(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 322 241**

(51) Int. Cl.:
H04L 12/46 (2006.01)
H04L 12/28 (2006.01)
H04L 29/14 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **02026538 .5**
(96) Fecha de presentación : **27.11.2002**
(97) Número de publicación de la solicitud: **1394995**
(97) Fecha de publicación de la solicitud: **03.03.2004**

(54) Título: **Configuración de red redundante.**

(30) Prioridad: **28.08.2002 EP 02019298**
28.08.2002 EP 02019297

(45) Fecha de publicación de la mención BOPI:
18.06.2009

(45) Fecha de la publicación del folleto de la patente:
18.06.2009

(73) Titular/es:
Nokia Siemens Networks GmbH & Co. KG.
St. Martin Strasse 76
81541 München, DE

(72) Inventor/es: **Arnold, Robert;**
Hertlein, Thomas y
Stademann, Rainer

(74) Agente: **Zuazo Araluze, Alexander**

DESCRIPCIÓN

Configuración de red redundante.

Los sistemas de comunicaciones de alta fiabilidad exigen la utilización de rutas de mensajes redundantes, con lo que una avería de una ruta de mensajes individual no da lugar a limitaciones en la comunicación. La redundancia de las rutas de mensajes, es decir, la existencia para cada ruta de mensajes de al menos una ruta de mensajes sustitutoria, a la que puede conmutarse en caso de avería, debe ser apoyada entonces por las plataformas de service o bien servidores (hosts), al igual que por el propio sistema de comunicaciones, es decir, por sus elementos, por ejemplo conmutadores y enrutadores, y por su estructura.

Para sistemas de comunicaciones con exigencias de tiempo real, por ejemplo en el caso de la transmisión de voz, son además de gran importancia tiempos muy cortos para la conmutación de una ruta de mensajes averiada a una ruta de mensajes sustitutoria, para limitar a un mínimo las repercusiones negativas sobre el servicio cuando falla una ruta de mensajes.

Las averías a considerar incluyen fallos totales y/o fallos parciales en elementos individuales del sistema de comunicaciones, por ejemplo plataforma de service, conmutadores, enrutadores y fallos de los enlaces entre los distintos elementos.

Un sistema de comunicaciones muy frecuente en la práctica está compuesto por uno o varios servidores (hosts) o bien plataformas de service, que están conectados a través de una red, al menos una LAN (LAN = Local Area Network, red de área local) y dos pasarelas (gateways), a una red IP (IP = Internet Protocol, protocolo de Internet).

Una configuración de red redundante para conectar varios servidores (hosts) con pasarelas (gateways) se describe en la solicitud de patente europea 02019298 con el título “Configuración de red redundante” de la misma solicitante. Un procedimiento de comprobación para configuraciones de red, en particular para configuraciones de red redundantes según 02019298, se describe en la solicitud de patente europea 02019297 con el título “Procedimiento de comprobación para rutas de mensajes en redes de comunicaciones, así como elemento de red” de la misma solicitante.

Las soluciones descritas en las citadas solicitudes de patente 02019297 y 02019298 son adecuadas especialmente para la utilización con redes locales, es decir, para hosts y gateways no muy distanciados espacialmente.

El documento EP 0 924 901 A2 da a conocer una interfaz Ethernet Gigabit hacia un anillo de red síncrona (SONET).

Se describe un procedimiento y un dispositivo para transmitir paquetes de datos con ayuda de SONET de aparatos terminales, que están conectados a una LAN, a aparatos terminales que están conectados a otra LAN.

El documento “Point to point label switching protocol for optical access networks” (protocolo de conmutación de etiquetas punto a punto para redes de acceso ópticas), Jungloon Lee y colab., IEEE, vol. 1 OF2, 19 agosto 2001 se concentra en la puesta a disposición de servicios con ayuda de PPP (Point to Point Protocol, protocolo punto a punto) y MPLS (Multiprotocol Label Switching, conmutación de etiquetas multiprotocolo) en IP sobre redes de acceso DWDM (Dense Wavelength Division Multiplexing, multiplexado denso por división de longitudes de onda).

Es una tarea de la presente invención indicar una configuración de red redundante que pueda utilizarse con elementos de red muy alejados espacialmente. Al respecto, debe posibilitar la configuración de red una detección rápida de rutas de mensajes averiadas y una rápida conmutación a rutas de mensajes no averiadas.

Esta tarea se resuelve mediante una configuración de red según las características de la reivindicación 1.

Formas de ejecución preferentes son objeto de las reivindicaciones subordinadas.

Según la presente invención, se prevé una configuración de red para una red de comunicaciones N que conecta un primer equipo servidor (host) y un segundo equipo G0,

- compuesto por una primera subred N_0 y al menos una segunda subred N_1,
- estando compuesta la primera subred (N_0) por primeros elementos de conmutación S_{00}, S_{01}, S_{02}, y estando compuesta la segunda subred N_1 por segundos elementos de conmutación S_{10}, S_{11}, S_{12}, y
- estando configuradas la primera y la segunda subred independientes entre sí,
- con al menos una conexión transversal Q_1 entre las subredes N_0, N_1 y
- con al menos un primer enlace L_{00} entre la primera subred y una primera interfaz IF0 del primer equipo host y al menos un segundo enlace L_{10} entre la segunda subred y una segunda interfaz IF1 del primer equipo host y con al menos un tercer enlace L_{03} entre la primera subred y el segundo equipo G0,

- estando configurados enlaces L_{01}, L_{02} entre los primeros elementos de conmutación S_{00}, S_{01}, S_{02}, y/o enlaces L_{11}, L_{12} entre los segundos elementos de conmutación S_{10}, S_{11}, S_{12}, y/o la(las) conexión(es) transversales Q_1 como enlaces de tráfico de larga distancia WAN.

Una ventaja esencial de la invención ha de considerarse que es que cuando se conectan varios equipos host con el segundo equipo G0 mediante la configuración de red correspondiente a la invención N, cada equipo host presenta a través de en cada caso dos interfaces IF0, IF1, dos rutas de mensajes redundantes hacia el segundo equipo G0. Una de las rutas de mensajes discurre entonces a través de la conexión transversal Q_1 entre las dos subredes redundantes, discurriendo la otra dentro de una subred.

Para el ejemplo de ejecución preferente, en el que se forman las rutas de mensajes mediante una red N entre un host y una gateway G0, puede utilizarse por razones de fiabilidad ventajosamente una segunda gateway G1. De esta manera se evita que cuando falla la gateway averiada G0 se produzca un aislamiento de toda la red N.

En combinación con la segunda gateway G1 resultan ventajosamente varias rutas de mensajes, que posibilitan la comunicación entre hosts y al menos una de las gateways G0, G1 incluso cuando hay averías en rutas de mensajes individuales debido a enlaces averiados o elementos de conmutación averiados.

Una ventaja adicional reside en que mediante la(las) conexión(es) transversal(es) Q_1 entre las subredes N_0 y N_1, pueden comunicarse entre sí varios hosts independientemente de las gateways, incluso cuando diversas interfaces de los hosts estén activas. Por ejemplo, puede intercambiar mensajes a través de la(s) conexión(es) transversal(es) un primer host con la primera interfaz activa, en conexión con la primera subred N_0, con un segundo host con una segunda interfaz activa, en conexión con la segunda subred N_1. Esto no sería posible sin la conexión transversal correspondiente a la invención.

Frente a soluciones en las que solamente se utilizan Local Area Networks LAN (redes de área local) para conectar el primer equipo host y los otros equipos G0, G1, posibilita la utilización según la invención de enlaces de tráfico de larga distancia (Wide Area Network WAN) distancias espaciales bastante superiores entre los citados equipos. Esto es por ejemplo ventajoso cuando se emplaza uno de los equipos de gateway redundantes G0, G1 en un lugar alejado, por ejemplo para reducir costes, para aumentar la seguridad y/o la disponibilidad.

Además es ventajoso que la configuración de red correspondiente a la invención facilite considerablemente la administración de toda la red, ya que puede llegarse a muchos hosts distribuidos en grandes superficies desde los equipos de gateway G0, G1 emplazados centralmente, a través de sólo una subred individual de IP. Esto minimiza la probabilidad de una administración incorrecta y aumenta la fiabilidad.

Para la comprobación de las rutas de mensajes puede utilizarse sin modificaciones un procedimiento de comprobación ventajoso para rutas de mensajes en redes de comunicaciones, ya que los tramos de tráfico de larga distancia de la red de comunicaciones retransmiten de manera transparente las tramas o bien paquetes a transportar de las redes N_0, N_1 o bien N_{01}, N_{02}, N_{11}, N_{12} y con ello no se ve influida la comprobación punto-a-punto de las rutas entre host y gateway(s) G0, G1.

A continuación se describirá la invención más en detalle en relación con tres figuras como ejemplo de ejecución.

Figura 1A representa esquemáticamente la conexión de un equipo host a un equipo de gateway a través de una red redundante.

Figura 1B muestra posibles rutas de mensajes en una red redundante según la figura 1A.

Figura 2A muestra esquemáticamente la conexión redundante de un equipo host a un equipo de gateway local y mediante un enlace de tráfico de larga distancia, a un equipo de gateway alejado.

Figura 2B muestra esquemáticamente la conexión redundante de un equipo host a equipos de gateway alejados mediante una conexión de red de larga distancia.

Figura 3B muestra esquemáticamente la conexión redundante de un equipo host con equipos de gateway alejados mediante Resilient Packet Ring (anillo de paquetes con protección).

En la figura 1 se representa un primer equipo host. Este primer equipo puede ser por ejemplo uno de los equipos host o plataformas de service citados al principio. No obstante, el primer equipo puede ser un equipo de comunicación cualquiera con capacidades de comunicación de la capa (layer) 3. A continuación se utiliza para simplificar la denominación host para el primer equipo.

El host se conecta a través de una red de comunicaciones N con un segundo equipo G0. Este segundo equipo puede ser por ejemplo una de las gateways citadas al principio. No obstante, el segundo equipo puede ser igualmente cualquier equipo de comunicaciones con capacidades de comunicación L3. A continuación se utiliza para simplificar la denominación gateway para el segundo equipo.

La red de comunicación N es en el ejemplo de ejecución preferente una red que respecto a la capa (layer) 2 funciona por ejemplo según el estándar Ethernet. Pueden utilizarse otras redes y/o protocolos para el transporte transparente de mensajes entre host y gateway.

La red N está dividida en dos subredes N_0, N_1 independientes. Esta división se realiza en el caso más sencillo a nivel lógico, pero ventajosamente se realiza también espacialmente, para prever la mayor seguridad posible frente a fallos. Entonces está compuesta la subred N_0 por un conjunto de componentes de conmutación o conmutadores S_{00}, S_{01}, S_{02}. Se representan tres componentes de conmutación, siendo desde luego esta cantidad sólo a modo de ejemplo y siendo cualquiera desde el punto de vista de esta invención, al igual que es cualquiera la estructura de la subred N_0, que sólo se ha representado como lineal a modo de ejemplo.

Los conmutadores S_{00}, S_{01} están conectados mediante un enlace L_{01}, representando este enlace un enlace lógico, bidireccional entre los conmutadores y pudiendo estar formado físicamente por varios enlaces. De la misma manera están conectados los conmutadores S_{01}, S_{02}, mediante un enlace L_{02}.

La subred N_1 está compuesta por un conjunto de componentes de conmutación o conmutadores S_{10}, S_{11}, S_{12}. Se representan tres componentes de conmutación, siendo desde luego esta cantidad solamente a modo de ejemplo y pudiendo ser cualquiera desde el punto de vista de esta invención, al igual que es cualquiera la estructura de subred N_0, que sólo se ha representado como lineal a modo de ejemplo. Los conmutadores S_{10}, S_{11}, están conectados mediante un enlace L_{11}, representando este enlace un enlace lógico, bidireccional entre los conmutadores y pudiendo estar formado físicamente por varios enlaces. De la misma manera están conectados los conmutadores S_{11}, S_{12}, mediante un enlace L_{12}.

La subred N_0 está conectada con el host mediante un enlace L_{00}. La subred N_1 está conectada con el host mediante un enlace L_{10}. Aquí presenta el host dos interfaces IF0, IF1 separadas, sirviendo una primera interfaz IF0 para la conexión con N_0 y una segunda interfaz IF1 para la conexión con N_1.

Para la conexión de la subred N_0 con la gateway G0 sirve un enlace L_{03}. En función del tipo de topología de redundancia, dispone la subred N_1 igualmente de una conexión con la gateway G0 -no representado- y/o de al menos una conexión transversal Q_1 con N_0. Ventajosamente se realiza esta conexión transversal lo más cerca posible de la transición de N_0 a la gateway G0, es decir, tal como se representa en la figura 1 por ejemplo entre S_{02}, y S_{12}. Si la conexión transversal Q_1 no está dispuesta directamente en la transición de la subred N_0 a la gateway G0, entonces pueden utilizarse protocolos adecuados para evitar bucles L2 en relación con la presente invención. Se entiende que la conexión transversal Q_1 puede estar compuesta físicamente por varios enlaces.

En una configuración ventajosa, se prevé adicionalmente a la gateway G0 una gateway sustitutoria G1 -representada con línea discontinua- para el caso de que falle la gateway G0. Entonces pueden estar conectadas las gateways G0, G1 igualmente mediante una conexión transversal Q_2. Un enlace L_{13} conecta la subred N_1 y la gateway G1. En función del tipo de topología de redundancia, dispone la subred N_0 igualmente de una conexión (no representada) a la gateway G1.

Puede realizarse una priorización de las gateways G0, G1 administrando correspondientemente las gateways. Por ejemplo puede equiparse la conexión de la gateway G0 con la subred N_0 como ruta de más bajo coste (lower-cost) y la conexión de la gateway G1 con la subred N_1 como ruta de coste más alto (higher-cost). La priorización es una posibilidad de asegurar en el caso de una avería de la conexión transversal Q_1 que tanto todos los hosts como también la red IP siempre utilizan la subred (aquí: N_0) conectada a la gateway G0 averiada para la comunicación. Esto asegura a la vez también todas las vías internas de comunicación de servidor a servidor (host-host).

Con la topología de red representada resultan a modo de ejemplo las siguientes rutas de mensajes indicadas en la figura 1B. Al respecto se consideran sólo rutas internas respecto a la red N:

ruta1: host <-> IF0 <-> N_0 <-> G0 <-> IP

ruta2: host <-> IF1 <-> N_1 <-> Q_1 <-> S_{02} <-> G0 <-> IP

ruta3: host <-> IF0 <-> N_0 <-> Q_1 <-> S_{12} <-> G1 <-> IP

ruta4: host <-> IF1 <-> N_1 <-> G1 <-> IP

Si está prevista para las gateways G0, G1 la citada priorización y se realiza además adicionalmente una priorización de las interfaces IF0, IF1, teniendo por ejemplo IF0 la prioridad más alta, resulta la siguiente priorización de las citadas rutas, en el caso de que la priorización de la gateway deba ser más fuerte que la priorización de las interfaces:

Ruta1 > ruta2 > ruta3 > ruta4

Otras rutas de mensajes resultan de manera análoga cuando existen los citados enlaces en cruz de N_0 a G1 y N_1 a G0 y/o cuando existen otras conexiones transversales o también enlaces cruzados dentro de la red N entre las subredes N_0 y N_1.

De manera ventajosa resulta mediante la configuración de red representada en la figura 1 que cada host puede llegar a la gateway G0 (averiada) a través de al menos dos vías y que un primer host con interfaz activa IF0 e interfaz standby IF1 puede comunicar con otro host con interfaz standby IF0 e interfaz activa IF1 -no representada- a través de rutas de mensajes. Incluso cuando están averiadas ambas gateways G0 y G1 pueden intercambiar los hosts entre sí mensajes a través de la conexión transversal.

Aún cuando pueden preverse varios enlaces transversales entre las subredes N_0, N_1, es ventajoso prever solamente una conexión transversal Q_1 en los conmutadores que se encuentran más próximos a las gateways G0, G1. Así pueden evitarse bucles (loops) de la capa 2 y con ello la utilización de un Spanning Tree Protocol SPT (protocolo de árbol de expansión).

No obstante, no es necesaria una priorización en todos los casos, por ejemplo en el caso de que la conexión transversal Q_1 -no representado- esté compuesta físicamente por varios enlaces. En este caso no es necesaria la priorización, ya que cuando falla uno de estos enlaces al menos se dispone de otro enlace.

Los enlaces L_{01}, L_{02} y L_{11}, L_{12} representados en la figura 1 entre los elementos de conmutación S_{00}, S_{01}, S_{02} y S_{10}, S_{11}, S_{12}, así como la conexión transversal Q_1, están realizados tradicionalmente como enlaces locales, con lo que las redes N_0 y N_1 son simples redes de área local (Local Area Networks) LANs. Las configuraciones implantadas espacialmente entre equipos host y equipo(s) gateway pueden realizarse por el contrario configurando todos o algunos elegidos de entre los citados enlaces, por ejemplo respecto a la capa (layer) 1, como enlaces de tráfico de larga distancia.

Esto se representa esquemáticamente en las figuras 2A y 2B. En la figura 2A se prevé un equipo de gateway G0 alejado, que mediante una red local N_{01} compuesta por los conmutadores S_{00} y S_{01}, así como el enlace L_{01}, de una red de área amplia WAN esquemáticamente representada y una segunda red local N_{02}, compuesta por el conmutador S_{02}, está unido con un componente host. Además, se conduce la conexión transversal entre las subredes N_{02} y N_1 igualmente a través de la red de área amplia WAN. Respecto a la representación básica de la figura 1, se han realizado en la figura 2A los enlaces L_{02} y Q_1 como conexiones de tráfico de larga distancia; la conexión de la segunda gateway G1 local opcional se realiza mediante la red local N_1.

En la figura 2B se conecta el equipo host con dos equipos gateway G0, G1 alejados. La conexión redundante se logra por un lado mediante una red local N_{01} compuesta por los conmutadores S_{00} y S_{01}, así como por el enlace L_{01} y una red local N_{02} compuesta por el conmutador S_{02}, estando unidas las redes locales N_{01} y N_{02} mediante una red de área amplia WAN, así como por otro lado mediante una red local N_{11} compuesta por los conmutadores S_{10} y S_{11}, así como el enlace L_{11} y una red local N_{12}, compuesta por el conmutador S_{12}, estando unidas las redes locales N_{11} y N_{12} mediante la red de área amplia WAN. Respecto a la representación básica de la figura 1, están realizados en la figura 2A los enlaces L_{02}, L_{12}, y Q_1 como enlaces de tráfico de larga distancia.

Los ejemplos de ejecución representados básicamente en la figura 2 de la conexión de un equipo host a un equipo o equipos gateway se describirán más en detalle ahora con referencia a las figuras 3A y 3B.

La figura 3A muestra, en concordancia con la representación de la figura 2A, el caso de un equipo host que está conectado con una gateway G1 local y una gateway G0 alejada. La conexión del equipo host a la gateway G1 local se realiza entonces mediante una red local (por ejemplo LAN) N_1. Tal como se describe en relación con la figura 2A, están formados en la figura 3A el enlace L_{02} y la conexión transversal Q_1 por un enlace de tráfico de larga distancia (WAN = Wide Area Network, red de área local). La WAN esta configurada en el ejemplo de la figura 3A como anillo de ethernet sobre SONET. Cuatro elementos, preferiblemente cuatro multiplexadores ADD/DROP M_1, M_2, M_3, M_4, están entonces dispuestos en una estructura anular, es decir, el anillo R une M_1 con M_2, M_2 con M_3, M_3 con M_4 y M_4 con M_1, en cada caso bidireccionalmente. Como particularidad se configura preferiblemente el anillo SONET realizándose enlaces punto-a-punto.

Las rutas de mensajes representadas esquemáticamente en la figura 1B pueden realizarse en el ejemplo de ejecución de la figura 3A por ejemplo como sigue:

ruta1: host <-> IF0 <-> N_{01} <-> M_1 <-> M_4 <-> N_{02} <-> IP

ruta2: host <-> IF1 <-> N_1 <-> M_2 <-> M_3 <-> N_{02} <-> IP

ruta3: host <-> IF0 <-> N_{01} <-> M_1 <-> M_2 <-> N_1 <-> IP

ruta4: host <-> IF1 <-> N_1 <-> IP

Entonces permite la estructura anular redundante la configuración de vías sustitutorias; por ejemplo cuando falla un segmento anular entre M_1 y M_4, puede realizarse la conexión sustitutoria de este tramo de la ruta1 como sigue:

M_1 <-> M_2 <-> M_3 <-> M_4 ó

M_1 <-> M_2 <-> M_3 <-> N_{02}

De manera análoga pueden indicarse vías sustitutorias internas respecto a la WAN para otros fallos; los procedimientos para ello son suficientemente conocidos.

La figura 3B muestra al respecto, apoyándose en la representación de la figura 2B, el caso de un equipo host que está conectado con dos gateways G0, G1 alejadas, siendo la gateway G1 opcional. La conexión del equipo host a la gateway G0 se realiza entonces mediante una red local (por ejemplo LAN) N_0, así como un Resilient Packet Ring RPR (anillo de paquetes con protección) según IEEE 802.17 u otro anillo WAN comparable (por ejemplo Extreme Networks Ethernet Automatic Protection Switching EAPS, Conmutación de protección automática de Ethernet de Extreme Networks, o Cisco Resilient Packet Ring Technology, tecnología de anillo de paquetes con protección de Cisco). El enlace L_{02} conecta la subred N_0 con el RPR, estando representado éste a modo de ejemplo compuesto por cuatro conmutadores Ethernet (preferiblemente Ethernet Gigabit) E_1, E_2, E_3, E_4, y un enlace anular RPR. El anillo RPR conecta E_1 con E_2, E_2 con E_3, E_3 con E_4 y E_4 con E_1, en cada caso bidireccionalmente.

A diferencia de la representación de la figura 2B, se realiza en la figura 3B el enlace entre la WAN y las gateways directamente mediante los enlaces L_{03} y L_{13}, pero puede incluir también, tal como se representa en la figura 2B, otros elementos. La conexión transversal Q_1 está formada por el RPR. Considerado esquemáticamente, sustituye el RPR en la figura 3B los conmutadores S_{02} y S_{12}, así como la conexión transversal Q_1 de la figura 1.

La conexión del equipo host a la gateway (opcional) G1 se realiza mediante una red local (p.e. LAN) N_1, así como el RPR. El enlace L_{12} conecta la subred N_1 con el RPR.

Las rutas de mensajes representadas esquemáticamente en la figura 1B pueden realizarse en el ejemplo de ejecución de la figura 3B por ejemplo como sigue:

ruta1: host <-> IF0 <-> N_0 <-> E_1 <-> RPR <-> E_4 <-> IP

ruta2: host <-> IF1 <-> N_1 <-> E_2 <-> RPR <-> E_4 <-> IP

ruta3: host <-> IF1 <-> N_0 <-> E_1 <-> RPR <-> E_3 <-> IP

ruta4: host <-> IF0 <-> N_1 <-> E_2 <-> RPR <-> E_3 <-> IP

Del estado en ese momento del propio anillo depende cómo discurren las vías de comunicación en el RPR y para el procedimiento aquí descrito es irrelevante, ya que la estructura redundante del anillo y el protocolo del anillo aseguran la configuración automática de vías sustitutorias; por ejemplo cuando falla el segmento de anillo entre E_1 y E_4, se conecta sustitutoriamente este tramo mediante el protocolo del anillo como sigue: E_1 <-> E_2 <-> E_3 <-> E_4.

De manera análoga pueden indicarse vías sustitutorias internas relativas a la WAN para otros fallos; existen procedimientos suficientemente conocidos para ello.

La configuración de red correspondiente a la invención puede combinarse ventajosamente con un procedimiento para comprobar las rutas de mensajes, lo cual se describirá a continuación brevemente.

La comprobación de las rutas de mensajes se realiza enviando el host a través de cada interfaz IF0, IF1 a cada gateway G0, G1 a intervalos de tiempo muy cortos, por ejemplo cada 100 ms, datagramas IP especiales de comprobación. Como dirección IP fuente y como dirección IP de destino, se inscriben la dirección IP de la correspondiente interfaz propia IF0 e IF1, respectivamente. Así se refleja el paquete de comprobación a través de la gateway de nuevo a la interfaz IF0, IF1 emisora del host.

La siguiente tabla muestra las direcciones IP y MAC a elegir para la comprobación de las rutas de mensajes Pfad1...Pfad4:

	Ruta1	Ruta2	Ruta3	Ruta4
MAC de destino	G0	G0	G1	G1
MAC de origen	IF0	IF1	IF0	IF1
IP de destino	IF0	IF1	IF0	IF1
IP de origen	IF0	IF1	IF0	IF1

Básicamente se realiza por tanto el direccionamiento de los mensajes de la capa (layer) 2 correctamente en base a las correspondientes direcciones MAC (MAC = Media Access Control, control de acceso a medios), modificándose por el contrario el direccionamiento de los mensajes de capa 3 superiores tal que los mensajes de capa 3 se vuelven

a enrutar de retorno a la instancia emisora. Este principio se basa en el hecho de que por lo general los mensajes de la capa n durante el transporte a través de una red de la capa n-1 no son modificados y de que las informaciones de direcciones de la capa n no son evaluadas por la red de la capa n-1.

Para mensajes de comprobación IP, reside una ventaja importante en que sólo la función "IP-Forwarding" (retransmisión IP), que está realizada sobre tarjetas de interfaz potentes de las gateways, es necesaria para reflejar o devolver los mensajes de comprobación a la instancia emisora. De esta manera no puede presentarse una situación de sobrecarga en la gateway debido al procedimiento de comprobación, ya que el procesador de conmutación de las gateways no está implicado en absoluto en el procesamiento de los mensajes de comprobación.

Si dentro de un determinado espacio de tiempo, por ejemplo 100 ms, el mensaje de comprobación reflejado en el correspondiente destino no es recibido de nuevo por el host, entonces existe probablemente una avería en la correspondiente ruta de mensajes. Esto se anota por ejemplo en una memoria. La avería de la ruta de mensajes puede también indicarse primeramente como avería duradera cuando tampoco se recibe de nuevo en el host el siguiente mensaje de comprobación asociado a esta ruta de mensajes. También puede configurarse adaptándose a las circunstancias correspondientes la cantidad de mensajes consecutivos que pueden perderse por cada ruta de mensajes antes de que ello se evalúe como avería.

Existe además la posibilidad de señalar los mensajes de comprobación enviados con números consecutivos o números secuenciales. Éstos se inscriben en los datos útiles (payloads) de los mensajes de comprobación. La pérdida de una cantidad configurable de mensajes de comprobación no necesariamente consecutivos, puede igualmente incluirse como criterio para la detección de un fallo, es decir, las rutas de mensajes son vigiladas mediante numeración de los mensajes de comprobación. El contador de mensajes de comprobación perdidos puede entonces configurarse tal que un mensaje de comprobación perdido aumenta el contador en 1 y una cantidad configurable de mensajes de comprobación recibidos sin pérdida, por ejemplo 1000, reduce el contador en 1. Alternativamente, puede realizarse la reducción del contador tras transcurrir un intervalo de tiempo durante el que no ha habido ninguna pérdida de mensajes de comprobación. Si alcanza el contador un valor límite, se evalúa la ruta de mensajes como averiada.

Si se comprueban las rutas de mensajes a intervalos de tiempo suficientemente cortos con ayuda del procedimiento correspondiente a la invención, por ejemplo cada 100 ms, y se repite exactamente una vez una comprobación fallida antes de evaluar la correspondiente ruta como averiada, entonces se reconoce la ruta de mensajes como averiada, cuando falla la comprobación repetida con un retardo muy pequeño, aquí 200 ms.

Al especialista le es posible sin más, en base al caso de aplicación concreto, adaptar los parámetros descritos del procedimiento de comprobación al correspondiente caso de aplicación.

Una vez que una avería ha sido detectada y anotada, existe la necesidad de desviar el tráfico de datos útiles de la ruta de mensajes averiada a otra ruta de mensajes no averiada. Los procedimientos para ello son muy conocidos. Por ejemplo, envía el host un "Gratituous ARP" (ARP innecesario), es decir, una solicitud (request) ARP relativa a la dirección IP propia. Como dirección MAC de origen (source) utiliza el host la interfaz de la que parte la solicitud, y como dirección IP buscada la dirección IP propia. Mediante la difusión (broadcast) ARP, se actualizan los ARP Caches de todos los hosts y gateways conectados con la relación de direcciones MAC/IP. La conmutación se realiza por ejemplo sobre las rutas de mensajes sustitutorias mencionadas, que se eligen según su priorización.

Aunque el ejemplo de ejecución de la invención se ha descrito con referencia a un entorno IP/LAN, la invención no queda limitada a este entorno de protocolo. Pueden utilizarse por ejemplo protocolos orientados al enlace para el enlace host-gateway. Si se detecta mediante el protocolo una interrupción del enlace, puede originarse una conmutación a una vía de transmisión redundante. Ejemplo de tales protocolos son los protocolos de tiempo real (Real Time Protocol, RTP) o Stream Control Transmission Protocol (protocolo de transmisión de control del flujo) SCTP.

Con SONET y Resilient Packet Ring (anillo de paquetes con protección) se ha descrito la presente invención para dos procedimientos WAN típicos redundantes. Otros procedimientos WAN pueden utilizarse evidentemente de la misma forma, en particular en relación con las conclusiones de las figuras 1 y 2 para la presente invención.

REIVINDICACIONES

1. Configuración de red para una red de comunicaciones (N) que conecta un primer equipo servidor (host) y una gateway o pasarela (G0),

- compuesto por una primera subred (N_0) y al menos una segunda subred (N_1),
- estando compuesta la primera subred (N_0) por primeros elementos de conmutación (S_{00}, S_{01}, S_{02}), y estando compuesta la segunda subred (N_1) por segundos elementos de conmutación (S_{10}, S_{11}, S_{12}), y
- estando configuradas la primera y la segunda subred independientes entre sí,
- con al menos una conexión transversal (Q_1) entre las subredes (N_0, N_1) y
- con al menos un primer enlace (L_{00}) entre la primera subred y una primera interfaz (IF0) del primer equipo (host) y al menos un segundo enlace (L_{10}) entre la segunda subred y una segunda interfaz (IF1) del primer equipo (host) y con al menos un tercer enlace (L_{03}) entre la primera subred y el segundo equipo (G0),
- estando configurados enlaces (L_{01}, L_{02}) entre los primeros elementos de conmutación (S_{00}, S_{01}, S_{02}) y/o enlaces (L_{11}, L_{12}) entre los segundos elementos de conmutación (S_{10}, S_{11}, S_{12}) y/o la(las) conexión(es) transversales (Q_1) como enlaces de tráfico de larga distancia (WAN),

caracterizado porque al menos una de las conexiones transversales (Q_1) está dispuesta directamente en la transición de la red de comunicaciones (N) a la pasarela o gateway (G0).

2. Configuración de red según la reivindicación 1,

con al menos un cuarto enlace (L_{13}) entre la segunda subred y un tercer equipo (G1) del mismo tipo que la gateway (G0).

3. Configuración de red según la reivindicación 1,

caracterizada porque la comunicación entre el primer equipo y la gateway y/o el tercer equipo se realiza mediante mensajes de una primera capa de protocolo, cuya transmisión en la red de comunicaciones (N) se realiza mediante una segunda capa de protocolo subordinada a la primera capa de protocolo.

4. Configuración de red según la reivindicación 3,

caracterizada porque la primera capa de protocolo está formada por el protocolo de Internet y la segunda capa de protocolo mediante un protocolo de una red de área local (Local Area Network) LAN.

5. Configuración de red según la reivindicación 4,

caracterizada porque el(los) enlace(s) de tráfico de larga distancia (WAN) están realizados como enlaces Ethernet sobre SONET.

6. Configuración de red según la reivindicación 4,

caracterizada porque el(los) enlace(s) de tráfico de larga distancia (WAN) están realizados como Resilient Packet Ring (anillo de paquetes con protección) RPR.

FIG 1A

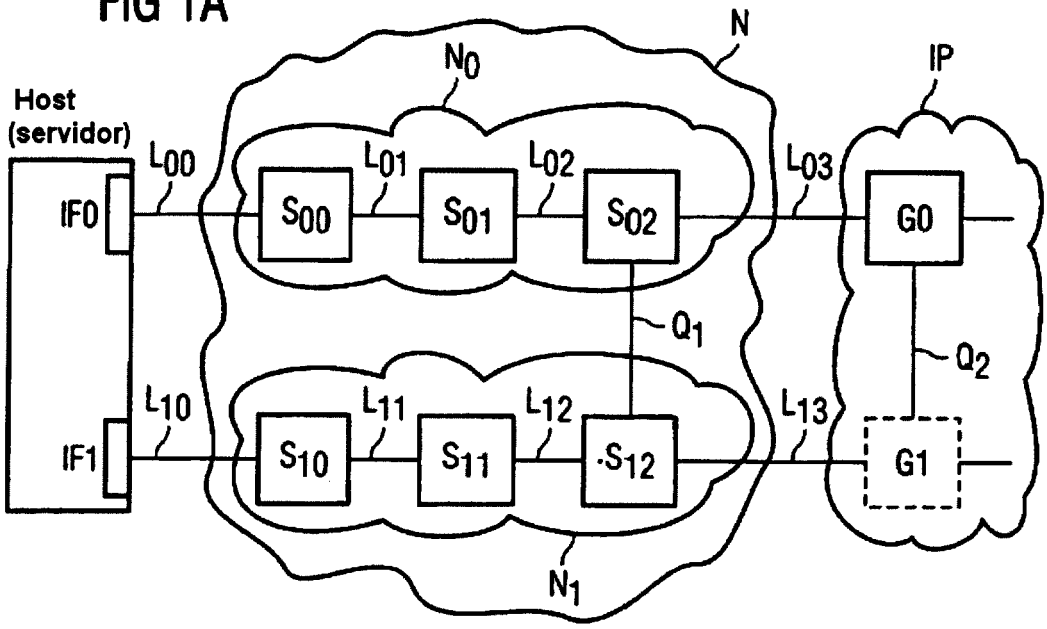

Host
(servidor)
IF0
IF1
L00
L01
L02
L03
L10
L11
L12
L13
S00
S01
S02
S10
S11
S12
N
N0
N1
IP
G0
G1
Q1
Q2

FIG 1B

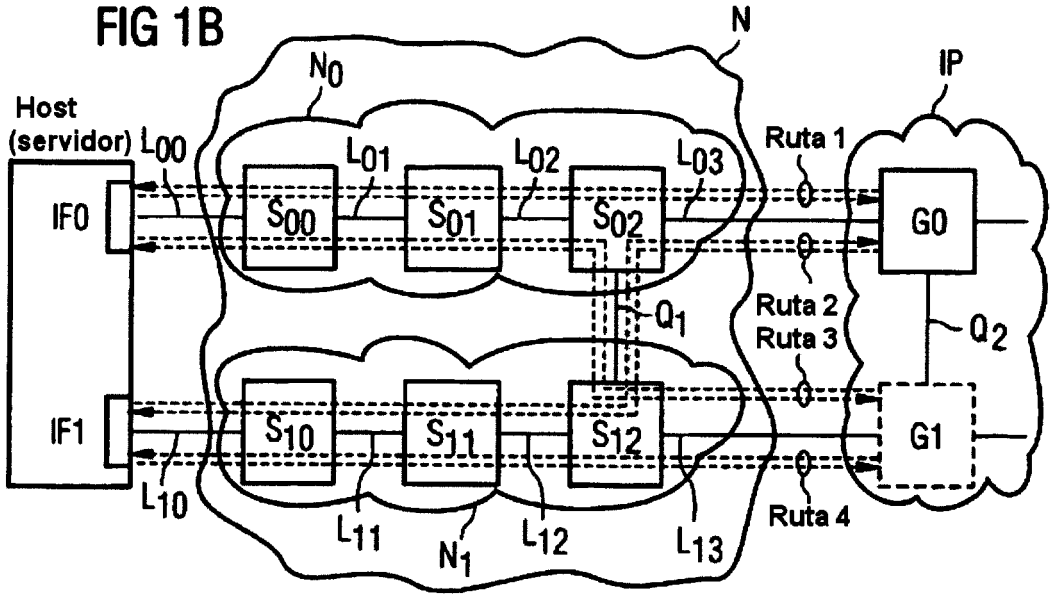

Host
(servidor)
IF0
IF1
L00
L01
L02
L03
L10
L11
L12
L13
S00
S01
S02
S10
S11
S12
N
N0
N1
IP
G0
G1
Q1
Q2
Ruta 1
Ruta 2
Ruta 3
Ruta 4

FIG 2A

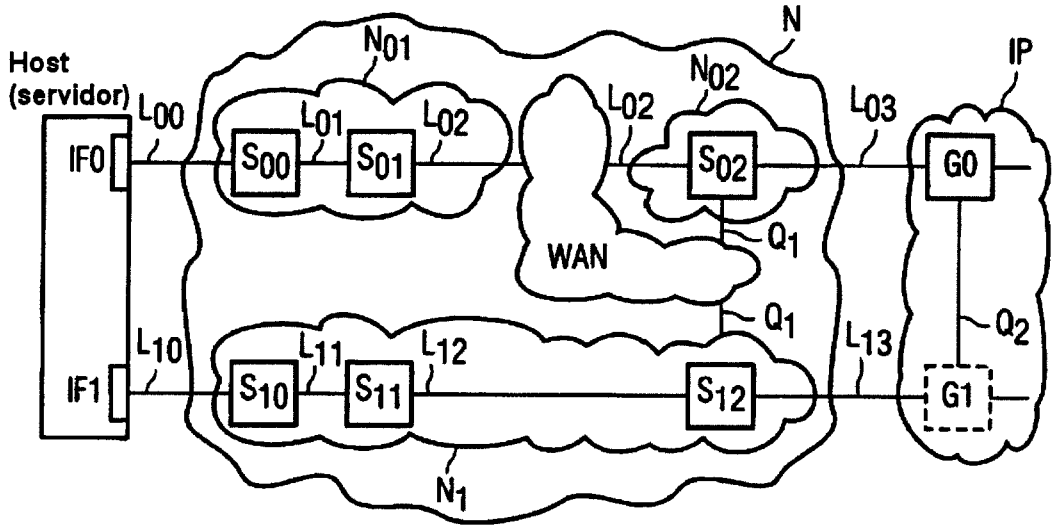

Host
(servidor)
IF0
IF1
L00
L10
N01
S00
S01
L01
L02
N
N02
L02
S02
L03
IP
G0
WAN
Q1
Q1
Q2
L10
L11
L12
S10
S11
S12
L13
G1
N1

FIG 2B

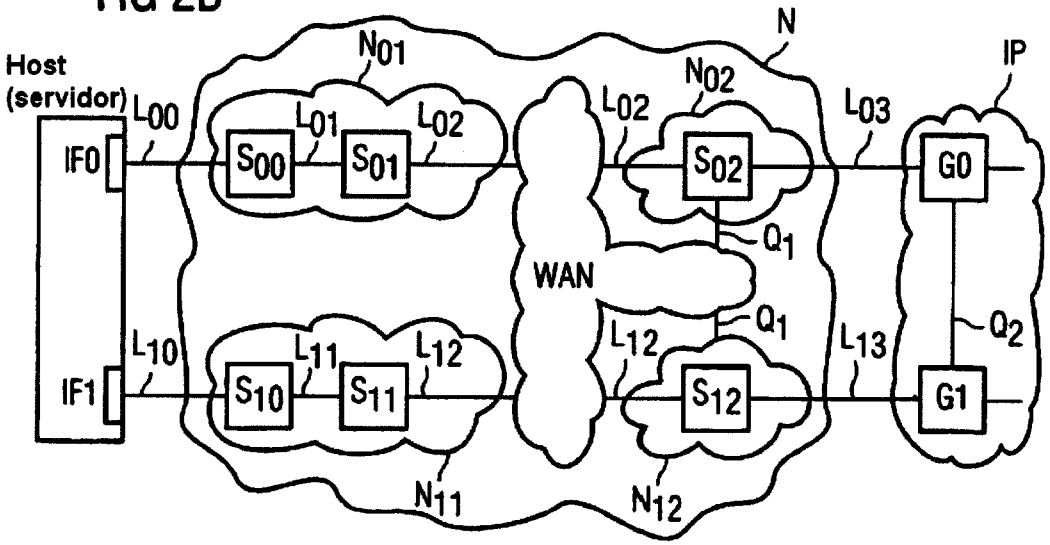

Host
(servidor)
IF0
IF1
L00
L10
N01
S00
S01
L01
L02
N
N02
L02
S02
L03
IP
G0
WAN
Q1
Q1
Q2
L10
L11
L12
L12
S10
S11
S12
L13
G1
N11
N12

FIG 3A

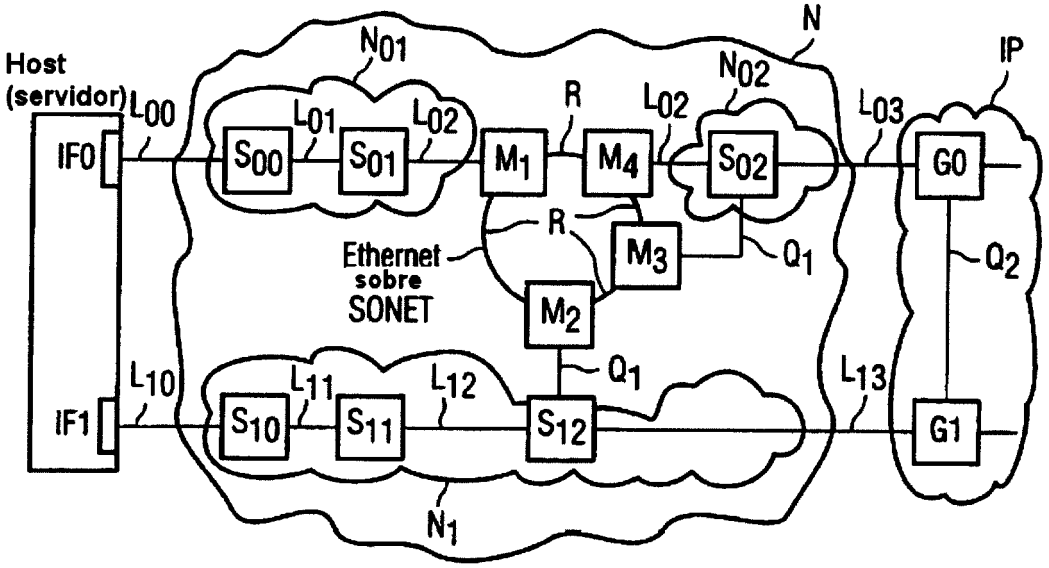
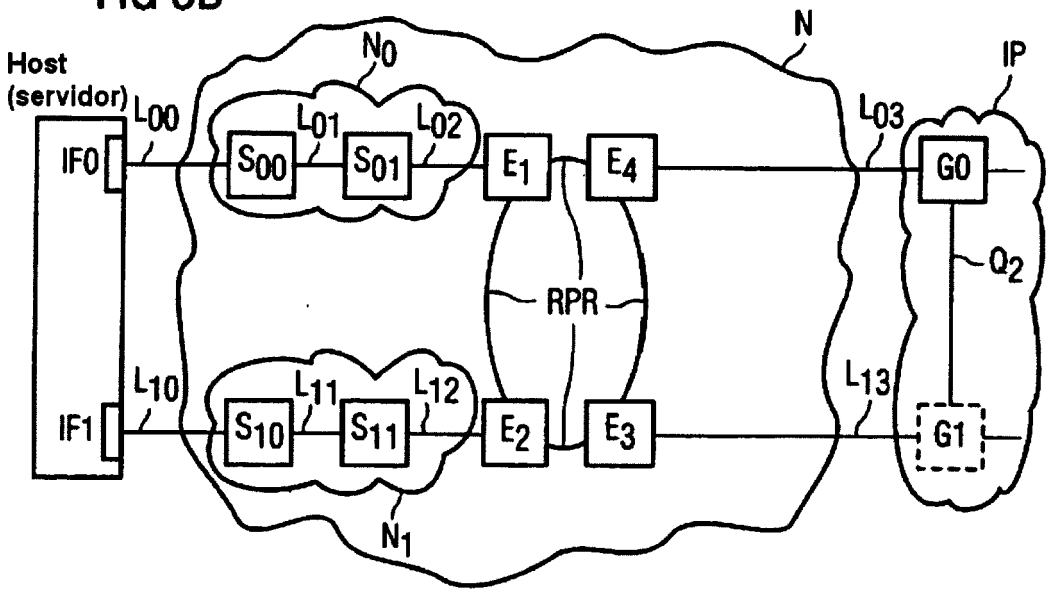

Host
(servidor)
IF0
IF1
L00
L01
L02
L03
L10
L11
L12
L13
N01
N02
N
IP
S00
S01
S02
S10
S11
S12
M1
M2
M3
M4
R
Q1
Q2
Ethernet
sobre
SONET
G0
G1
N1

FIG 3B


Host
(servidor)
IF0
IF1
L00
L01
L02
L03
L10
L11
L12
L13
N0
N
IP
S00
S01
S10
S11
E1
E2
E3
E4
RPR
G0
G1
Q2
N1