(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 351 870**

(51) Int. Cl.:
***H04L 12/56*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08165251 .3**
(96) Fecha de presentación : **26.09.2008**
(97) Número de publicación de la solicitud: **2043310**
(97) Fecha de publicación de la solicitud: **01.04.2009**

(54) Título: **Comunicación de una información de riesgo en una red multidominio.**

(30) Prioridad: **28.09.2007 FR 07 06846**

(45) Fecha de publicación de la mención BOPI:
**11.02.2011**

(45) Fecha de la publicación del folleto de la patente:
**11.02.2011**

(73) Titular/es: **ALCATEL LUCENT**
**54, rue la Boétie**
**75008 Paris, FR**

(72) Inventor/es: **Douville, Richard**

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

# DESCRIPCIÓN

El presente invento se refiere al campo del encaminamiento en las redes multidominio, en particular con dominios que están bajo la responsabilidad de diferentes operadores.

La noción de compartir el riesgo de fallo es un concepto importante para los problemas de cálculo de ruta o trayecto. El concepto del grupo de riesgo compartido (SRG para grupo de riesgo compartido) ha sido introducido para identificar recursos de una red que son susceptibles de ser afectados colectiva y conjuntamente por un acontecimiento o evento particular, por ejemplo el fallo de un equipo que presenta una relación funcional con todos los recursos miembros del grupo. Por ejemplo, en una red óptica, se puede definir un grupo de uniones de riesgo compartido (SRLG para un grupo de uniones de riesgo compartido) para designar todas las fibras ópticas que están localizadas en un mismo conducto físico, y que comparten por tanto un riesgo de rotura en caso de daño de este conducto. Grupos de riesgo compartido pueden también ser definidos para otros tipos de recursos de la red (nudos, uniones) y otros tipos de riesgos compartidos (localización en una misma zona geográfica, un mismo edificio, dependencia de una misma fuente de alimentación eléctrica, etc.).

En la práctica, la pertenencia de un recurso a un grupo de riesgo compartido es marcada asociando un identificador de grupo de riesgo compartido (SRG ID o SRLG ID) a este recurso. Un recurso, por ejemplo un nudo o una unión, puede pertenecer simultáneamente a varios grupos de riesgo compartido. Las informaciones de riesgo compartido, a saber las asociaciones entre recursos físicos de una red y los grupos de riesgo compartido definidos en esta red son informaciones relativamente estáticas que pueden ser recogidas en los mensajes de un protocolo de encaminamiento interior (IGP) y almacenadas en una base de datos de ingeniería de tráfico para ser explotadas por un dispositivo de cálculo de ruta o trayecto, en particular a fin de calcular rutas disjuntas. Por convenio, un camino de conexión es considerado «atravesar un grupo de riesgo compartido» cuando este camino de conexión utiliza al menos un recurso asociado a este grupo de riesgo compartido. Otros detalles sobre la utilización de los SRLG pueden ser encontrados por ejemplo en “Interferencia y Tratamiento de Grupos de Enlace de Riesgo Compartido”, draft-papadimitriou-ccamp-processing-02. IETF, Junio de 2003.

Otro documento que describe el estado de la técnica es el documento EP 1.675.326.

Para hacer posible su gestión y su funcionamiento, las grandes redes modernas, por ejemplo Internet, están estructuradas en dominios entre los cuales los intercambios de

información están sometidos a ciertas restricciones. Ejemplos de dominios son en particular los dominios de encaminamiento, las áreas y las subáreas de los protocolos de encaminamiento IGP y los sistemas autónomos (AS) de los protocolos de encaminamiento EGP. Estas restricciones tienen a la vez motivaciones funcionales, por ejemplo preservar la característica de extensión de la red e impedir su saturación y motivaciones administrativas, por ejemplo preservar la confidencialidad de ciertas informaciones relativas a la red de un operador frente a otros operadores. En particular, las informaciones de riesgo compartido en una red de operador son datos sensibles susceptibles de revelar vulnerabilidades, y que deben por tanto ser convenientemente protegidas.

Con el desarrollo de los planes de control de IP (Protocolo de Internet) basados sobre las pilas protocolarias MPLS y GMPLS, es posible automatizar los cálculos de ruta y las reservas de recursos para establecer conexiones (LSP para etiqueta de trayecto conmutado) que tienen características de ingeniería de tráfico controladas (en términos de banda pasante, protección, etc.) a través de las redes multidominio. Sin embargo, por el hecho de las restricciones impuestas entre los dominios, el cálculo de ruta entre dominios sigue siendo un problema imperfectamente resuelto, en particular cuando deben satisfacerse tensiones complejas.

Un propósito del invento es facilitar la determinación de las rutas disjuntas en una red multidominio. Otro propósito del invento es permitir la detección de un riesgo compartido entre conexiones de una capa de cliente imbricadas en conexiones de una capa de servidor.

Para ello, el invento proporciona un procedimiento para comunicar una información de riesgo en una red que incluye una pluralidad de dominios interconectados al nivel de nudos límite de dichos dominios, caracterizado por las operaciones que consisten en:

determinar un camino de conexión en un primer dominio, extendiéndose dicho camino entre un nudo límite del primer dominio conectado a un segundo dominio y un nudo de destino,

determinar un conjunto de grupos de riesgo compartido del primer dominio que son atravesados por dicho camino de conexión,

atribuir un código de identificación de riesgo compartido a dicho camino de conexión, almacenar, en un dispositivo de gestión de los grupos de riesgo

compartido asociado al primer dominio, una estructura de datos que asocia dicho código de identificación de riesgo compartido con dicho conjunto de grupos de riesgo compartido, y

transmitir al segundo dominio informaciones de ruta relativas a dicho camino de conexión e informaciones de riesgo, incluyendo dichas informaciones de riesgo dicho código de identificación de riesgo compartido y un identificador del dispositivo de gestión de los grupos de riesgo compartido que permite interrogar a dicho dispositivo para explotar dicho código de identificación de riesgo compartido.

La atribución de un código de identificación de riesgo compartido puede ser efectuada localmente en el primer dominio. Este código de identificación de riesgo compartido permite agregar la información de riesgo compartido relativa a la conexión, es decir dar una representación abreviada de la totalidad o parte de los grupos de riesgo compartido del primer dominio atravesados por la conexión. Resulta de ello una reducción del volumen de los datos a comunicar, con relación a una comunicación directa de los grupos de riesgo compartido en cuestión.

Además, mientras los grupos de riesgo compartido son informaciones que tienen una correlación fuerte con la organización y la topología de los recursos del primer dominio, es posible generar el código de identificación de riesgo compartido de manera abstracta para suprimir sensiblemente esta correlación. Así, el código de identificación de riesgo compartido puede ser comunicado al exterior del primer dominio sin comprometer informaciones sensibles relativas a la organización del primer dominio.

La explotación del código de identificación de riesgo compartido puede revestir varias formas, por ejemplo verificar a partir de sus códigos de identificación de riesgo compartido que dos caminos son SRG disjuntos (es decir que no existe ningún grupo de riesgo compartido atravesado por los dos caminos), o determinar un nuevo camino que satisfaga una tensión de carácter disjunto, especificándolo por medio de uno o varios códigos de identificación de riesgo compartido debiendo los recursos ser excluidos del nuevo camino.

Las informaciones de ruta que son comunicadas al segundo dominio pueden ser más o menos desarrolladas según las restricciones que se aplican entre los dos dominios. Informaciones relativas a los nudos y uniones atravesados por el camino en el interior del primer dominios pueden ser comunicadas o no. Una posibilidad para comunicar estas informaciones de ruta respetando los esfuerzos de confidencialidad es utilizar un “clave

de trayecto” como se ha descrito en la proposición “Preservar la Confidencialidad de la Topología en el Cálculo del Trayecto Entre Dominios Usando un Mecanismo Basado en una Clave”, R, Bradford y col., Internet Engineering Task Force, 1 de mayo de 2007.

Según otros modos de realización ventajosos, el procedimiento puede presentar una o varias de las características siguientes:

- la determinación del camino de conexión es efectuada en respuesta a la recepción de una solicitud de determinación de camino que procede del segundo dominio,

- la solicitud de determinación de camino incluye tensiones de ingeniería de tráfico y el camino de conexión es determinado para satisfacer dichas tensiones de ingeniería de tráfico.

- la solicitud de determinación de camino es recibida en un mensaje de señalización que tiende al establecimiento de una conexión entre dicho nudo límite del primer dominio y dicho nudo de destino y dichas informaciones de ruta e informaciones de riesgos son transmitidas en un mensaje de señalización que confirma el establecimiento de dicha conexión. Tal solicitud está por ejemplo constituida por un mensaje RSVP-TE PATH que incluye una ruta incompleta.

- la solicitud de determinación de camino es recibida por un elemento de cálculo de camino del primer dominio en un mensaje de solicitud del protocolo PCEP y dichas informaciones de ruta e informaciones de riesgo son transmitidas por dicho elemento de cálculo de camino del primer dominio en un mensaje de respuesta del protocolo PCE. Este modo realización permite determinar el camino de conexión antes de establecer la conexión.

- el nudo de destino es otro nudo límite del primer dominio conectado al segundo dominio. En este caso, el procedimiento puede incluir además la operación que consiste en establecer entre dos nudos de dicho segundo dominio una conexión que atraviesa dicho primer dominio a lo largo de dicho camino de conexión. Este modo de realización puede servir en particular para explotar una capa de transporte para hacer un túnel entre dos puntos de un dominio de cliente.

- el segundo dominio pertenece a una capa de red de cliente que incluye una pluralidad de nudos unidos a uniones de comunicación de un tipo cliente y el primer dominio pertenece a una capa de red de servidor que incluye una pluralidad de nudos unidos a uniones de comunicación de un tipo servidor diferente del tipo cliente, incluyendo dichas interfaces de interconexión entre el primer dominio y el segundo dominio módulos de adaptación para adaptar señales del tipo servidor al tipo cliente y para adaptar señales del tipo cliente al tipo servidor. En tal red multicapas, las tecnologías de transmisión empleadas pueden ser por ejemplo IP, Ethernet, SONET/SDH, ATM, Frame Relay, fotónica, WDM, etc.

- el procedimiento incluye la operación que consiste en difundir por medio de un protocolo de encaminamiento interior del segundo dominio, por ejemplo OSPF-TE o IS-IS-TE, un anuncio de unión que se refiere a una conexión establecida entre dos nudos de dicho segundo dominio, atravesando dicha conexión dicho primer dominio a lo largo de dicho camino de conexión, a incluyendo dicho anuncio de unión dichas informaciones de riesgo.

- el procedimiento incluye la operación que consiste en grabar en una base de datos de encaminamiento del segundo dominio una unión establecida entre dos nudos de dicho segundo dominio, correspondiendo dicha unión a una conexión que atraviesa dicho primer dominio a lo largo de dicho camino de conexión, incluyendo dicho registro de unión dichas informaciones de riesgo.

- el identificador del dispositivo de gestión de los grupos de riesgo compartido incluye una dirección IP, por ejemplo IPv4 o IPv6.

- el código de identificación de riesgo compartido y el identificador del dispositivo de gestión de los grupos de riesgo compartido son transmitidos en dos campos de un mismo objeto. Tal formalismo permite conservar la asociación entre los dos datos en el curso de los diferentes tratamientos protocolarios a efectuar.

El invento proporciona igualmente un dispositivo de gestión de los grupos de riesgo compartido para una red de comunicación, comprendiendo dicho dispositivo:

un módulo de almacenamiento de datos para almacenar informaciones de grupos de riesgo compartido relativos a un dominio de la red atribuido a dicho dispositivo, comprendiendo dichas informaciones asociaciones entre recursos de comunicación que pertenecen a dicho dominio de red y grupos de riesgo compartido,

un módulo de gestión de código de identificación de riesgo compartido apto para atribuir un código de identificación de riesgo compartido a un camino de conexión de dicho dominio de la red, para determinar un conjunto de grupos de riesgo compartido que son atravesados por dicho camino de conexión, y para engendrar una estructura de datos que asocia dicho código de identificación de riesgo compartido con dicho conjunto de grupos de riesgo compartido del dominio,

un módulo de explotación apto para acceder a la estructura de datos engendrada por el módulo de gestión de código de identificación de riesgo compartido, para tratar una solicitud de explotación que comprende dicho código de identificación de riesgo compartido, y medios de comunicación entre dominios aptos, por una parte, para comunicar con el exterior del dominio los códigos de identificación de riesgo compartido atribuidos a los caminos de conexión del dominio de red y un identificador del dispositivo de gestión de los grupos de riesgo compartido que permiten trasmitir al dispositivo solicitudes de explotación y, por otra parte, recibir una solicitud de explotación desde el exterior del dominio y para transmitir una respuesta a dicha solicitud de explotación.

El invento proporciona igualmente una red de comunicación multidominio que incluye un primer dominio atribuido a un dispositivo de gestión de los grupos de riesgo compartido ya citados y un elemento de red dispuesto en el exterior de dicho primer dominio, incluyendo dicho elemento de red:

un módulo de comunicación para transmitir en dominios de dicha red solicitudes de determinación de camino entre dominios y para recibir desde dichos dominios de la red mensajes de respuesta relativos a caminos de conexión correspondientes a dichas solicitudes, comprendiendo dichos mensajes de respuesta informaciones de ruta e informaciones de riesgo, comprendiendo dichas informaciones de riesgo ciertos mensajes de respuesta que comprenden dicho identificador del dispositivo de gestión de los grupos de riesgo compartido atribuido al primer dominio y códigos

de identificación de riesgo compartido asociados,

un módulo de análisis de riesgo compartido para analizar dichas informaciones de riesgo recibidas y, en respuesta a la detección de dicho identificador del dispositivo de gestión de los grupos de riesgo compartido para dos caminos de conexión diferentes, trasmitir a dicho dispositivo de gestión de los grupos de riesgo compartido una solicitud de explotación que incluye los códigos de identificación de riesgo compartido asociados a los dos caminos de conexión para determinar un carácter disjunto o no de dichos caminos de conexión.

El invento proporciona igualmente un procedimiento de cálculo de ruta en una red de comunicación multidominio que incluye un primer dominio atribuido a un dispositivo de gestión de los grupos de riesgo compartido ya citados, que incluyen las operaciones consistentes en:

recibir en un segundo dominio de la red una solicitud de determinación de camino que procede de otro dominio de la red, requiriendo dicho dominio, dicha solicitud que tiende a determinar un camino de conexión en dicho segundo dominio, determinar un camino de conexión entre dos nudos del segundo dominio para responder a dicha solicitud,

determinar que una parte del camino de conexión entre los dos nudos del segundo dominio está situada en dicho primer dominio de la red,

obtener de dicho dispositivo de gestión de los grupos de riesgo compartido informaciones de riesgo que incluyen un código de identificación de riesgo compartido atribuido a la parte del camino de conexión situada en el primer dominio y el identificador del dispositivo de gestión de los grupos de riesgo compartido,

y transmitir al dominio que solicita una respuesta a dicha solicitud que incluye informaciones de ruta relativas a dicho camino de conexión y dichas informaciones de riesgo.

Una idea en la base del invento es, en cada dominio de encaminamiento de una red multidominio, enmascarar grupos de riesgo compartido asociados a un camino por un código abstracto asociado a un nudo de referencia del dominio. Sólo el nudo de referencia de un dominio es capaz de extraer los grupos asociados a los códigos, y puede ser contactado para ello en una dirección de la red que está comunicada en los otros

dominios. Así, se ha propuesto una solución que concilia la detección de los conflictos de riesgo y la confidencialidad de los grupos de riesgo compartido de los dominios.

El invento será mejor comprendido, y otros propósitos, detalles, características y ventajas de éste aparecerán más claramente en el curso de la siguiente descripción de varios modos de realización particulares del invento, dados únicamente a título ilustrativo y no limitativo, en referencia a los dibujos adjuntos. En estos dibujos:

La fig. 1 es una representación esquemática funcional de una red multidominio en la que pueden ser empleados los modos de realización del invento.

La fig. 2 es un diagrama de flujo de los mensajes de señalización RSVP-TE que pueden ser empleados en la red de la fig. 1, para establecer una conexión N11-N12.

La fig. 3 es un diagrama de flujo que ilustra el funcionamiento de un gestor de los grupos de riesgo compartido en la red de la fig. 1.

La fig. 4 es una representación de otra red multidominio en la que pueden ser empleados modos de realización del invento.

La fig. 5 es un diagrama de flujo de mensajes de señalización RSVP-TE que pueden ser empleados en la red de la fig. 4 para establecer una conexión N41-N52.

La fig. 6 es un diagrama de flujo de los mensajes PCEP que pueden ser empleados en la red de la fig. 4 para determinar un camino de conexión N41-N52.

La fig. 7 representa un formato de objeto que puede ser utilizado en modos de realización del invento.

Con referencia a la fig. 1, el ejemplo de red de comunicación representado incluye dos dominios de encaminamiento 1 y 2. Por dominio de encaminamiento, se entiende generalmente un conjunto de elementos de red en el que la gestión de las direcciones o el cálculo de los caminos está situado bajo la responsabilidad de una entidad común, y en particular una red que pertenece a un único operador, un sistema autónomo o un grupo de sistemas autónomos, o un área o un grupo de áreas de un protocolo IGP.

El dominio 1 incluye tres nudos N11, N12 y N13, por ejemplo encaminadores IP/MPLS. Una unión entre dominios 14 une los nudos N12 y N13. Ninguna unión entre dominios une los nudos N11 y N12. Los nudos N11 y N12 son encaminadores de a bordo que interconectan el dominio 1 con el dominio 2.

El dominio 2 incluye cuatro nudos N21 a N24. Unas uniones entre dominios

unen los nudos N21 a N24. Los nudos N21 y N24 son encaminadores de a bordo que interconectan el dominio 2 con el dominio 1. Una unión entre dominios 19, respectivamente 29, une los nudos N11 y N21, respectivamente N12 y N24.

La tecnología de transmisión en el dominio 2 puede ser idéntica o diferente del dominio 1. Si las tecnologías de transmisión son diferentes, los dominios 1 y 2 son llamados a pertenecer a dos capas de red diferentes. Una pila protocolaria GMPLS puede ser empleada para desplegar un plan de control unificado sobre capas de red diferentes.

En cada dominio, existe al menos un dispositivo de cálculo de camino 60 que accede al contenido de una base de datos de ingeniería de tráfico 61 para calcular caminos que verifican tensiones particulares en el interior del dominio. El dispositivo de cálculo de camino 60 puede estar integrado en un nudo, por ejemplo un encaminador IP/MPLS, o ser realizado separadamente de los nudos, por ejemplo en forma de un elemento PCE (Elemento de Cálculo de Trayecto). La base de datos de ingeniería de tráfico 61 puede estar configurada manualmente o alimentada por un protocolo de encaminamiento interior como OSPF-TE o IS-IS-TE. Según un modo de realización GMPLS, la base de datos de ingeniería de tráfico 61 incluye una base de datos de estado de las uniones (Base de Datos de Estado de las Uniones) y una base de datos de uniones en ingeniería de tráfico (Base de Datos de Uniones TE).

Se supone también que grupos de riesgo compartido son definidos en cada dominio y que identificadores SRLG ID son atribuidos a los diferentes recursos (uniones, nudos, etc.). Estas atribuciones de grupos de compartimientos de riesgo, que son relativamente estáticas, son almacenadas de manera centralizada o distribuida en al menos un almacenamiento de datos del dominio, por ejemplo en la base de datos de ingeniería de tráfico 61.

Por razones de seguridad o de administración, las informaciones de topología, de conectividad y de grupos de riesgo compartido de un dominio se supone que son conservadas en este dominio. Los dominios tienen pues una visibilidad ilimitada uno sobre el otro. Por ejemplo, el dominio 1 no conoce más que los nudos límite N21 y N24 del dominio 2 y las uniones entre dominios correspondientes 19 y 29.

Se supone que una conexión entre N11 y N12 es deseada en el dominio 1. El dispositivo de cálculo de la ruta 60 del dominio 1 es capaz de determinar que tal conexión puede ser demandada en el dominio 2. Con referencia a la fig. 2, se describe sucintamente un procedimiento de señalización RSVP-TE que puede ser empleado para establecer esta conexión LSP (Etiqueta de Trayecto Conmutado).

En la fig. 2, en la etapa 62, el nudo N11 envía al nudo N21 un mensaje de petición de conexión PATH que incluye las características de la conexión a establecer (por ejemplo banda pasante requerida) y el destino N12. La ruta no puede ser completamente explicitada en este estado por el dominio 1. El mensaje PATH incluye por tanto un camino incompleto (salto perdido) y un Objeto de Grabación de Ruta (RRO) para pedir la grabación del camino seguido, según la técnica conocida. El camino de conexión que debe ser seguido en el dominio 2 es determinado en el interior del dominio 2, bien por un cálculo centralizado efectuado por el nudo N21 o un PCE, bien por decisiones de los nudos (encaminamiento salto por salto). Se supone que el camino que resulta de ello es en el N21-N22-N23-N24-N12, el nudo N12 responde al mensaje PATH por un mensaje de reserva RSEV en el que el objeto RRO es completado por los nudos sucesivos para informar al nudo N11 iniciador del camino. Sin embargo como el camino atraviesa dos dominios, los saltos intermedios en el dominio 2 no son comunicados necesariamente a N11 y pueden ser reemplazados por un código Clave de Trayecto PKS según la técnica conocida.

Antes de transmitir el mensaje RSEV con el objeto RRO al dominio 1, el nudo 21 añade informaciones de riesgo relativas a los recursos de comunicación del dominio 2 utilizadas por la conexión. Para ello, el dominio 2, incluye un gestor de los grupos de riesgo compartido 27, que puede ser realizado de manera integrada en un nudo o en un PCE o de manera separada. Su funcionamiento está explicado con referencia a la fig. 3.

El gestor 27 está encargado de varias tareas. Determina qué grupos de riesgo compartido del dominio 2 son atravesados por la conexión. Para ello, utiliza una descripción del camino de conexión, proporcionada por ejemplo por el nudo 21 (fig. 3 operación 64). Luego accede a las atribuciones del grupo de riesgo compartido (SRLG ID) de los recursos, por ejemplo en la base de datos 61. Luego atribuye una o varias claves de riesgo compartido a la conexión (diferentes de las claves ya atribuidas por él a otras conexiones) y graba, en un almacenamiento de datos 28, una estructura de datos que asocia la o las claves de riesgo compartido con los grupos de riesgo compartido del dominio 2 que son atravesados por la conexión (operación 65). Finalmente retransmite al nudo 21 las informaciones de riesgo, designadas SRK, que deben ser añadidas al mensaje RESV (operación 66). Estas informaciones son la o las claves de riesgo compartido y una dirección de red del gestor 27, que permite a elementos situados en otros dominios de la red interrogar al gestor 27, como se describirá más abajo. El almacenamiento de datos 28 puede estar y eventualmente integrado en la base de datos

de ingeniería de tráfico 61 del dominio.

La fig. 7 representa un formato que puede ser utilizado para transportar las informaciones de riesgo relativas a la conexión. Este formato consiste en un objeto 67, denominado por ejemplo SRKO para Clave de Riesgo Compartido, que contiene un subobjeto 68 para almacenar la dirección de red del gestor 27 y un subobjeto 69 para almacenar la o las claves de riesgo compartido. El subobjeto 68, denominado por ejemplo Dirección de Nudo de Referencia, puede ser similar a la sección 4.1 del proyecto de Internet «draft-ietf-pce-disco-proto-ospf-08». El subobjeto 69, denominado por ejemplo SRLG, puede ser conforme a la sección 2.1 de la RFC4874.

De vuelta a la fig. 2, el nudo 11 recibe por tanto un mensaje de RSEV en el que el RRO incluye el objeto SRKO. Un LSP 70 (fig. 1) está por tanto establecido entre N11 y N12. En el dominio 1, el LSP 70 puede ser considerado como una unión virtual entre el nudo de entrada N11 y el nudo de salida N12 y ser utilizado como un túnel para transportar conexiones ulteriores. Para ello, en la operación 71, el controlador de encaminamiento del nudo N11 difunde un mensaje de anuncio de unión en el dominio 1, lo que permite grabar esta unión virtual en la base de datos 61 en asociación con el objeto SRKO. Por ejemplo, el mensaje de anuncio de unión puede ser transmitido con el protocolo OSPF-TE o IS-IS-TE. Para transportar el objeto SRKO, Los mecanismos protocolarios existentes para transportar y almacenar los SRLG ID pueden ser reutilizados, véase por ejemplo la sección 5,2 del proyecto de Internet «draft-papadimitriou-ccamp-selg-processing-02», de junio de 2003.

La descripción precedente sigue siendo válida para un LSP cuyas extremidades no serían nudos límite del dominio 1.

En la base de datos 61 del dominio 1, puede que no se almacene en ninguna información de ruta que indique que el LSP 70 atraviesa el dominio 2, sino solamente las extremidades de la conexión. Sin embargo, guardando el objeto SRKO asociado al LSP, sigue siendo posible detectar, en el dominio 2 o en otro dominio, problemas de riesgo compartido que se producen en el dominio 1. Este punto va a ser ilustrado a continuación con referencia a la fig. 4.

La fig. 4 representa otra red multidominio que incluye dominios 1 a 5. Las cifras de referencia idénticas a las de la fig. 1 designan elementos idénticos o similares. En este ejemplo, los dominios 1, 3, 4 y 5 pertenecen a una capa de red 10, por ejemplo de tipo IP/MPLS, mientras que el dominio 2 pertenece a otra capa 20, por ejemplo una capa de transporte de tipo SDH u otra. Los nudos N21 a N24 son nudos multi-servicio unidos a la

capa 10 y capaces de adaptar las señales a las dos tecnologías de transporte. En la capa 20 se han representado por separado controladores de nudos 75 para cada nudo, por ejemplo para formar un plano de control GMPLS.

En la fig. 4, se supone que el nudo N41 del dominio 4 debe establecer dos LSP disjuntos, en términos de riesgo para unir el nudo N52 del dominio 5. Unos caminos entre dominios disjuntos pueden ser necesarios por ejemplo por motivos de protección o de distribución de carga. Como los dominios no tienen más que una visibilidad ilimitada unos sobre otros, no es posible en general determinar una ruta completa al nivel del dominio 5. Es por tanto generalmente necesario dejar que varios dominios calculen partes sucesivas del camino. La fig. 5 representa a título de ejemplo un procedimiento RSVP-TE para establecer un LSP 80 de esta manera.

En la fig. 5, se supone que el nudo N41 sabe que el LSP debe partir hacia el nudo N11 del dominio 1, por ejemplo gracias a informaciones de conectividad entre dominios difundidas a la escala de la red. En la operación 81, el nudo N41 envía al nudo N43 un mensaje de petición de conexión PATH que incluye las características de la conexión a establecer (por ejemplo banda pasante requerida) y el destino N52. El mensaje PATH incluye un objeto de Grabación de Ruta (RRO) para pedir la grabación del camino seguido, según la técnica conocida. El mensaje PATH alcanza el nudo límite N11 en el dominio 1, lo que provoca un cálculo de camino entre dominios en el dominio 1 ya que el camino no está explicitado (operación 82). El resultado de este cálculo es por ejemplo hacer pasar la conexión en el LSP 70 hasta el nudo N12 y en la unión 14 hasta el nudo N13. El mensaje PATH es por tanto transmitido en el túnel 70 como si se tratara de un solo salto (operación 83). El mensaje PATH alcanza a continuación el nudo límite N53 del dominio 5 y finalmente el nudo 52. Lo mismo que en la fig. 2, el mensaje RESV graba el camino en el sentido inverso en un objeto RRO, pero algunos saltos pueden ser enmascarados, por ejemplo el nudo N12 que no es un nudo límite. En la operación 85 antes de transmitir el mensaje RESV con el objeto RRO al dominio 4, el nudo límite N11 añade a él informaciones de riesgo relativas a los recursos de comunicación del dominio 1 utilizadas por la conexión. Para ello, el nudo N11 puede solicitar a un gestor de los grupos de riesgo compartido 17 similar al gestor 27 del dominio 2. El procedimiento descrito más arriba es repetido por tanto, pero a partir de las informaciones del grupo de riesgo compartido relativas a los recursos del dominio 1 para formar un objeto SRKO apropiado para el dominio 1. En las atribuciones del grupo de riesgo compartido, en lo que concierne a la unión 70, el gestor 17 encuentran el objeto SRKO que ha sido recibido desde el

dominio 2 y almacenado. El gestor 17 debe insertar este objeto sin modificación en el objeto RRO que sale del dominio 1, lo que permite guardar una información de riesgo que significa indirectamente que el dominio 2 está implicado en la conexión. En lo que se refiere a las informaciones de ruta, el RRO no contiene normalmente ninguna indicación relativa al dominio 2 en este caso ya que el túnel 70 es empleado. Finalmente, el mensaje de reserva alcanza el nudo iniciador N41 y el LSP 80 es por tanto establecido.

Para establecer un segundo LSP si el dominio 4 no tiene generalmente bastante información para especificar previamente un camino disjunto del LSP 80, dispone sin embargo de las informaciones de conectividad entre dominios que permiten saber que una ruta es susceptible de existir a través del dominio 3. Un comienzo lógico para encontrar un camino disjunto sería por tanto pedir el establecimiento del segundo LSP a través del dominio 3, pidiendo de excluir los nudos de los dominios 4 y 5 utilizados por el LSP 80. Sin embargo si el dominio 3 posee como el dominio 1, un túnel 86 en el dominio 2, el resultado no será necesariamente un LSP disjunto en términos de riesgo, como se ha ilustrado por el LSP 90 en la fig. 4. En efecto, un riesgo compartido existe sobre la unión N22-N23, como se ha representado en la cifra 100.

Sin embargo, si el establecimiento del LSP 90 sigue un procedimiento similar al descrito para el LSP 80 y un gestor de los grupos de riesgo compartido 87 es desplegado de la misma manera en el dominio 3, este riesgo compartido va a poder ser detectado por el nudo 41. En efecto, en el objeto RRO del LSP 90, el nudo N41 recibe también un objeto SRKO que emana del gestor 27 del dominio 1. Para determinar si los LSP 80 y 90 son disjuntos en términos de riesgos, el nudo N41 u otro elemento de red del dominio 4 incluye un controlador 88 de análisis de riesgo compartido que compara las informaciones de riesgo disponibles relativas a los dos LSP. Comparando los dos objetos SRKO, el controlador de análisis va a detectar la misma dirección de gestor en el subobjeto 68. En respuesta a esta detección, transmite a esta dirección, es decir al gestor 27 del dominio 2, una solicitud de verificación del carácter disjunto en la que incluye los subobjetos 69, es decir las llaves de riesgo compartido de los dos LSP.

En respuesta a esta solicitud de verificación, el gestor 27 desarrolla las claves de riesgo compartido, es decir extrae del almacenamiento de datos 28 los grupos de riesgo compartido del dominio 2 a los que son asociadas estas claves, y puede así determinar si las claves vuelven a enviar a grupos enteramente disjuntos o no. Una respuesta correspondiente, negativa en este ejemplo, es transmitida al emisor de la solicitud de verificación.

Otra utilización posible del objeto SRKO es insertarlo en un objeto XRO (Excluir Objeto de Ruta) del protocolo RSVP-TE para especificar grupos de riesgo compartido que deben ser evitados por la conexión, por analogía con la sección 3.1.5 de la RFC4874, o en un objeto ERO (Explicitar Objeto de Ruta) para especificar grupos de riesgo compartido que deben ser atravesados por la conexión.

Las comunicaciones de informaciones de ruta y de riesgo entre los dominios, que han sido descritas anteriormente en forma de mensaje de señalización intercambiadas por controladores de señalización de los nudos, pueden también ser efectuadas entre elementos de cálculo de camino PCE unidos a cada dominio y que cooperan para calcular una ruta entre dominios. En este caso, el protocolo PCEP es empleado. Un objeto SRKO puede ser transportado en un objeto ERO, en la respuesta de camino calculada por uno o una cadena de PCE como consecuencia de una solicitud por el protocolo PCEP. La fig. 6 ilustra tal modo realización en un caso en el que el dominio 4 busca calcular una ruta entre dominios para él LSP 80, antes de pedir su establecimiento.

De preferencia, un gestor de los grupos de riesgo compartido está asociado a cada dominio de encaminamiento de la red. Puede estar previsto un gestor por dominio de encaminamiento. Sin embargo, el dominio de responsabilidad de un gesto de los grupos de riesgo compartido puede también englobar varios dominios de encaminamiento, por ejemplo para varios operadores que tienen un acuerdo de cooperación para asegurar esta funcionalidad de manera común.

Ciertos de los elementos representados o descritos, en particular los controladores, los gestores de los grupos de riesgo compartido y otros módulos, pueden ser realizados en formas diferentes, de manera unitaria o distribuida, por medio de componentes materiales y/o de programación. Unos componentes materiales utilizables son los circuitos integrados específicos ASIC, las redes lógicas programables FPGA o los microprocesadores. Unos componentes de programación pueden ser escritos en diferentes lenguajes de programación, por ejemplo C, C++, Java o VHDL. Esta lista no es exhaustiva.

Aunque el invento ha sido descrito en unión con varios modos de realización particulares, es bien evidente que no está en ninguna forma limitada a ellos y que comprende todos los equivalentes técnicos de los medios descritos así como sus combinaciones si éstas entran en el marco del invento. En particular, el número y la topología de las uniones, de los nudos, de los dominios y de las capas de red que aparecen en las figuras son puramente ilustrativos y no limitativos.

El uso del verbo “incluir”, “comprender” o “contener” y de sus formas conjugadas no excluye la presencia de otros elementos o de otras operaciones que los enunciados en una reivindicación. El uso del artículo indefinido “un” o “una” para un elemento o una operación no excluye, salvo mención contraria, la presencia de una pluralidad de tales elementos u operaciones. Varios medios o módulos pueden ser representados por un mismo elemento material.

En las reivindicaciones, cualquier signo de referencia entre paréntesis no debería ser interpretado como una limitación de la reivindicación.

**REIVINDICACIONES**

1.- Un procedimiento para comunicar una información de riesgo en una red que incluye una pluralidad de dominios interconectados al nivel de nudos límite de dichos dominios, caracterizado por las operaciones que consisten en:

determinar un camino de conexión en un primer dominio (2), extendiéndose dicho camino entre un nudo límite (N21) del primer dominio conectado a un segundo dominio y un nudo de destino; determinar un conjunto de grupos de riesgo compartido del primer dominio que son atravesados por dicho camino de conexión; atribuir un código (69) de identificación de riesgo compartido a dicho camino de conexión; almacenar, en un dispositivo (28) de gestión de los grupos de riesgo compartido asociado al primer dominio, asociar una estructura de datos dicho código de identificación de riesgo compartido con dicho conjunto de grupos de riesgo compartido, y transmitir al segundo dominio informaciones de ruta relativas a dicho camino de conexión e informaciones de riesgo, incluyendo dichas informaciones de riesgo dicho código (69) de identificación de riesgo compartido, **caracterizado por que** dicho nudo de destino es otro nudo límite (N24) del primer dominio conectado al segundo dominio, incluyendo el procedimiento las operaciones consistentes en:

establecer una conexión entre dos nudos de dicho segundo dominio, atravesando dicha conexión dicho primer dominio a lo largo de dicho camino de conexión, y grabar en una base de datos de encadenamiento del segundo dominio una unión (70) correspondiente a dicha conexión y capaz de ser utilizada como un túnel para transportar conexiones ulteriores, incluyendo dichos registros de unión informaciones de riesgo (68, 69), comprendiendo dichas informaciones de riesgo también un identificador del dispositivo (68) de gestión de los grupos de riesgo compartido que permite interrogar a dicho dispositivo para explotar dicho código de identificación de riesgo compartido.

2.- un procedimiento según la reivindicación 1, **caracterizado por que** la determinación del camino de conexión es efectuada en respuesta a la recepción de una solicitud de determinación de camino que procede del segundo dominio.

3.- Un procedimiento según la reivindicación 2, **caracterizado por que** dicha solicitud de determinación de camino incluye tensiones o restricciones de ingeniería de tráfico y porque el camino de conexión es determinado para satisfacer dichas tensiones de ingeniería de tráfico.

4.- Un procedimiento según la reivindicación 2, **caracterizado por que** dicha solicitud de determinación de camino es recibida en un mensaje de señalización (62) que tiende al establecimiento de una conexión entre dicho nudo límite del primer dominio y dicho nudo de destino y porque dichas informaciones de ruta en informaciones de riesgo son transmitidas en un mensaje de señalización que confirma el establecimiento de dicha conexión.

5.- Un procedimiento según la reivindicación 2, **caracterizado por que** dicha solicitud de determinación de camino es recibida por un elemento de cálculo de camino del primer dominio en un mensaje de solicitud del protocolo PCEP, y porque dichas informaciones de ruta e informaciones de riesgo, son transmitidas por dicho elemento de cálculo de camino del primer dominio en un mensaje de respuesta del protocolo PCEP.

6.- Un procedimiento según la reivindicación 1, caracterizado **por que** dicha conexión entre dos nudos del segundo dominio es una conexión de la capa de cliente que está imbricada en una conexión de la capa de servidor.

7.- Un procedimiento según la reivindicación 1, **caracterizado por que** el segundo dominio pertenece a una capa de red de cliente (10) que incluye una pluralidad de nudos unidos a uniones de comunicación de un tipo cliente y porque el primer dominio (2) pertenece a una capa de red de servidor (20) que incluye una pluralidad de nudos conectados a uniones de comunicación de un tipo de servidor diferente del tipo de cliente, incluyendo dichas interfaces de interconexión entre el primer dominio y el segundo dominio módulos de adaptación para adaptar señales del tipo servidor al tipo cliente y para adaptar señales del tipo cliente al tipo servidor.

8.- Un procedimiento según la reivindicación 1, **caracterizado por que** consiste en difundir (71) por medio de un protocolo de encaminamiento interior del segundo

dominio, un anuncio de unión que se refiere a dicha conexión establecida entre los nudos de dicho segundo dominio, incluyendo dicho anuncio de unión dichas informaciones de riesgo.

9.- Un procedimiento según la reivindicación 1, **caracterizado por que** el identificador del dispositivo de gestión de los grupos de riesgo compartido incluye una dirección IP.

10.- Un procedimiento según la reivindicación 1, **caracterizado por que** el código de identificación de riesgo compartido y el identificador del dispositivo de gestión de los grupos de riesgo compartido son transmitidos en dos campos de un mismo objeto.

11.- Una base de datos de ingeniería de tráfico (61) para un dispositivo de cálculo de camino de un segundo dominio (1), **caracterizado por que** incluye un registro de una unión (70) entre dos nudos (N11, N12) de dicho segundo dominio, correspondiendo dicha unión a una conexión establecida entre dichos dos nudos y que atraviesa un primer dominio (2) a lo largo de un camino de conexión, siendo apta dicha unión para ser utilizada como un túnel para transportar conexiones ulteriores, estando asociado dicho registro de unión a informaciones de riesgo que incluyen:

un código (69) de identificación de riesgo compartido atribuido a dicho camino de conexión del primer dominio (2) y un identificador (68) de un dispositivo de gestión de los grupos de riesgo compartido asociado al primer dominio (2), incluyendo dicho dispositivo (28) de gestión de los grupos de riesgo compartido una estructura de datos que asocia dicho código de identificación de riesgo compartido con un conjunto de grupos de riesgo compartido que son atravesados por dicho camino de conexión del primer dominio (2).

12.- Un elemento de cálculo de camino PCE para calcular caminos en el interior de un segundo dominio (1), **caracterizado por que** es apto para tener acceso al contenido de una base de datos (61) de ingeniería de tráfico según la reivindicación 11, siendo dicho elemento de cálculo de camino apto para:

calcular un camino en dicho segundo dominio, pasando dicho camino por dicha

unión que atraviesa el primer dominio, y emplear el protocolo PCEP para transmitir una respuesta de camino a otro dominio (4), incluyendo dicha respuesta de camino informaciones de ruta y de riesgo relativas a los recursos de comunicación utilizados por dicho camino en el segundo dominio, incluyendo dichas informaciones de riesgo dicho código (69) de identificación de riesgo compartido y dicho identificador (68) del dispositivo de gestión de los grupos de riesgo compartido asociados al registro de unión.

13.- Un controlador de encadenamiento para un nudo de conmutación (N11) de un dominio (1), **caracterizado por que** es apto para tener acceso al contenido de una base de datos (61) de ingeniería de tráfico según la reivindicación 11, y porque es apto para difundir (71) por medio de un protocolo de encaminamiento interior de dicho segundo dominio un anuncio de unión que se refiere a dicha unión que atraviesa el primer dominio, incluyendo dicho anuncio de unión informaciones de riesgo que incluye en dicho código (69) de identificación de riesgo compartido y dicho identificador (68) del dispositivo de gestión de los grupos de riesgo compartido asociados al registro de unión.

14.- Un procedimiento para establecer una conexión entre dominios **caracterizado por que** incluye las operaciones de:

recibir un mensaje de solicitud de conexión en un segundo dominio (1), incluyendo dicho segundo dominio (1) una base de datos (61) de ingeniería de tráfico según la reivindicación 11, y un dispositivo de cálculo del camino que tiene acceso a dicha base de datos de ingeniería de tráfico, procediendo dicho mensaje de solicitud de conexión de otro dominio (4), determinar un camino de conexión en el segundo dominio (1), pasando dicho camino por dicho unión (70) que atraviesa el primer dominio grabado en la base de datos de ingeniería de tráfico, transmitir dicho mensaje de petición de conexión en el segundo dominio (1) a lo largo de dicho camino de conexión, transmitir un mensaje de reserva en el segundo dominio (1) a lo largo de dicho camino de conexión en sentido inverso al de dicho mensaje de solicitud de conexión, y transmitir dicho mensaje de reserva hacia dichos otros dominios (4), incluyendo dicho mensaje de reserva trasmitido a dicho otro dominio informaciones de riesgo relativas a los recursos de comunicación utilizados por dicho camino de conexión en el segundo dominio, incluyendo dichas informaciones

de riesgo, en lo que se refiere a dicha unión que atraviesa el primer dominio, dicho código (69) de identificación de riesgo compartido y dicho identificador (68) del dispositivo de gestión de los grupos de riesgo compartido asociados al registro de unión.

15.- Un procedimiento según la reivindicación 14 **caracterizado por que** las informaciones de riesgo son transmitidas en un objeto de Grabar Ruta del protocolo RSVP-TE.

FIG_1

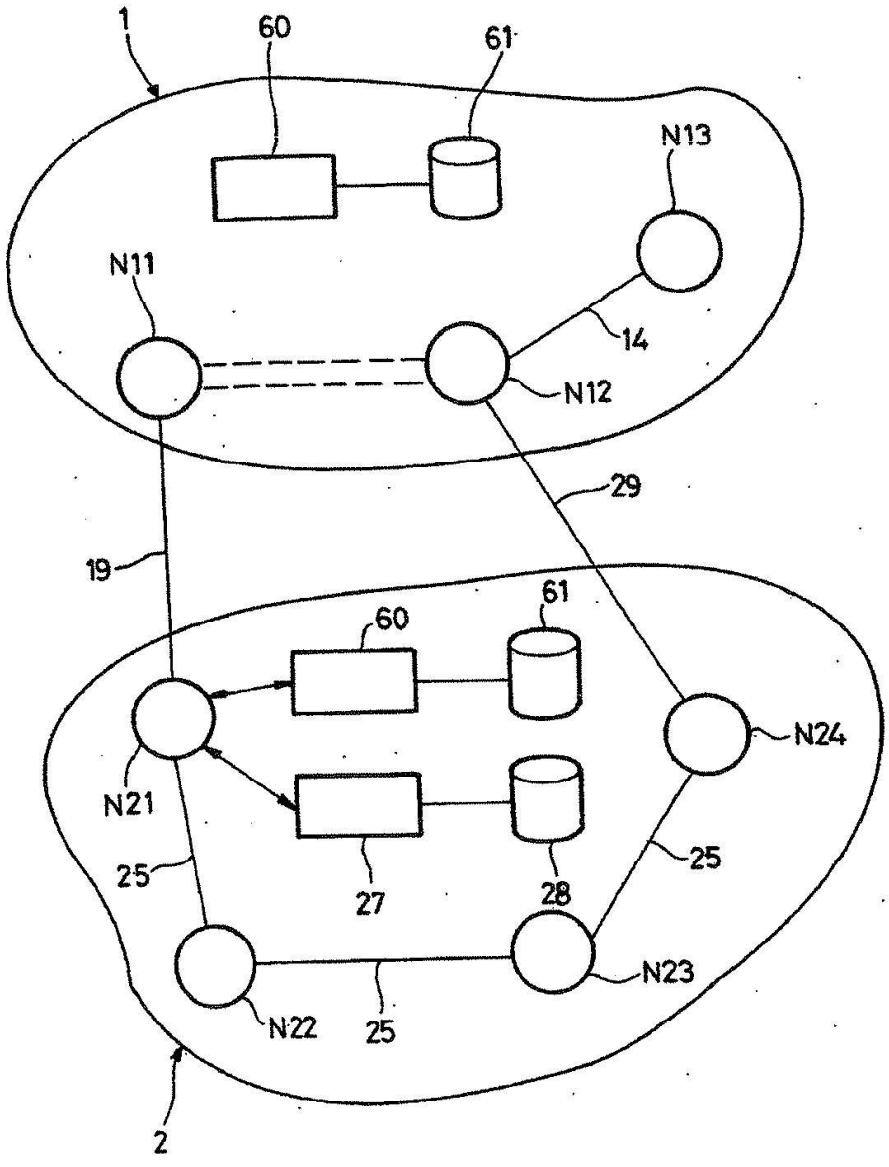


FIG_2

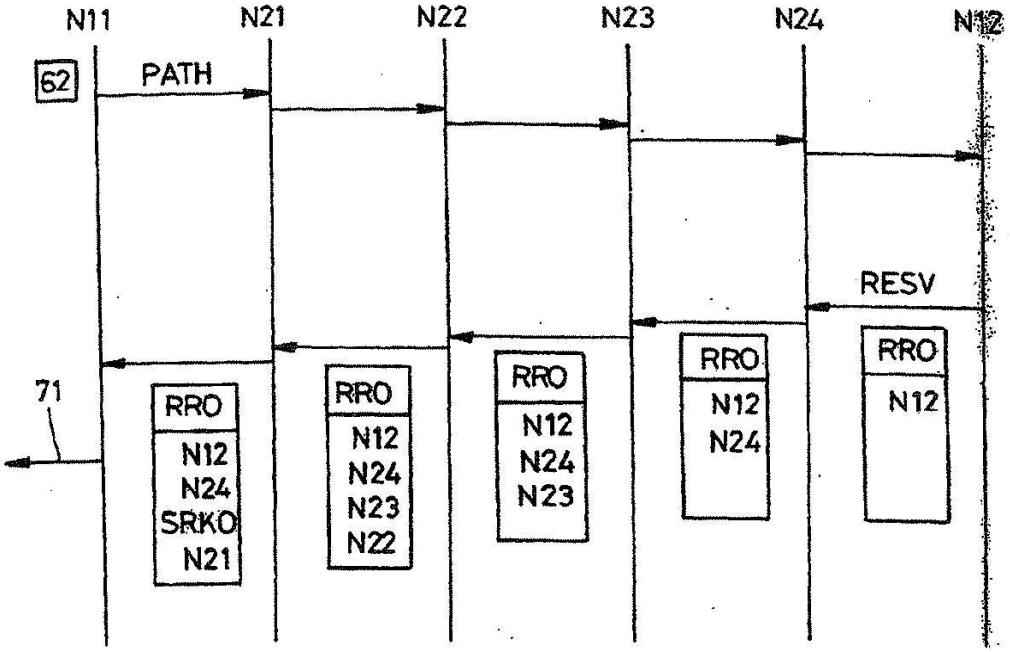
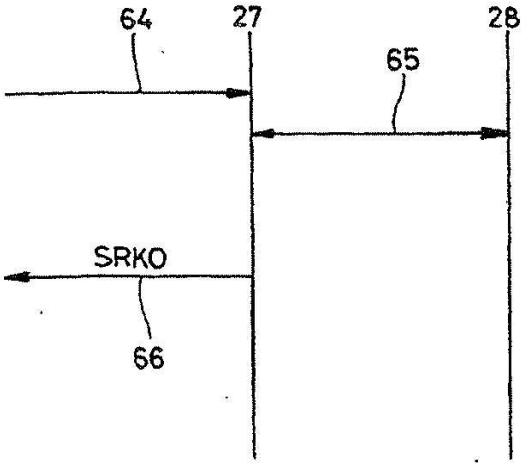

N11
N21
N22
N23
N24
N12
62
PATH
RESV
71
RRO
N12
N24
SRKO
N21
RRO
N12
N24
N23
N22
RRO
N12
N24
N23
RRO
N12
N24
RRO
N12

FIG_3


64
27
28
65
SRKO
66

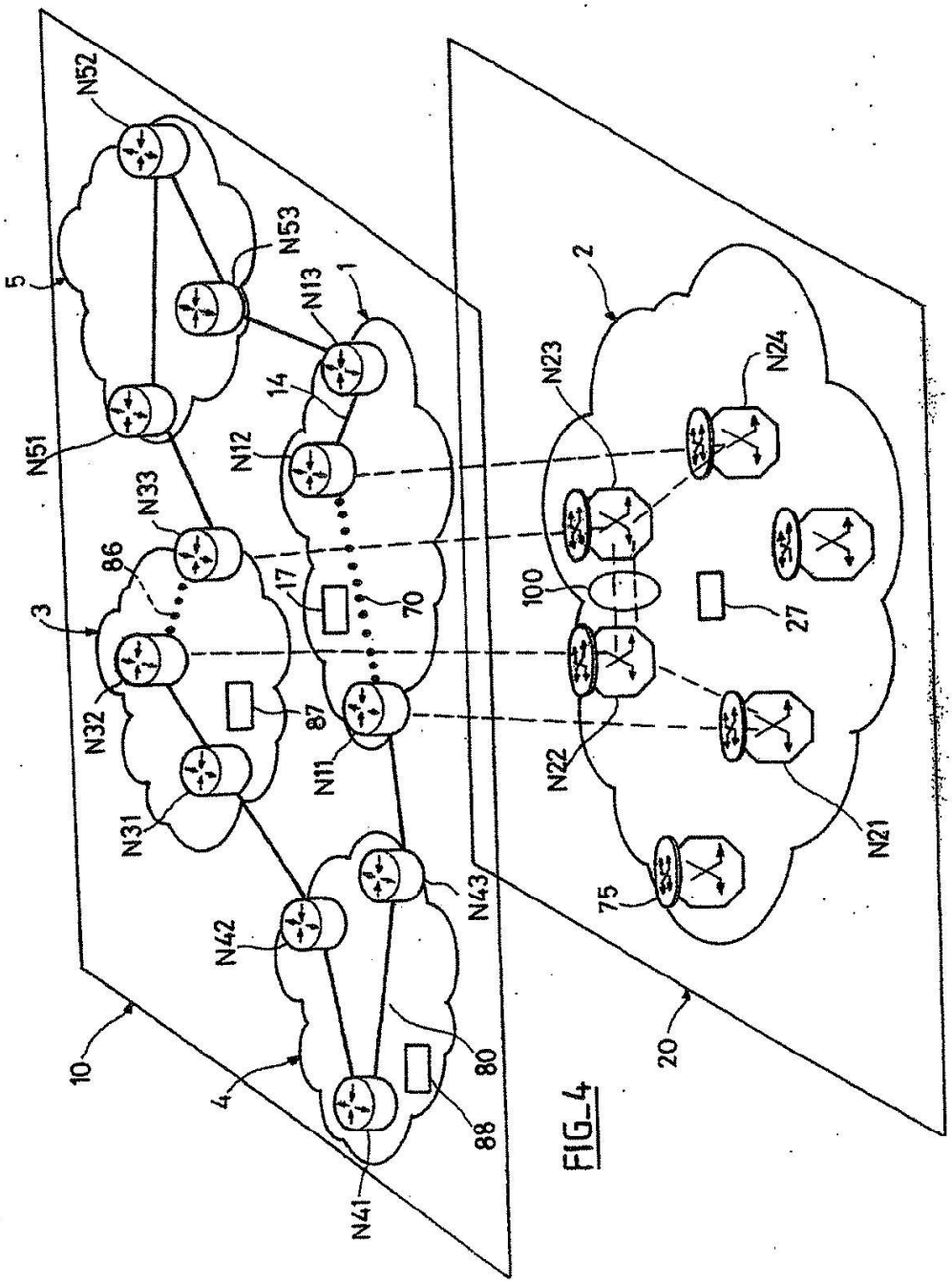

N52
N53
N13
1
5
14
N51
N12
N33
86
17
70
3
N32
87
N11
N31
N42
N43
80
88
N41
10
4
2
N23
N24
100
27
N22
N21
75
20

FIG_4

FIG_5

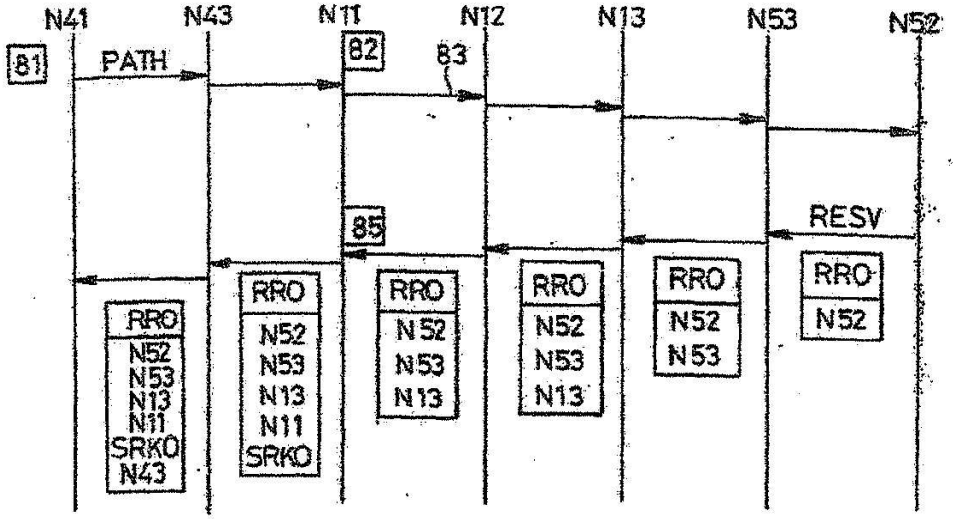



FIG_6

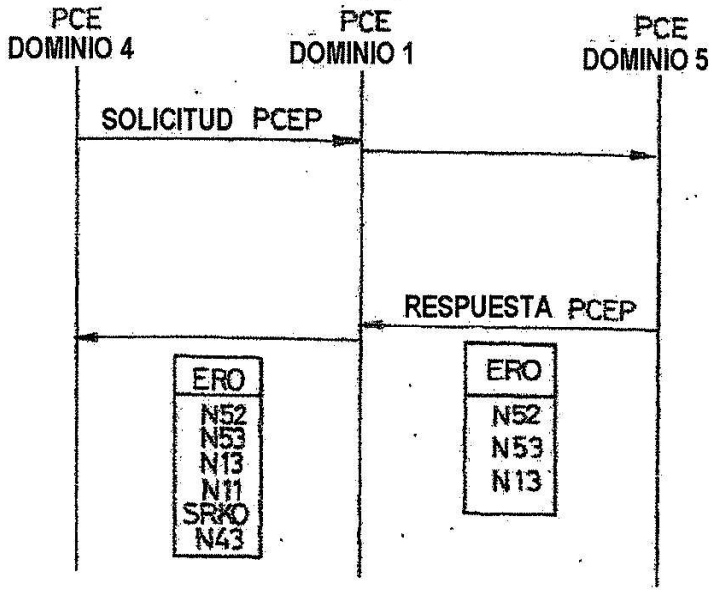



FIG_7