario, el método 1100 no puede extraer el tráfico de datos del nodo de origen. En la etapa 1108, el método 1100 puede actualizar el estado de las entradas de reenvío para el LSP de seguridad. Cuando se ha detectado un fallo de nodo de ingreso primario y/o cuando el nodo de ingreso de seguridad ha recibido el tráfico de datos, el estado de las entradas de reenvío para uno o más LSP primarios y/o el estado de las entradas de reenvío para uno o más LSP de seguridad en la tabla de reenvío se pueden actualizar. El estado de las entradas de reenvío para uno o más LSP primarios puede cambiar de activo a inactivo y el estado de las entradas de reenvío para uno o más LSP de seguridad puede cambiar de inactivo a activo. En una realización a modo de ejemplo, el estado de las entradas de reenvío para el LSP primario y el estado de las entradas de reenvío para el LSP de seguridad pueden cambiar de forma sustancialmente simultánea. En la etapa 1110, el método 1100 puede enviar el tráfico de datos usando las entradas de reenvío para el LSP de seguridad. El método 1100 puede enviar el tráfico de datos a uno o más nodos de salto siguiente del nodo de ingreso de seguridad, uno o más nodos de salto siguiente del nodo de ingreso primario, y/o uno o más nodos de salto siguiente de nodos de red a lo largo de un trayecto entre el nodo de ingreso primario y el nodo de ingreso de seguridad mediante el uso de las entradas de reenvío para los LSP de seguridad en la tabla de reenvío.

Al menos se describe una realización y las variaciones, combinaciones y/o modificaciones de las realizaciones y/o características de las realizaciones llevadas a cabo por una persona con experiencia ordinaria en la técnica se encuentran dentro del alcance de la descripción. Las realizaciones alternativas que resultan de combinar, integrar y/u omitir características de las realizaciones se encuentran también dentro del alcance de la descripción. En los casos en los que se indican expresamente limitaciones o intervalos numéricos, debe entenderse que dichos intervalos o limitaciones expresas incluyen intervalos o limitaciones iterativas de la misma magnitud comprendidas dentro de los intervalos o limitaciones expresamente indicadas (p.ej., desde alrededor de 1 a alrededor de 10 incluye 2, 3, 4, etc.; mayor que 0,10 incluye 0,11, 0,12, 0,13, etc.). Por ejemplo, cuando se describe un intervalo numérico con un límite inferior, R_1 y un límite superior, R_u, se está describiendo de manera específica cualquier número comprendido dentro del intervalo. En particular, se describen de manera específica los siguientes números comprendidos dentro del intervalo: $R = R_1 + k * (R_u - R_1)$, en donde k es una variable que oscila entre 1 por ciento y

100 por ciento con un incremento de 1 por ciento, a saber, k es 1 por ciento, 2 por ciento, 3 por ciento, 4 por ciento, 5 por ciento, ..., 50 por ciento, 51 por ciento, 52 por ciento, ..., 95 por ciento, 96 por ciento, 97 por ciento, 98 por ciento, 99 por ciento, o 100 por ciento. Asimismo, cualquier intervalo numérico definido por dos números R como se define más arriba también se describe de manera específica. El uso del término "alrededor de" significa +/-10% del número subsiguiente, a menos que se establezca lo contrario. El uso del término "opcionalmente" con respecto a cualquier elemento de una reivindicación significa que el elemento se requiere o, de forma alternativa, que el elemento no se requiere, estando ambas alternativas comprendidas dentro del alcance de la reivindicación. El uso de términos más amplios como, por ejemplo, "comprende", "incluye" y "tiene" puede entenderse como un complemento para términos más específicos como, por ejemplo, "consiste en", "consiste esencialmente en" y "comprende sustancialmente". Por consiguiente, el alcance de la protección no está limitado por la descripción establecida más arriba sino que está definido por las reivindicaciones siguientes, dicho alcance incluyendo todos los equivalentes del objeto de las reivindicaciones. Cada reivindicación se incorpora como una descripción adicional a la memoria descriptiva y las reivindicaciones son realizaciones de la presente descripción. La discusión de una referencia en la descripción no es una admisión de que es una técnica anterior, especialmente cualquier referencia que tenga una fecha de publicación posterior a la fecha de prioridad de la presente solicitud. La descripción de todas las patentes, solicitudes de patente y publicaciones citadas en la descripción se incorporan a la presente por referencia, en la medida en que provean detalles a modo de ejemplo, de procesos u otros detalles complementarios a la descripción.

Aunque se han provisto varias realizaciones en la presente descripción, se debe comprender que los sistemas y métodos descritos se pueden realizar de muchas otras maneras específicas sin apartarse del espíritu o alcance de la presente descripción. Los presentes ejemplos se considerarán ilustrativos y no limitativos, y la intención no se limitará a los detalles dados en la presente memoria. Por ejemplo, se pueden combinar o integrar en otro sistema varios elementos o componentes, o ciertas características se pueden omitir o no implementar.

Además, las técnicas, sistemas, subsistemas y métodos descritos e ilustrados en las diferentes realizaciones como discretos o separados se pueden combinar o integrar en otros sistemas, módulos, técnicas o métodos sin apartarse del alcance de la presente descripción. Los artículos que se muestran o describen como acoplados o directamente acoplados o en comunicación entre sí pueden acoplarse directamente o comunicarse a través de alguna interfaz, dispositivo o componente intermedio, ya sea de forma eléctrica, mecánica u otra. Otros ejemplos de cambios, sustituciones y alteraciones son comprobables por una persona con experiencia en la técnica y se pueden llevar a cabo sin apartarse del alcance descrito en la presente memoria.

REIVINDICACIONES

1. Un método para proveer protección de fallo de ingreso en un nodo de red, en una red conmutada por etiquetas, el método comprende:

recibir (1102) información de trayecto que identifica uno o más de otros nodos de red a lo largo de un trayecto primario conmutado por etiquetas, LSP;

crear un LSP de seguridad para los otros nodos de red;

generar (1104) una o más entradas de reenvío a lo largo del LSP de seguridad, en donde las entradas de reenvío a lo largo del LSP de seguridad comprenden un identificador de estado que indica un estado activo cuando el tráfico de datos se envía usando el LSP de seguridad y un estado inactivo cuando el tráfico de datos no se envía usando el LSP de seguridad;

comunicar el tráfico de datos de un primer trayecto de origen a uno o más de los otros nodos de red;

recibir (1106) el tráfico de datos de un segundo trayecto de origen en respuesta a un fallo de nodo de ingreso del primer trayecto de origen; y

enviar (1110) el tráfico de datos del segundo trayecto de origen usando las entradas de reenvío y el LSP de seguridad,

en donde el nodo de red es un miembro del LSP primario.

2. El método de la reivindicación 1, en donde el nodo de red es un nodo de salto siguiente de un nodo de ingreso primario para el LSP primario.

3. El método de la reivindicación 1, en donde el identificador de estado cambia del estado inactivo al estado activo después del fallo de nodo de ingreso del primer trayecto de origen.

4. El método de la reivindicación 1, en donde las entradas de reenvío comprenden una clase de equivalencia de reenvío, FEC, que identifica un origen de tráfico de datos y una etiqueta saliente que identifica un nodo de salto siguiente.

5. El método de la reivindicación 1, que además comprende generar una o más entradas de reenvío a lo largo del LSP primario para los otros nodos de red.

6. El método de la reivindicación 5, en donde comunicar el tráfico de datos del primer trayecto de origen comprende enviar el tráfico de datos a los otros nodos de red a lo largo del LSP primario.

7. El método de la reivindicación 1, que además comprende detectar el fallo de nodo de ingreso del primer trayecto de origen usando uno o más enlaces de detección de fallo.

8. El método de la reivindicación 1, que además comprende extraer el tráfico de datos del segundo trayecto de origen cuando el fallo de nodo de ingreso del primer trayecto de origen no está presente.

9. El método de la reivindicación 1, en donde el tráfico de datos no se encuentra disponible desde el segundo trayecto de origen cuando el fallo de nodo de ingreso del primer trayecto de origen no está presente.

10. El método de la reivindicación 1, en donde crear el LSP de seguridad comprende:

crear una primera entrada de reenvío para un primer subLSP para un nodo de salto siguiente del nodo de red;

señalizar un segundo subLSP para uno o más de los otros nodos de red; y

crear una segunda entrada de reenvío para el segundo subLSP según la señalización del segundo subLSP,

en donde crear la primera entrada de reenvío comprende usar una o más etiquetas para el LSP primario y sin señalizar el primer subLSP.

11. El método de la reivindicación 1, en donde el LSP de seguridad es un LSP punto a punto, P2P, o un LSP punto a multipunto, P2MP.

12. Un aparato que comprende:

un receptor configurado para recibir un mensaje de protección de ingreso que identifica el aparato como un nodo de ingreso de seguridad e identifica uno o más nodos de red a lo largo de un trayecto primario conmutado por etiquetas,

LSP, y para recibir el tráfico de datos de un segundo trayecto de origen en respuesta a un fallo de nodo de ingreso de un primer trayecto de origen;

un procesador acoplado a un dispositivo de memoria y al receptor, en donde el dispositivo de memoria comprende instrucciones ejecutables por ordenador almacenadas en un medio legible por ordenador no transitorio de modo que, cuando se ejecutan por el procesador, hacen que el procesador:

cree un LSP de seguridad; y

genere una tabla de reenvío que comprende una o más entradas de reenvío para los nodos de red a lo largo del LSP primario y una o más entradas de reenvío para los nodos de red a lo largo del LSP de seguridad, en donde las entradas de reenvío a lo largo del LSP de seguridad comprenden un identificador de estado que indica un estado activo cuando el tráfico de datos se transmite usando el LSP de seguridad y un estado inactivo cuando el tráfico de datos no se transmite usando el LSP de seguridad; y

un transmisor acoplado al procesador, en donde el transmisor se configura para enviar el tráfico de datos desde el segundo trayecto de origen usando las entradas de reenvío y el LSP de seguridad, y

en donde el aparato es un miembro del LSP primario.

13. El aparato de la reivindicación 12, en donde las instrucciones ejecutables por ordenador, cuando se ejecutan por el procesador, hacen que el procesador detecte el fallo de nodo de ingreso a lo largo del primer trayecto de origen usando uno o más enlaces de detección de fallo.

14. El aparato de la reivindicación 12, en donde el identificador de estado cambia del estado inactivo al estado activo después del fallo de nodo de ingreso a lo largo del primer trayecto de origen.

15. El aparato de la reivindicación 12, en donde el tráfico de datos se recibe de un primer trayecto de origen cuando un fallo de nodo de ingreso a lo largo del primer trayecto de origen no está presente, en donde el tráfico de datos se recibe de un segundo trayecto de origen cuando el fallo de nodo de ingreso a lo largo del primer trayecto de origen está presente, en donde el tráfico de datos se transmite usando las entradas de reenvío para los nodos de red a lo largo del LSP primario cuando el fallo de nodo de ingreso a lo largo del primer trayecto de origen no está presente, y en donde el tráfico de datos se transmite usando las entradas de reenvío para los nodos de red a lo largo del LSP de seguridad cuando el fallo de nodo de ingreso a lo largo del primer trayecto de origen está presente.

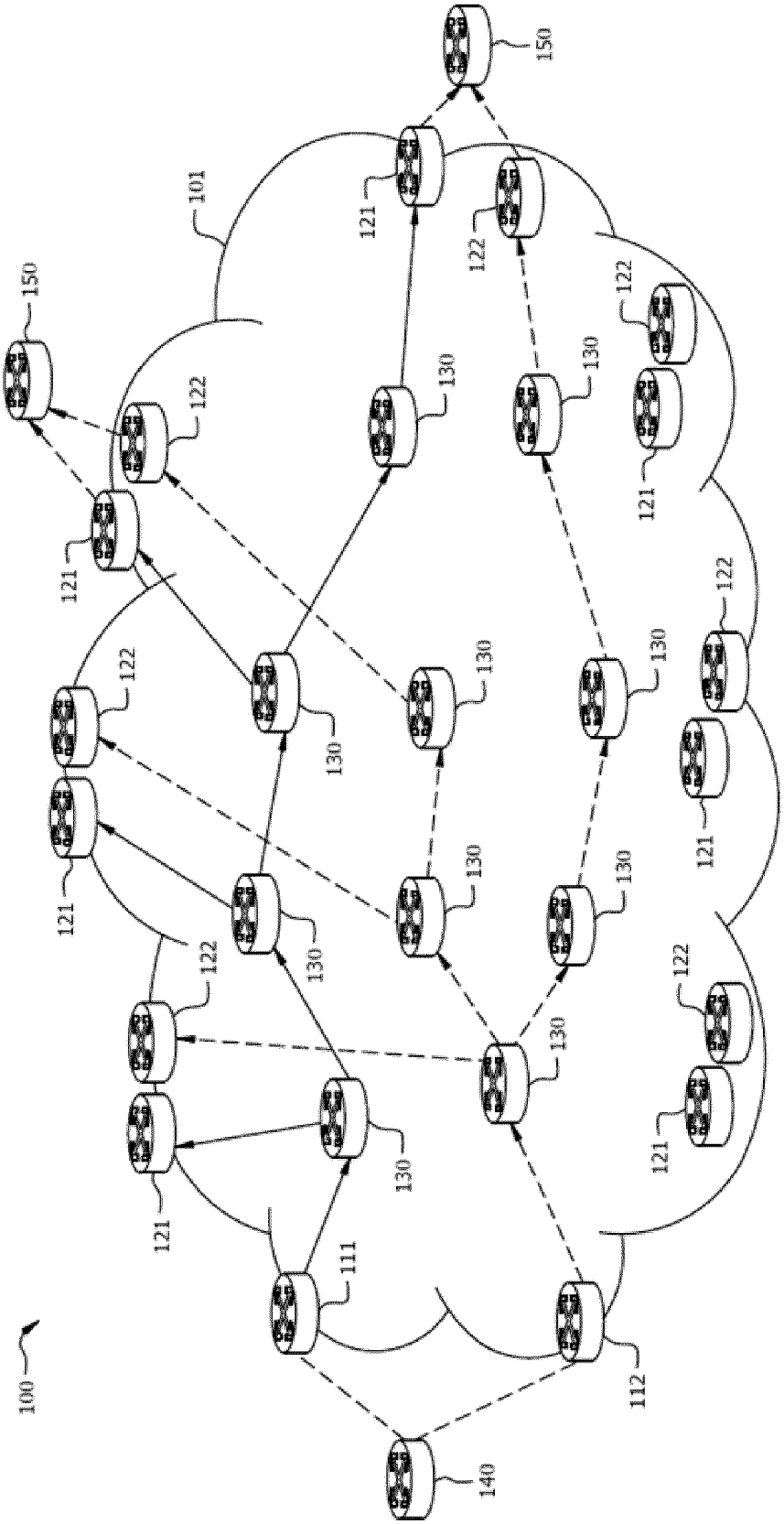

FIG. 1

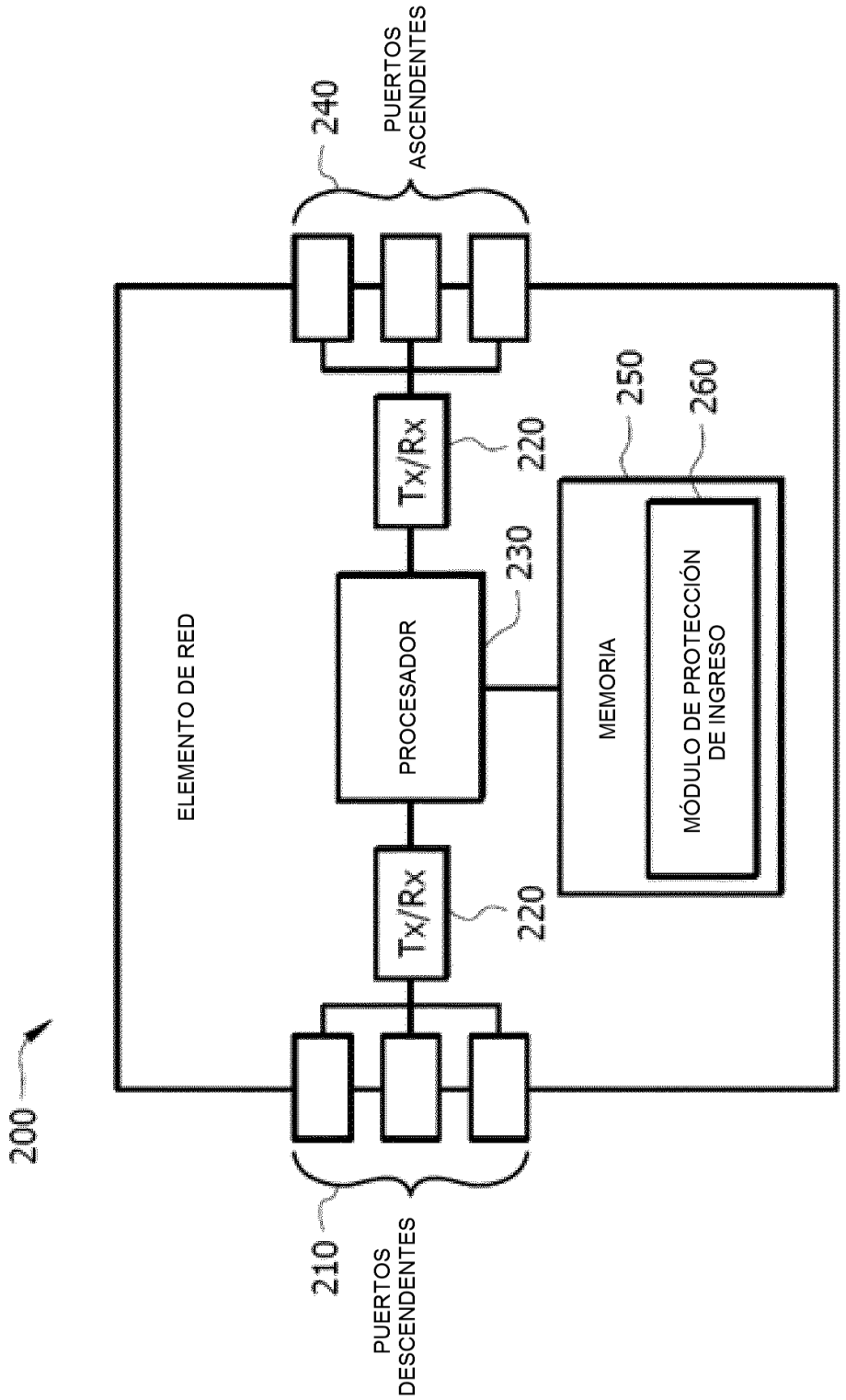
200
ELEMENTO DE RED
240
PUERTOS ASCENDENTES
210
PUERTOS DESCENDENTES
Tx/Rx
220
Tx/Rx
220
PROCESADOR
230
MEMORIA
250
MÓDULO DE PROTECCIÓN DE INGRESO
260

FIG. 2

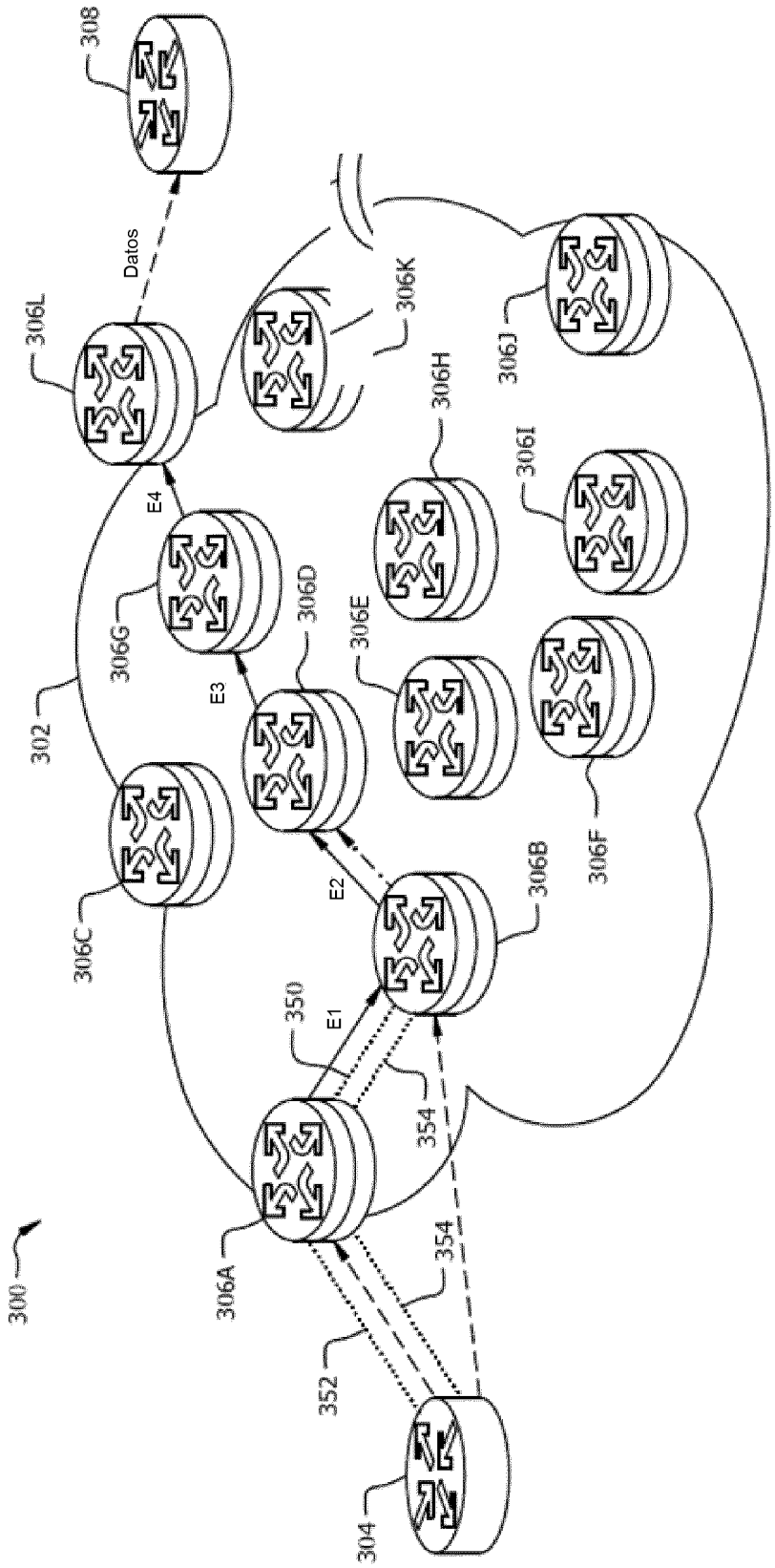
308
Datos
306L
306K
306J
306H
306I
E4
306G
306D
306E
E3
302
306F
306C
E2
306B
350
E1
354
354
306A
352
304
300

FIG. 3

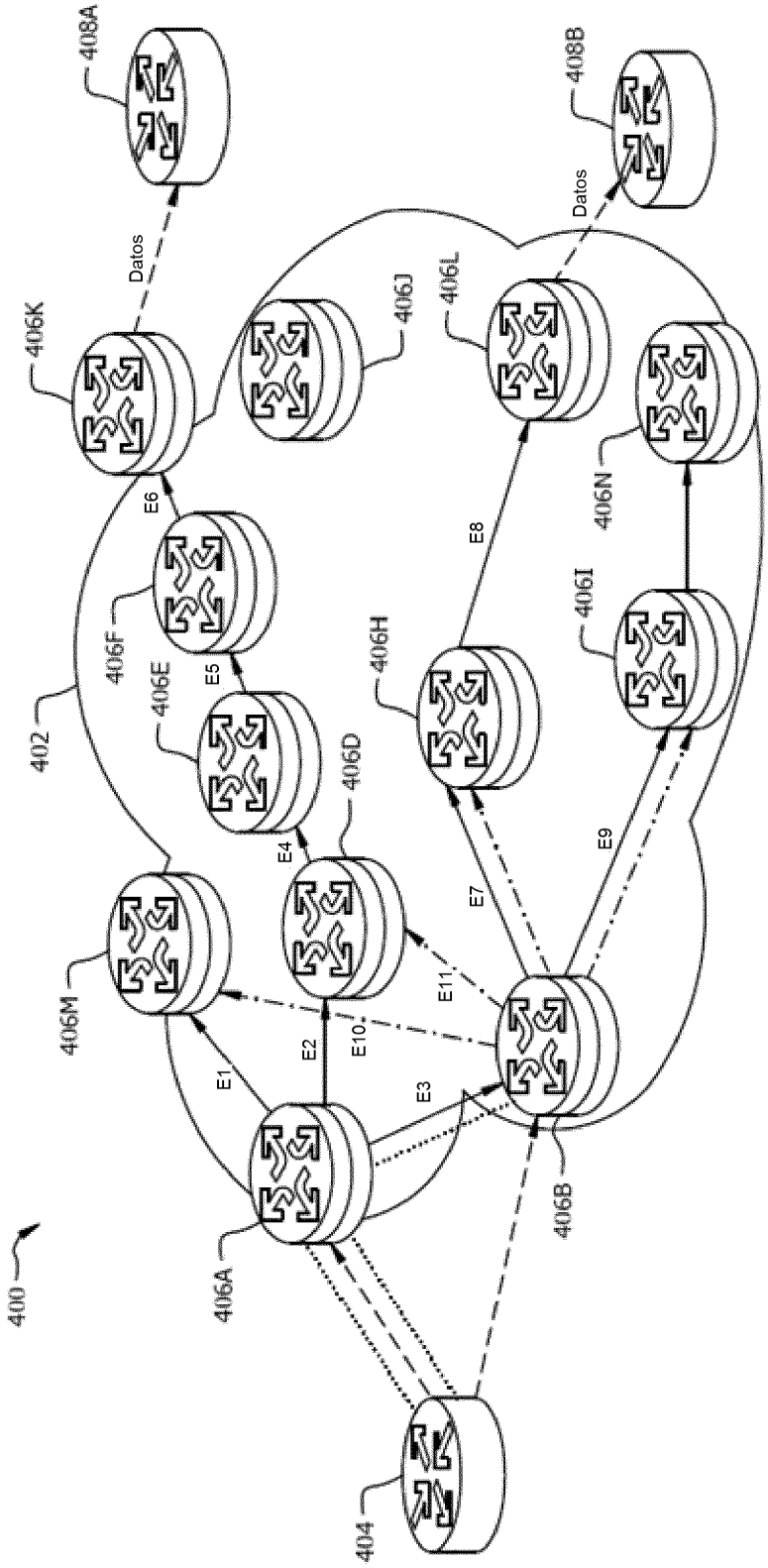
400
402
404
406A
406B
406D
406E
406F
406H
406I
406J
406K
406L
406M
406N
408A
408B
Datos
Datos
E1
E2
E3
E4
E5
E6
E7
E8
E9
E10
E11

FIG. 4

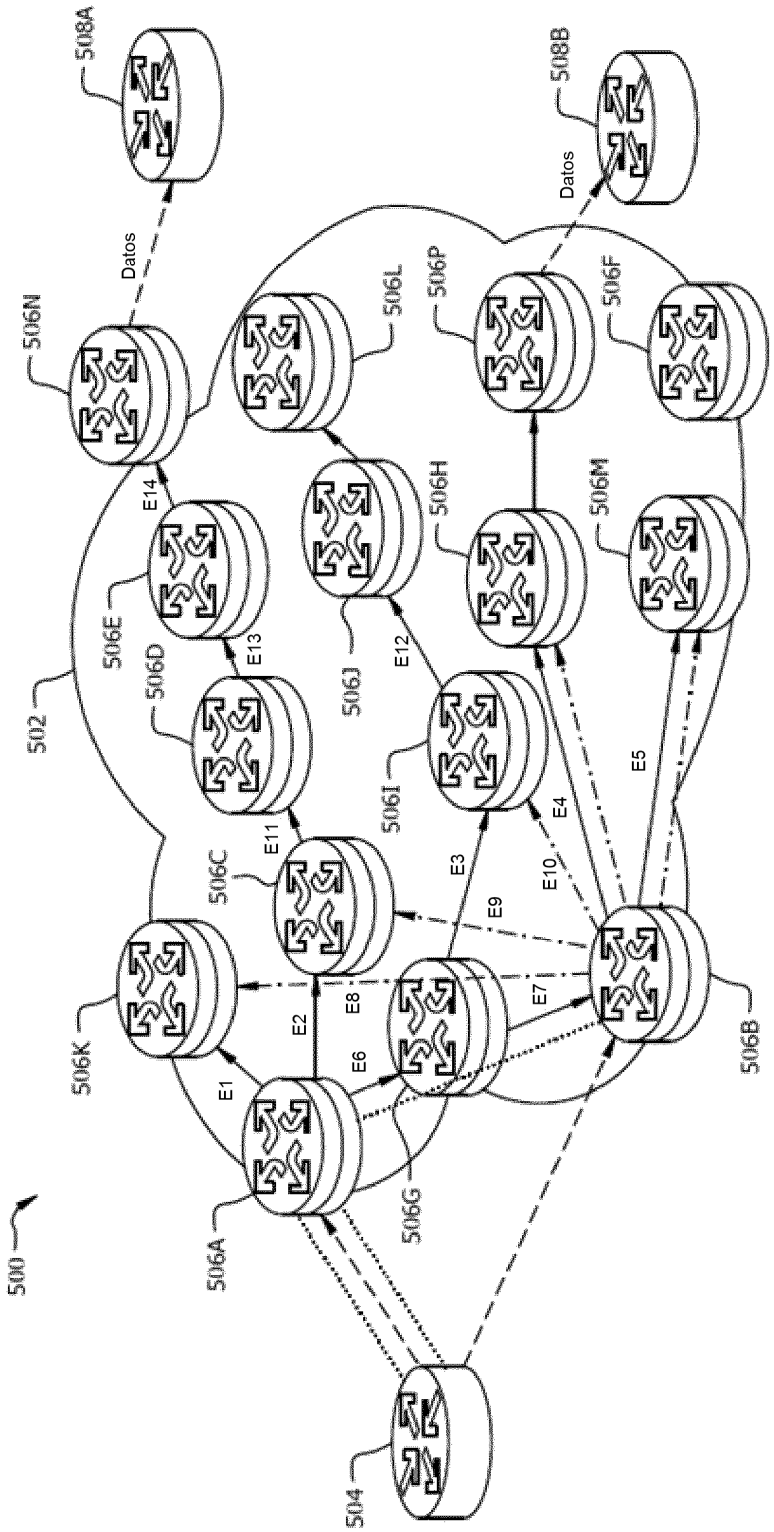
500
502
504
506A
506B
506C
506D
506E
506F
506G
506H
506I
506J
506K
506L
506M
506N
506P
508A
508B
Datos
Datos
E1
E2
E3
E4
E5
E6
E7
E8
E9
E10
E11
E12
E13
E14

FIG. 5

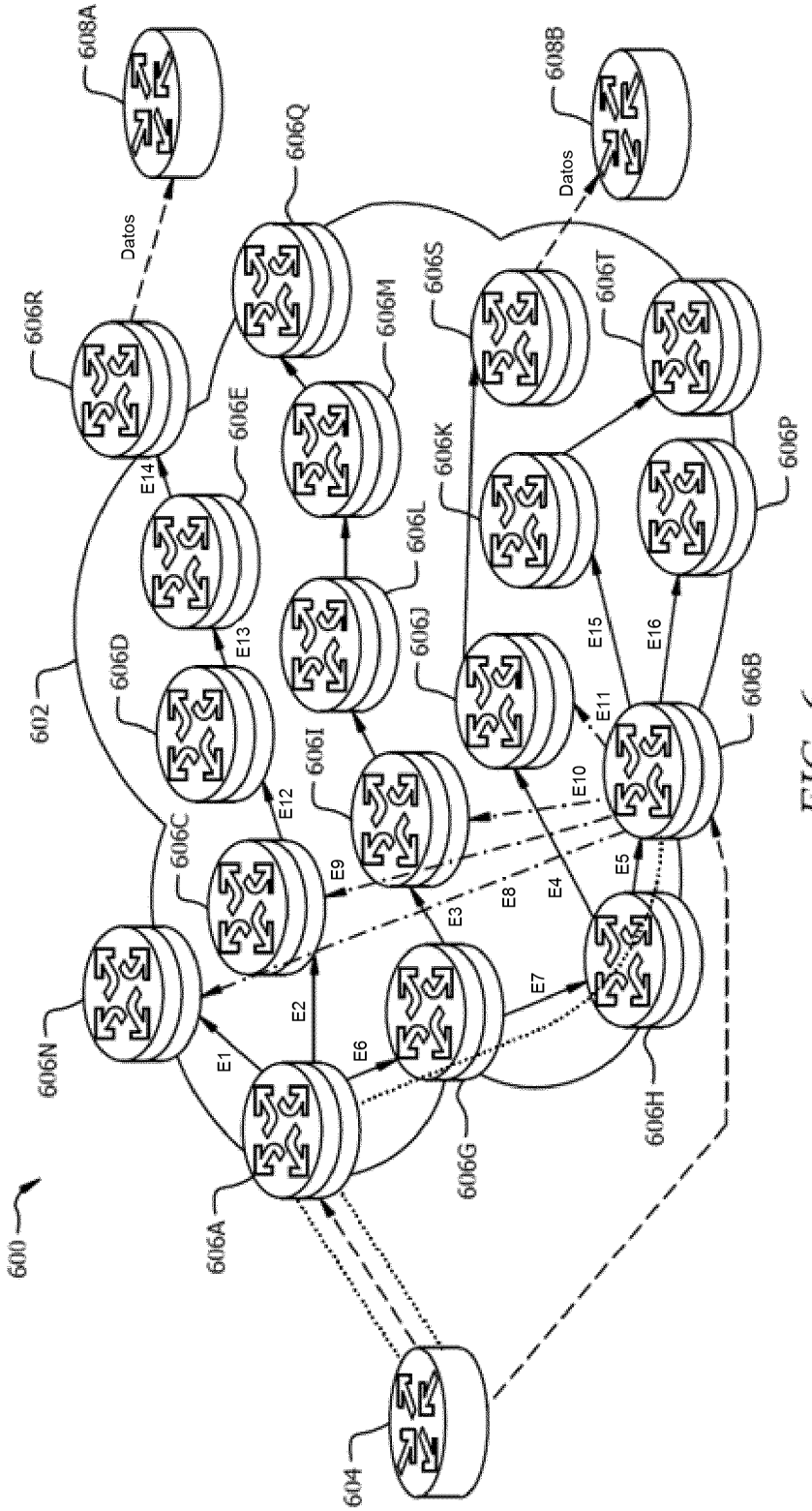
600
602
604
606A
606B
606C
606D
606E
606G
606H
606I
606J
606K
606L
606M
606N
606P
606Q
606R
606S
606T
608A
608B
Datos
Datos
E1
E2
E3
E4
E5
E6
E7
E8
E9
E10
E11
E12
E13
E14
E15
E16

FIG. 6

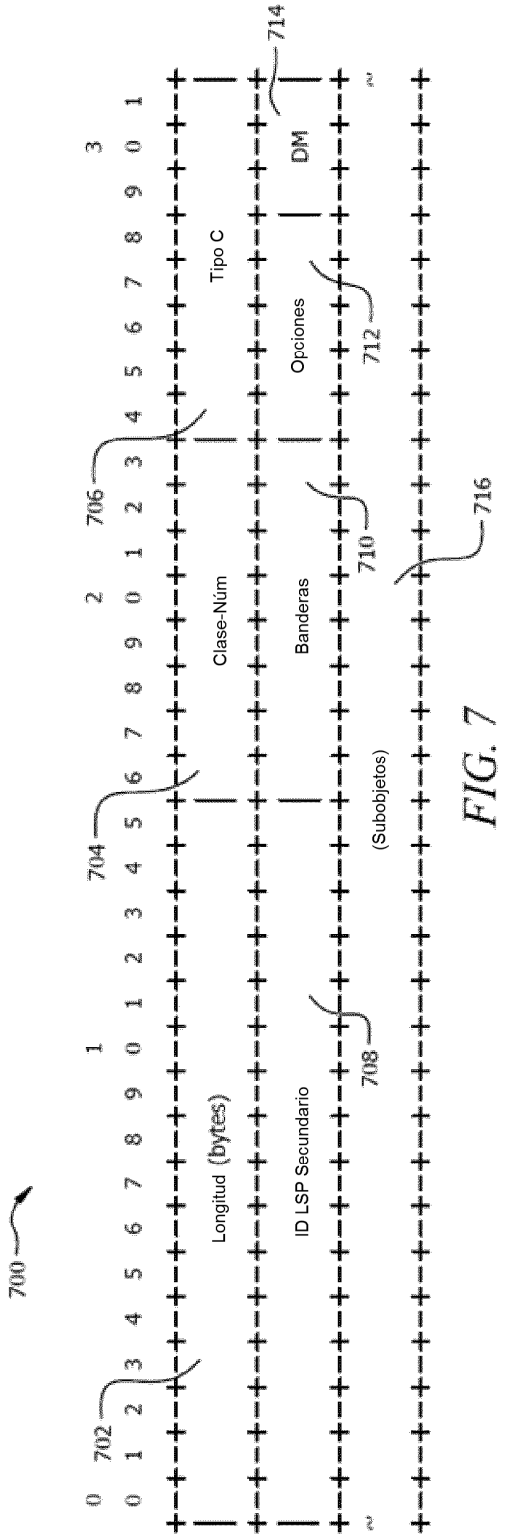
700
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
0 1 2 3
Longitud (bytes)
ID LSP Secundario
Clase-Núm
Tipo C
Banderas
Opciones
DM
(Subobjetos)
702
704
706
708
710
712
714
716

FIG. 7

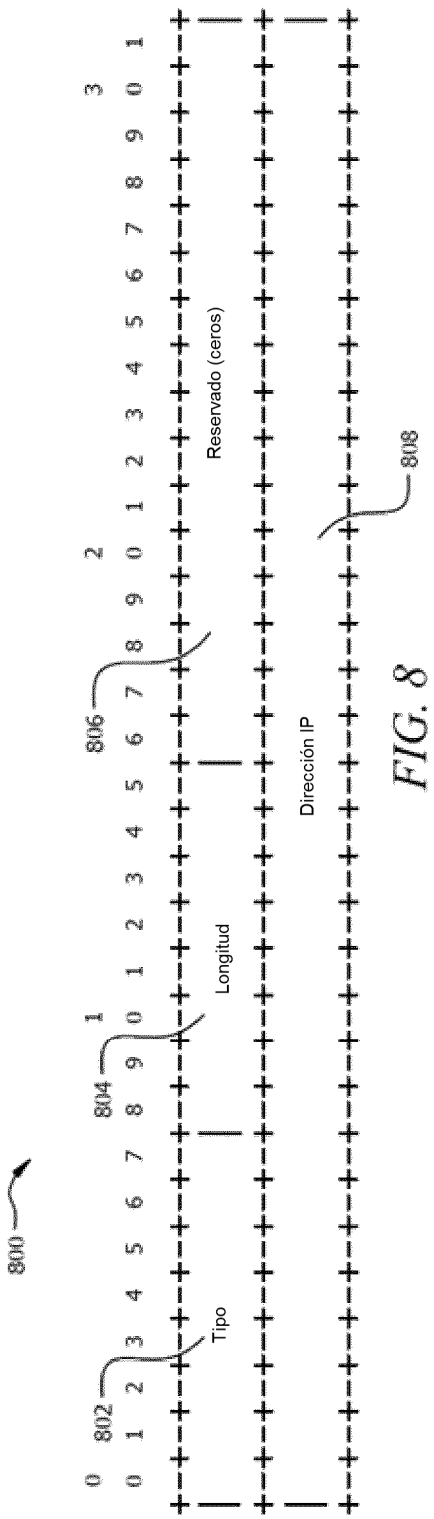
800
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
0
1
2
3
802
Tipo
Longitud
804
Reservado (ceros)
806
Dirección IP
808

FIG. 8

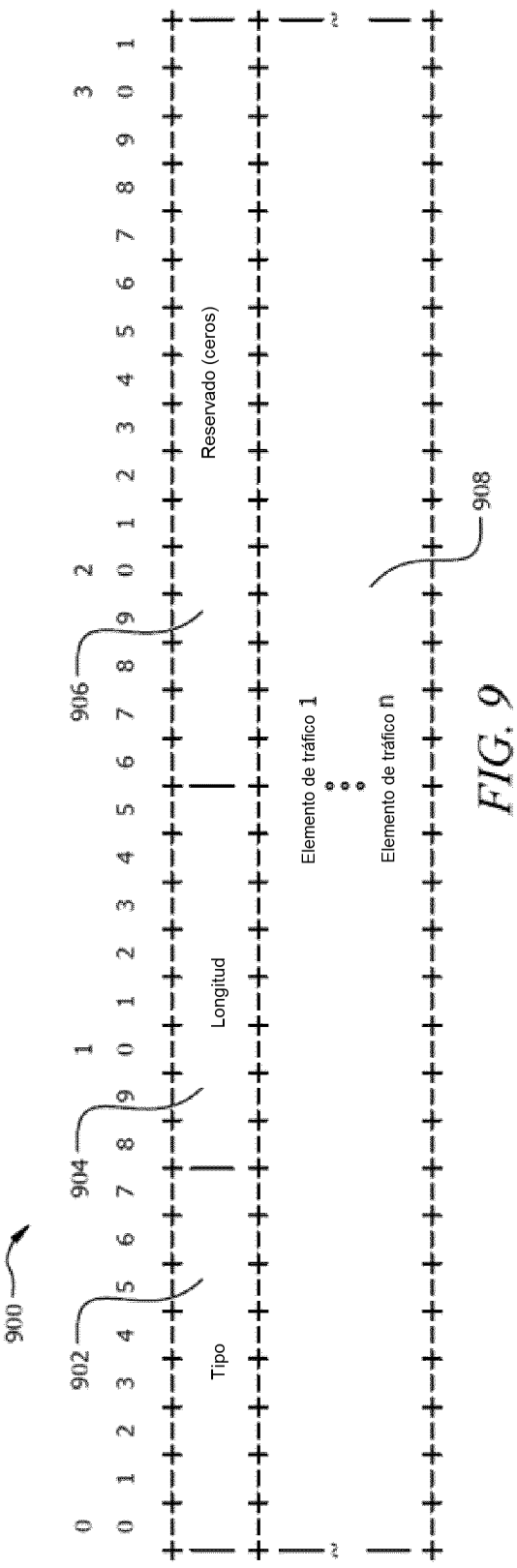
900
902
904
906
908
Tipo
Longitud
Reservado (ceros)
Elemento de tráfico 1
Elemento de tráfico n

FIG. 9

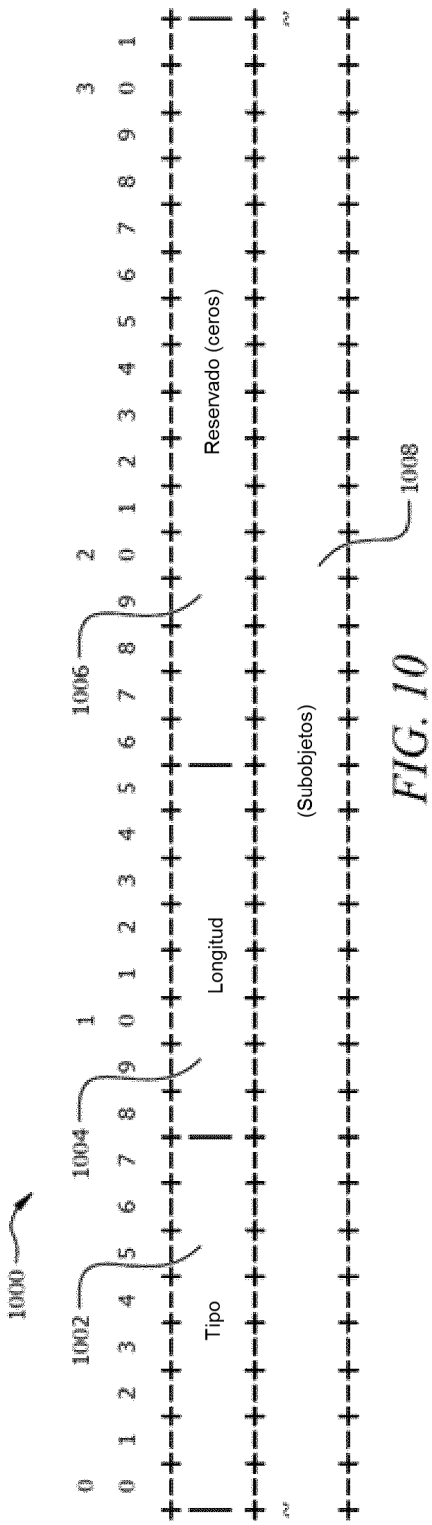
1000
1002
1004
1006
1008
Tipo
Longitud
Reservado (ceros)
(Subobjetos)

FIG. 10

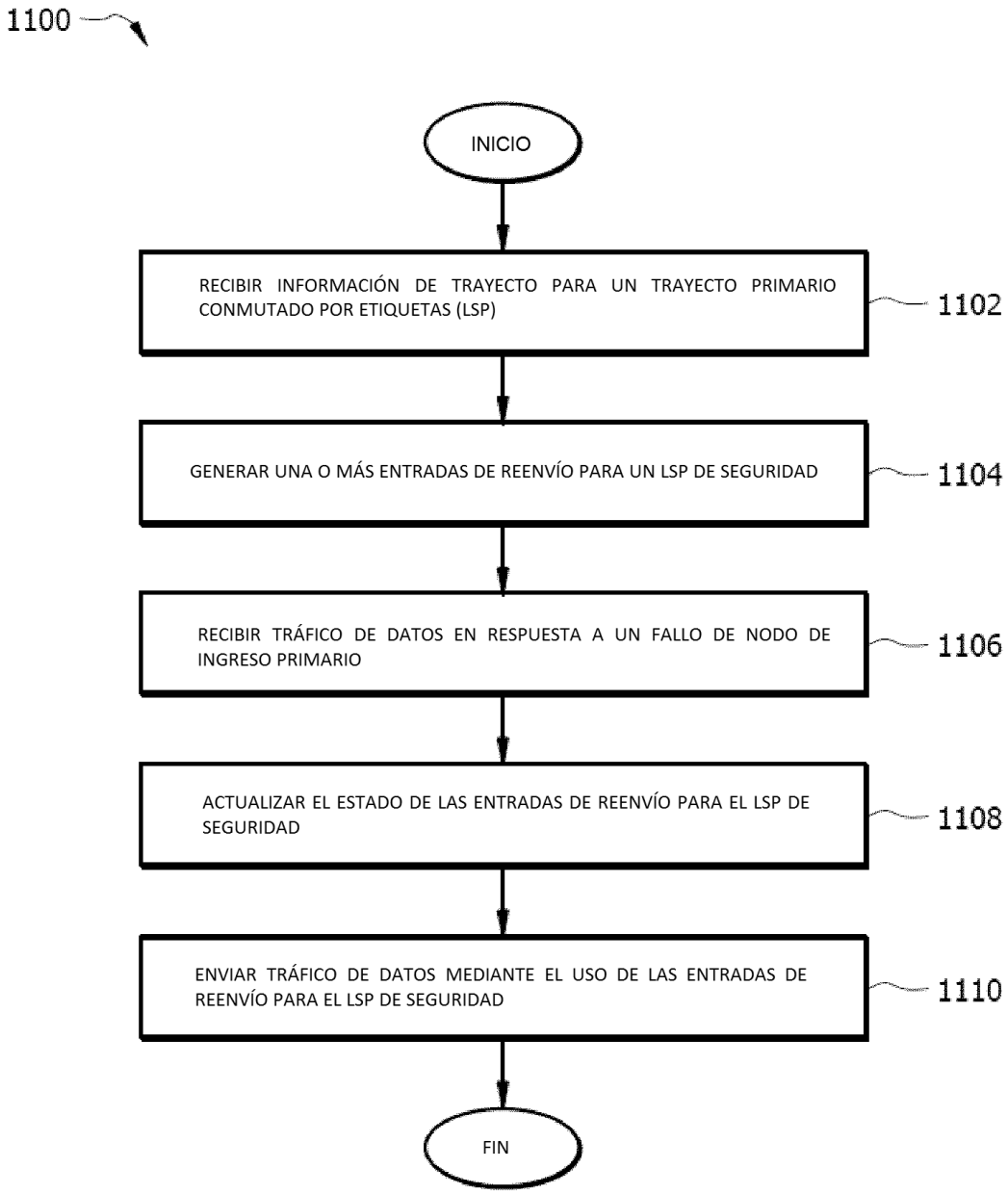
1100
INICIO
RECIBIR INFORMACIÓN DE TRAYECTO PARA UN TRAYECTO PRIMARIO CONMUTADO POR ETIQUETAS (LSP)
1102
GENERAR UNA O MÁS ENTRADAS DE REENVÍO PARA UN LSP DE SEGURIDAD
1104
RECIBIR TRÁFICO DE DATOS EN RESPUESTA A UN FALLO DE NODO DE INGRESO PRIMARIO
1106
ACTUALIZAR EL ESTADO DE LAS ENTRADAS DE REENVÍO PARA EL LSP DE SEGURIDAD
1108
ENVIAR TRÁFICO DE DATOS MEDIANTE EL USO DE LAS ENTRADAS DE REENVÍO PARA EL LSP DE SEGURIDAD
1110
FIN

FIG. 11