(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 766 325**

(51) Int. CI.:

H04L 29/12 (2006.01)
H04L 12/713 (2013.01)
H04L 12/721 (2013.01)
H04L 12/28 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.06.2014 PCT/IB2014/062273**

(87) Fecha y número de publicación internacional: **24.12.2014 WO14203154**

(96) Fecha de presentación y número de la solicitud europea: **16.06.2014 E 14759281 (0)**

(97) Fecha y número de publicación de la concesión europea: **21.08.2019 EP 3011708**

(54) Título: **Sistema para el enrutamiento de datos a redes informáticas**

(30) Prioridad:

21.06.2013 IT MO20130178

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.06.2020

(73) Titular/es:

C.R.D. CENTRO RICERCHE DUCATI TRENTO S.R.L. (100.0%)
Via Fortunato Zeni 8
38068 Rovereto (TN), IT

(72) Inventor/es:

ZANFEI, ADRIANO y
MARZADRO, CHRISTIAN

(74) Agente/Representante:

LÓPEZ CAMBA, María Emilia

DESCRIPCIÓN

Sistema para el enrutamiento de datos a redes informáticas

Campo técnico

La presente invención se refiere a un sistema para el enrutamiento de datos a redes informáticas.

Antecedentes de la técnica

Existe una necesidad cada vez más fuerte de conectar una aplicación en un ordenador cliente a una aplicación en un servidor remoto a través de Internet convencional. En general, la conexión tiene una serie de características comunes:

- el tráfico generado por las dos aplicaciones utiliza protocolos estándar de nivel 4 del denominado modelo ISO/OSI, típicamente protocolos TCP (protocolo de control de transmisión) o UDP (protocolo de datagramas de usuario);
- a cada aplicación (o servicio) se asocia estáticamente un puerto (base) diferente, que permite que varios procedimientos/aplicaciones activen múltiples conexiones TCP/UDP a pesar de compartir la misma dirección IP;
- el acceso a Internet por componentes o aparatos es de tipo indirecto.

Esto implica que la dirección IP asignada no es pública, sino que pertenece a una subred a la que está conectado el aparato y, por lo tanto, es una dirección privada y no unívoca en el espacio de direcciones asignadas en Internet.

Dentro de la subred, el uso es conocido y común de un componente/aparato electrónico, un denominado enrutador adecuado para enrutar datos hacia distintas redes y, en particular, adecuado para gestionar todas las solicitudes hacia direcciones IP públicas.

Dentro de las redes, también se gestiona el filtrado de comunicaciones según la dirección IP, al número de puerto TCP/UDP, además del texto sin formato de la comunicación.

El filtrado realizado por el cortafuegos puede ser más o menos estricto dependiendo del nivel de seguridad del ordenador previsto para la subred específica.

Teniendo en cuenta la necesidad de conectar una aplicación p en un ordenador cliente a una aplicación presente en un servidor remoto a través de Internet convencional y, en general, la necesidad de interconectar diferentes aparatos/componentes de cliente, se encuentran varias complejidades.

De hecho, los aparatos/componentes del cliente pueden tener las siguientes características: dirección IP privada y, por lo tanto, no unívocos;
las solicitudes hacia IP públicas son enrutadas por una puerta de terceros presente en la misma red; el cortafuegos de terceros puede no permitir el enrutamiento de paquetes vinculados a varios puertos y/o efectuar el filtrado según el contenido de los paquetes;
el cortafuegos de terceros no puede enviar las solicitudes provenientes del exterior hacia un cliente presente en su subred.

Para superar dichos inconvenientes y permitir el control completo del cliente, normalmente se utilizan sistemas de comunicación del tipo VPN (red privada virtual), que permiten establecer una conexión privada entre dos aparatos, más específicamente entre el cliente y el servidor, utilizando una red pública compartida.

En particular, una serie de programas VPN, como, por ejemplo, OpenVPN, permiten implementar la tunelización, es decir, la canalización de todas las conexiones TCP/UDP en diferentes puertos enrutados a un solo puerto, por ejemplo, el puerto 80 TCP/IP más común, resolviendo así el problema de filtrado efectuado por un cortafuegos de terceros y el enrutamiento de los paquetes desde y hacia el cliente.

Como la figura 1 muestra esquemáticamente, el uso de un sistema de tipo VPN prevé la asignación en el servidor de una dirección IP para un extremo de los túneles (srvtun1) y la asignación de una dirección IP diferente en cada cliente para cada otro extremo de los túneles (tun1-tunn).

Como se muestra en la figura 1, siempre a modo de ejemplo, en esta configuración, existe la posibilidad de que a la interfaz de red (eth0) del cliente (cliente 1) conectado a una LAN (3p LAN 1) se le asigne una dirección IP idéntica a la predeterminada para el túnel (tun1), con los consiguientes problemas de reenvío.

De hecho, en dicho caso, la dirección IP privada asignada a la interfaz de red (eth0) es asignada dinámicamente por el servicio DHCP de la red privada (3p LAN 1) y puede pertenecer a cualquier clase de direcciones IP privadas.

En particular, las tres clases de direcciones IP privadas son, respectivamente:

- direcciones de clase A 10.x.x.x, con direcciones IP de 10.0.0.0 a 10.255.255.255;
- direcciones de clase B 172.x.x.x, con direcciones IP de 172.16.0.0 a 172.31.255.255;
- direcciones de clase C 192.168.x.x, con direcciones IP de 192.168.0.0 a 192.168.255.255.

Para superar este inconveniente, se requiere, por lo tanto, la intervención del administrador de la red el cual, después de verificar el fallo, debe cambiar las direcciones IP asignadas de forma manual y estática.

En el documento de patente WO 01/82097 se describe un procedimiento y un aparato para integrar protocolos de tunelización con protocolos de enrutamiento estándar.

Descripción de la invención

El objetivo principal de la presente invención es proporcionar un sistema para el enrutamiento de datos a redes informáticas que garantice el enrutamiento correcto de los datos entre dispositivos que pertenecen a diferentes subredes, conectados a Internet tanto directa como indirectamente, de forma totalmente automática y sin la necesidad de la configuración manual de los datos enrutados.

Otro objetivo de la presente invención es proporcionar un sistema para el enrutamiento de datos a redes informáticas que permita superar los inconvenientes mencionados de la técnica anterior en el ámbito de una solución simple, racional, fácil y efectiva de usar, así como de bajo coste.

Los objetivos mencionados anteriormente se consiguen mediante el presente sistema para el enrutamiento de datos a redes informáticas según la reivindicación 1.

Breve descripción de los dibujos

Otras características y ventajas de la presente invención se harán más evidentes a partir de la descripción de una realización preferida de la invención, pero no exclusiva, de un sistema para el enrutamiento de datos a redes informáticas, ilustrado a modo de ejemplo indicativo, pero no limitativo, en los dibujos adjuntos, en los que:

la figura 2 es un diagrama de bloques que muestra el sistema según la invención en su conjunto;
la figura 3 es un diagrama de bloques que muestra con mayor detalle una unidad de enrutamiento, del tipo de cortafuegos/enrutador, que pertenece al sistema según la invención;
las figuras 4 a 7 muestran esquemáticamente diferentes posibles reenvíos que se pueden realizar a través de la unidad de enrutamiento de la figura 2;
la figura 8 muestra una segunda posible realización del sistema según la invención;
la figura 9 muestra una posible primera tabla de enrutamiento virtual implementable dentro de la unidad de enrutamiento de la figura 8; la figura 10 muestra una posible segunda tabla de enrutamiento implementable dentro de la unidad de enrutamiento de la figura 8.

Realizaciones de la invención

Con referencia particular a dichas ilustraciones, por S se ha indicado globalmente un sistema para el enrutamiento de datos a redes informáticas, capaz de permitir la interconexión automática de diferentes dispositivos o componentes de clientes conectados a diferentes redes patentadas privadas conectadas directa o indirectamente a Internet por medios de redes de terceros.

En particular, como se muestra esquemáticamente en la figura 2, el sistema S comprende:

- una unidad de servidor SRV conectada a una red pública I, que consiste, por ejemplo, en Internet convencional;
- una pluralidad de redes de área local patentadas, indicadas por la redacción Prop. LAN 1, ..., Prop. LAN m, que tienen dispositivos de cliente respectivos CL1, ... ; CLn;
- una pluralidad de unidades de enrutamiento FW1, ..., FWm, que consiste en componentes y/o dispositivos adecuados, conectados a las respectivas redes de área local patentadas y conectadas a la red pública I a través de las respectivas redes de área local de terceros 3p LAN 1, .. ., 3p LAN m.

Sin embargo, no se pueden descartar diferentes arquitecturas del sistema S donde, por ejemplo, algunas o todas las unidades de enrutamiento FW1, ... , FWm están conectadas directamente a la red pública I.

Las redes de área local de terceros 3p LAN 1,. .., 3p LAN m pueden consistir, por ejemplo, en las respectivas WAN (redes de área amplia) que se extienden dentro de un área geográfica determinada, por ejemplo, dentro de diferentes áreas municipales.

Las unidades de enrutamiento FW1, ... , FWm consisten en cortafuegos/enrutadores patentados respectivos y son

cruciales para la gestión de cada una de las redes de área local patentadas.

En particular, cada una de las unidades de enrutamiento FW1, ..., FWm tiene una primera interfaz de red eth0 conectada a la red pública I a través de una red de área local respectiva de terceros 3p LAN 1, ..., 3p LAN m.

Además, cada una de las unidades de enrutamiento FW1, ... , FWm tiene una segunda interfaz de red eth1 conectada a una red de área local respectiva Prop. LAN 1, ..., Prop. LAN m.

De manera útil, cada una de las unidades de enrutamiento FW1, ... , FWm tiene una tercera interfaz de red conectada a la unidad de servidor SRV a través de una conexión privada VPN (red privada virtual).

Dicha conexión privada VPN se realiza preferentemente por medio de Open VPN u otra solución de tunelización en un puerto identificado libre para comunicarse en redes de terceros.

Cada unidad de enrutamiento FW1, ... , FWm (cortafuegos/enrutador) puede gestionar:

- una dirección IP privada no conocida previamente en la primera interfaz de red eth0, que puede pertenecer a cualquier clase de direcciones IP privadas y que, por ejemplo, puede ser asignada dinámicamente por un servicio DHCP de la respectiva red de área local de terceros;
- el enrutamiento IP de dispositivos de cliente CL1, ... , CLn que pertenecen a redes de área local patentadas conectadas a la segunda interfaz de red eth1;
- una o más direcciones IP relacionadas con una o más terceras interfaces de red tun1 dedicadas a los túneles VPN;
- el enrutamiento de otros dispositivos de cliente CL1 ... , CLn que pertenecen a otras redes de área local patentadas.

Ventajosamente, cada unidad de enrutamiento FW1, ..., FWm comprende medios de enrutamiento automático VM0, que consisten en un componente o dispositivo adecuado, adecuado para enrutar los datos entre la unidad de servidor SRV y la red de área local respectiva Prop. LAN 1, ..., Prop. LAN m, independientemente de la dirección IP asignada a la primera interfaz de red eth0 respectiva.

De esta forma, cada unidad de enrutamiento FW1, ... , FWm garantiza el enrutamiento correcto de los datos entre los dispositivos del cliente que pertenecen a diferentes redes de área local, conectadas a Internet directa o indirectamente, de forma completamente automática y sin la necesidad de un manual configuraciones de la información de enrutamiento. Con referencia a una realización preferida de la invención, los medios de enrutamiento automático VM0 se implementan por medio de una máquina virtual colocada operativamente entre la primera interfaz de red eth0 y la segunda interfaz de red eth1.

En particular, la máquina virtual VM0 consiste en un software hecho específicamente para el reenvío/enrutamiento de datos.

Sin embargo, no se pueden descartar diferentes realizaciones donde, por ejemplo, los medios de enrutamiento automático se implementan mediante uno o más dispositivos de hardware y/o programas de software distintos y separados con respecto al cortafuegos/enrutador.

En particular, cada máquina virtual VM0 comprende al menos una primera interfaz de red virtual eth0' conectada a la primera interfaz de red eth0.

Además, cada unidad de enrutamiento FW1, ..., FWm comprende una interfaz de red ficticia dumtny0 y cada máquina virtual VM0 comprende una segunda interfaz de red virtual eth1' conectada a dicha interfaz de red ficticia dummy0. Cada máquina virtual VM0 comprende una tabla de enrutamiento virtual RT0 que contiene información sobre el reenvío de datos hacia la primera y la segunda interfaz de red virtual eth0' y eth1'.

Además, cada unidad de enrutamiento FW1, ..., FWm comprende una tabla de enrutamiento RT1 que contiene información sobre el reenvío de datos hacia la segunda interfaz de red eth1, la tercera interfaz de red tunI y la interfaz de red ficticia dummy0.

Ventajosamente, la dirección IP de dicha primera interfaz de red virtual eth0' corresponde a la dirección IP de la primera interfaz de red eth0.

Además, la máquina virtual VM0 comprende medios de determinación M adecuados para determinar una dirección IP que se asignará a la segunda interfaz de red virtual eth1' según la dirección IP de la primera interfaz de red virtual. Preferentemente, los medios de determinación se implementan mediante un algoritmo de software adecuado.

En particular, la dirección IP de la segunda interfaz de red virtual eth1':

- pertenece a una clase diferente de direcciones IP que la clase de direcciones IP de la dirección IP de la primera interfaz de red virtual eth0';
- no coincide con ninguna de las direcciones IP asignables a la red de área local respectiva Prop. LAN 1, ... , Prop. LAN m.

Además, el algoritmo de software M es adecuado para determinar una dirección IP que se asignará a la interfaz de red ficticia dummy0 según la dirección IP de la primera interfaz de red virtual eth0'.

En particular, la dirección IP de la interfaz de red ficticia dummy0:

- pertenece a una clase diferente de dirección IP que la clase de dirección IP de la primera interfaz de red virtual eth0';
- no coincide con ninguna de las direcciones IP asignables a dicha red de área local.

Preferentemente, el algoritmo de software M programa un servidor DHCP para asignar la dirección IP determinada al puerto de red ficticio dummy0.

Con referencia a una realización preferida de la invención del sistema S, se utiliza una clase específica y predefinida de direcciones IP para el enrutamiento de todas las redes de área local Prop. LAN 1, ..., Prop. LAN m.

Por ejemplo, las direcciones IP de la clase C de 192.168.x.0 a 192.168.x.255 se pueden usar para cada red de área local patentada.

Siempre con referencia a una realización preferida de la invención del sistema S, se utiliza una clase específica y predefinida de direcciones IP para el enrutamiento de los túneles VPN mediante las terceras interfaces de red tunI.

Por ejemplo, las direcciones IP de la clase B de 172.16.0.0 a 172.31.255.255 se pueden usar para cada interfaz de los túneles VPN.

Durante el funcionamiento del sistema S, cada unidad de enrutamiento FW1, ... , FWm puede gestionar cualquier asignación dinámica de IP en la primera interfaz de red eth0 conectada a la red de área local de terceros.

Las figuras de 4 a 7 muestran esquemáticamente diferentes posibles reenvíos que se pueden realizar por medio de cada unidad de enrutamiento FW1, ... , FWm.

En el ejemplo en la figura 4 a la primera interfaz de red eth0 se le asigna una dirección de clase A 10.4.247.106.

La primera interfaz de red virtual eth0' de la máquina virtual VM0 en la unidad de enrutamiento FW1 toma la misma dirección que eth0, por lo tanto, la dirección de clase A 10.4.247.106.

El algoritmo de software M implementado en la máquina virtual VM0 asigna la dirección de clase C C 192.169.200.254 a la segunda interfaz de red virtual eth1' y programa un servidor DHCP para asignar la dirección de clase C 192.169.200.2 a la interfaz de red ficticia dummy0 de la unidad de enrutamiento FW1.

A la tercera interfaz de red tunI, destinada a la comunicación por túnel VPN, le sigue asignada una dirección de clase B, por ejemplo, 172.18.1.2.

A la segunda interfaz de red eth1, conectada a la red de área local patentada, le sigue asignada una dirección de clase C, por ejemplo, 192.168.2.1.

En particular, la segunda interfaz de red eth1 puede gestionar de forma dinámica y estática todo el espacio de las direcciones de clase C, desde 192.168.0.0 a 192.168.255.255, excepto las direcciones 192.168.200.254 y 192.168.200.2 dedicadas a las interfaces eth1' y dummy0, lo que hace posible enrutar a todos los clientes de la red de área local patentada.

En el ejemplo en la figura 5 a la primera interfaz de red eth0 se le asigna una dirección de clase B 172.16.247.106.

La primera interfaz de red virtual eth0' de la máquina virtual VM0 en la unidad de enrutamiento FW1 toma la misma dirección que eth0, por lo tanto, la dirección de clase B 172.16.247.106.

El algoritmo de software M implementado en la máquina virtual VM0 asigna la dirección de clase C 192.169.200.254 a la segunda interfaz de red virtual eth1' y programa un servidor DHCP para asignar la dirección de clase C 192.169.200.2 a la interfaz de red ficticia dummy0 de la unidad de enrutamiento FW1.

A la tercera interfaz de red tun1, destinada a la comunicación por túnel VPN, le sigue asignada una dirección de clase B, por ejemplo, 172.18.1.2.

- A la segunda interfaz de red eth1, conectada a la red de área local patentada, le sigue asignada una dirección de clase C, por ejemplo, 192.168.2.1.

En particular, la segunda interfaz de red eth1 puede gestionar de forma dinámica y estática todo el espacio de direcciones de clase C, desde 192.168.0.0 a 192.168.255.255, excepto las direcciones 192.168.200.254 y 192.168.200.2 dedicadas a las interfaces eth1' y dummy0, lo que hace posible enrutar a todos los clientes de la red de área local patentada.

En el ejemplo en la figura 6, a la primera interfaz de red eth0 se le asigna una dirección de clase C 192.168.247.106.

La primera interfaz de red virtual eth0' de la máquina virtual VM0 en la unidad de enrutamiento FW1 toma la misma dirección que eth0, por lo tanto, la dirección de clase C 192.168.247.106.

El algoritmo de software M implementado en la máquina virtual VM0 asigna la dirección de clase B 172.17.200.254 a la segunda interfaz de red virtual eth1' y programa un servidor DHCP para asignar la dirección de clase C 172.17.200.2 a la interfaz de red ficticia dummy0 de la unidad de enrutamiento FW1.

A la tercera interfaz de red tunI, dedicada a la comunicación mediante túnel VPN, le sigue asignada una dirección de clase B, por ejemplo, 172.18.1.2.

A la segunda interfaz de red eth1, conectada a la red de área local patentada, le sigue asignada una dirección de clase C, por ejemplo, 192.168.2.1.

En particular, la segunda interfaz de red eth1 puede gestionar de forma dinámica y estática todo el espacio de las direcciones de clase C, desde 192.168.0.0 a 192.168.255.255, lo que permite enrutar a todos los clientes de la red de área local patentada.

En el ejemplo en la figura 7, a la primera interfaz de red eth0 se le asigna una dirección pública 109.205.109.10.

La primera interfaz de red virtual eth0' de la máquina virtual VM0 en la unidad de enrutamiento FW1 toma la misma dirección que eth0, por lo tanto, la dirección pública 109.205.109.10.

El algoritmo de software M implementado en la máquina virtual VM0 asigna la dirección de clase C 192.169.200.254 a la segunda interfaz de red virtual eth1' y programa un servidor DHCP para asignar la dirección de clase C 192.169.200.2 a la interfaz de red ficticia dummy0 de la unidad de enrutamiento FW1.

A la tercera interfaz de red tunI, dedicada a la comunicación mediante túnel VPN, le sigue asignada una dirección de clase B, por ejemplo, 172.18.1.2.

A la segunda interfaz de red eth1, conectada a la red de área local patentada, le sigue asignada una dirección de clase C, por ejemplo, 192.168.2.1.

En particular, la segunda interfaz de red eth1 puede gestionar de forma dinámica y estática todo el espacio de las direcciones de clase C, desde 192.168.0.0 a 192.168.255.255, excepto las direcciones 192.168.200.254 y 192.168.200.2 dedicadas a las interfaces eth1' y dummy0, lo que permite enrutar a todos los clientes de la red de área local patentada.

En la práctica, en cada uno de los ejemplos descritos anteriormente, las direcciones de clase C siempre son gratuitas y utilizables para las redes de área local patentadas Prop. LAN 1,. .., Prop. LAN m.

Para permitir la conexión de dos unidades cliente de dos redes de área local patentadas diferentes a través de los túneles VPN, cada una de las unidades de enrutamiento FW1, ... , FWm comprende medios de mapeo, implementados por medio de una o más reglas de mapeo de red almacenadas dentro de la propia unidad de enrutamiento adecuada para asociar las direcciones de clase A con otras redes de área local patentadas. Como se sabe, las direcciones de clase A van de 10.x.x.x a 10.255.255.255 y, por lo tanto, esto permite tener a disposición 256*256*256 direcciones.

Preferentemente, el segundo y el tercer campo disponibles de cada dirección IP de clase A están destinados a identificar las unidades de enrutamiento FW1, ... , FWm, mientras que el tercer campo disponible está destinado a identificar cada unidad de cliente CL1, ... , CLn dentro de la red de área local patentada específica Prop. LAN 1, ... , Prop. LAN m.

En particular, según una realización preferida pero no exclusiva de la invención del sistema S, las reglas de mapeo mencionadas anteriormente asocian las direcciones de clase C asociadas con cada unidad de cliente CL1, ... , CLn dentro de una red de área local patentada con las direcciones de clase A en el siguiente forma:

192.168.x.2 corresponde a 10. <campo de cortafuegos número 1>. <campo de cortafuegos número 2> .x.

Por ejemplo:

192.168.1.2 corresponde a 10.200.2.1;
192.168.2.2 corresponde a 10.200.2.2;
192.168.3.2 corresponde a 10.200.2.3;
192.168.4.2 corresponde a 10.200.2.4;
192.168.5.2 corresponde a 10.200.2.5.

Con referencia particular a una realización alternativa del sistema S que se muestra esquemáticamente a modo de ejemplo en la figura 8, se prevé el uso de redes VLAN (LAN virtual) conectadas a uno o más conmutadores de red SW.

Dicha realización particular permite gestionar de forma segura la conexión entre la unidad del cliente de la misma red de área local patentada, forzando su comunicación hacia el cortafuegos FW.

Además, se define una asociación unívoca entre cada número de puerto del conmutador de red SW y la dirección IP asignada a dicho puerto.

En particular, cada dirección IP del tipo 192.168.x.2 corresponde al aparato conectado al puerto x.

Por ejemplo:

192.168.1.2 corresponde al aparato conectado al puerto 1;
192.168.2.2 corresponde al aparato conectado al puerto 2;
192.168.3.2 corresponde al aparato conectado al puerto 3;
192.168.4.2 corresponde al aparato conectado al puerto 4;
192.168.5.2 corresponde al aparato conectado al puerto 5.

Además, solo a modo de ejemplo, las figuras 9 y 10 muestran posibles tablas de enrutamiento del sistema S.

En particular, la figura 9 muestra la posible información de enrutamiento almacenada dentro de una tabla de enrutamiento virtual RT0 de una máquina virtual VM0 del sistema S.

La figura 10 por otro lado, muestra la posible información de enrutamiento almacenada dentro de una tabla de enrutamiento RT1 de una unidad de enrutamiento FW1, ... FWm del sistema S.

De hecho, se ha determinado cómo la invención descrita logra los objetivos propuestos.

REIVINDICACIONES

1. Sistema (S) para el enrutamiento de datos a redes informáticas, que comprende:

- al menos una unidad de servidor (SRV) conectada a una red pública (I);
- al menos una red de área local (Prop. LAN 1, ... , Prop. LAN m) que tiene al menos un dispositivo cliente (CL1, ... , CLn);
- al menos una unidad de enrutamiento (FW1, ... , FWm) que tiene una primera interfaz de red (eth0) conectada a dicha red pública (I) directa o indirectamente a través de una red de área local de terceros (3p LAN 1, ... , 3p LAN m) y que tiene al menos una segunda interfaz de red (eth1) conectada a dicha red de área local (Prop. LAN 1, ..., Prop. LAN m);
- donde a dicha primera interfaz de red (eth0) se le asigna una dirección IP pública o una dirección IP privada determinada por dicha red de área local de terceros (3p LAN 1, ..., 3p LAN m);
- y donde a dicha red de área local (Prop. LAN 1, ..., Prop. LAN m) se le asigna al menos una clase predefinida de direcciones IP privadas;

caracterizado porque dicha unidad de enrutamiento (FW1, ... , FWm) comprende medios de enrutamiento automático (VMO) de datos entre dicha al menos una unidad de servidor (SRV) y dicha al menos una red de área local (Prop. LAN

1,. .., Prop. LAN m) independientemente de la dirección IP asignada a dicha primera interfaz de red (eth0), provista de al menos una primera interfaz de red virtual (eth0') conectada a dicha primera interfaz de red (eth0), con al menos una segunda interfaz de red virtual (ethl') y con medios de determinación (M) adecuados para determinar una dirección IP que se asignará a dicha segunda interfaz de red virtual (ethl') según dicha dirección IP de la primera interfaz de red virtual (eth0'), de modo que:

- dicha dirección IP de la segunda interfaz de red virtual (ethl') pertenece a una clase de direcciones IP diferentes a la clase de direcciones IP de dicha dirección IP de la primera interfaz de red virtual (eth0');
- dicha dirección IP de la segunda interfaz de red virtual (ethl') no coincide con ninguna de las direcciones IP asignables a dicha red de área local (Prop. LAN 1, ..., Prop. LAN m).

2. El sistema (S) según la reivindicación 1, **caracterizado porque** dicha unidad de enrutamiento (FW1, ... , FWm) comprende al menos una tercera interfaz de red (tun1) conectada a dicha unidad de servidor (SRV) a través de al menos una conexión VPN.

3. El sistema (S) según una o más de las reivindicaciones anteriores, **caracterizado porque** dichos medios de enrutamiento automático (VMO) comprenden al menos una máquina virtual (VMO) colocada operativamente entre dicha primera interfaz de red (eth0) y dicha segunda interfaz de red (eth1).

4. El sistema (S) según una o más de las reivindicaciones anteriores, **caracterizado porque** dicha unidad de enrutamiento (FW1,

..., FWm) comprende al menos una interfaz de red ficticia (dummy0).

5. El sistema (S) según una o más de las reivindicaciones anteriores, **caracterizado porque** dicha segunda interfaz de red virtual (ethl') está conectada a dicha interfaz de red ficticia (dummy0).

6. El sistema (S) según una o más de las reivindicaciones anteriores, **caracterizado porque** dicha máquina virtual (VMO) comprende al menos una tabla de enrutamiento virtual (RTO) que contiene información sobre el reenvío de datos a dichas primera y segunda interfaces de red virtual (eth0', eth1').

7. El sistema (S) según una o más de las reivindicaciones anteriores, **caracterizado porque** la dirección IP de dicha primera interfaz de red virtual (eth0') es la misma que dicha dirección IP de la primera interfaz de red (eth0).

8. El sistema (S) según una o más de las reivindicaciones anteriores, **caracterizado porque** dichos medios de determinación (M) son adecuados para determinar una dirección IP que se asignará a dicha interfaz de red ficticia (dummy0) según dicha dirección IP de la primera interfaz de red virtual (eth0'), de modo que:

- dicha dirección IP de la interfaz de red ficticia (dummy0) pertenece a una clase de direcciones IP diferentes a la clase de direcciones IP de dicha dirección IP de la primera interfaz de red virtual (eth0');
- dicha dirección IP de la interfaz de red ficticia (dummy0) no coincide con ninguna de las direcciones IP asignables a dicha red de área local (Prop. LAN 1, ..., Prop. LAN m).

9. El sistema (S) según una o más de las reivindicaciones anteriores, **caracterizado porque** dicha unidad de enrutamiento (FW1, ..., FWm) comprende al menos una tabla de enrutamiento (RT1) que contiene información sobre el reenvío de datos a dicha segunda interfaz de red (eth1), dicha tercera interfaz de red (tun1) y dicha interfaz

de red ficticia (dummy0).

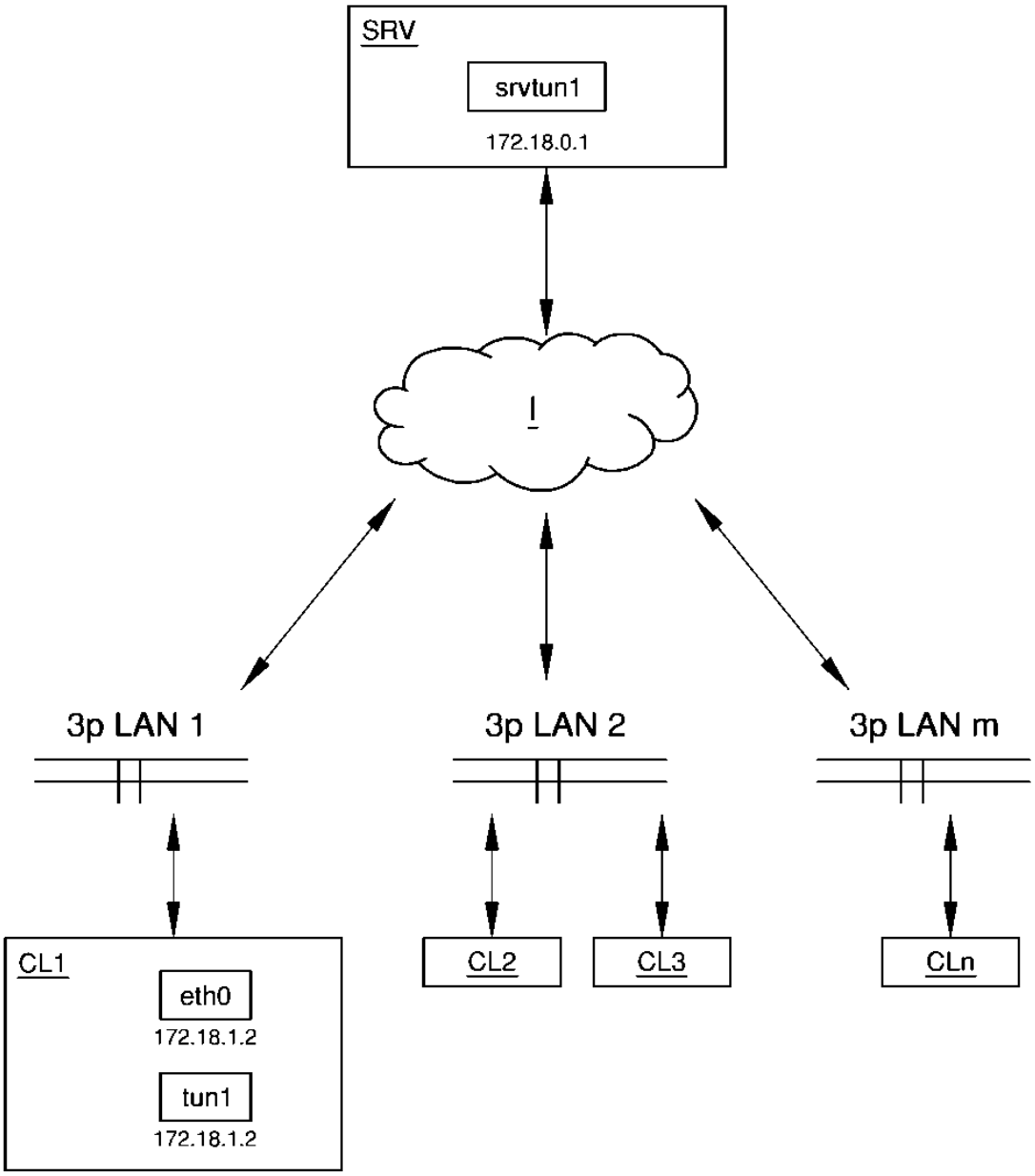

SRV
srvtun1
172.18.0.1
I
3p LAN 1
3p LAN 2
3p LAN m
CL1
eth0
172.18.1.2
tun1
172.18.1.2
CL2
CL3
CLn

Fig. 1

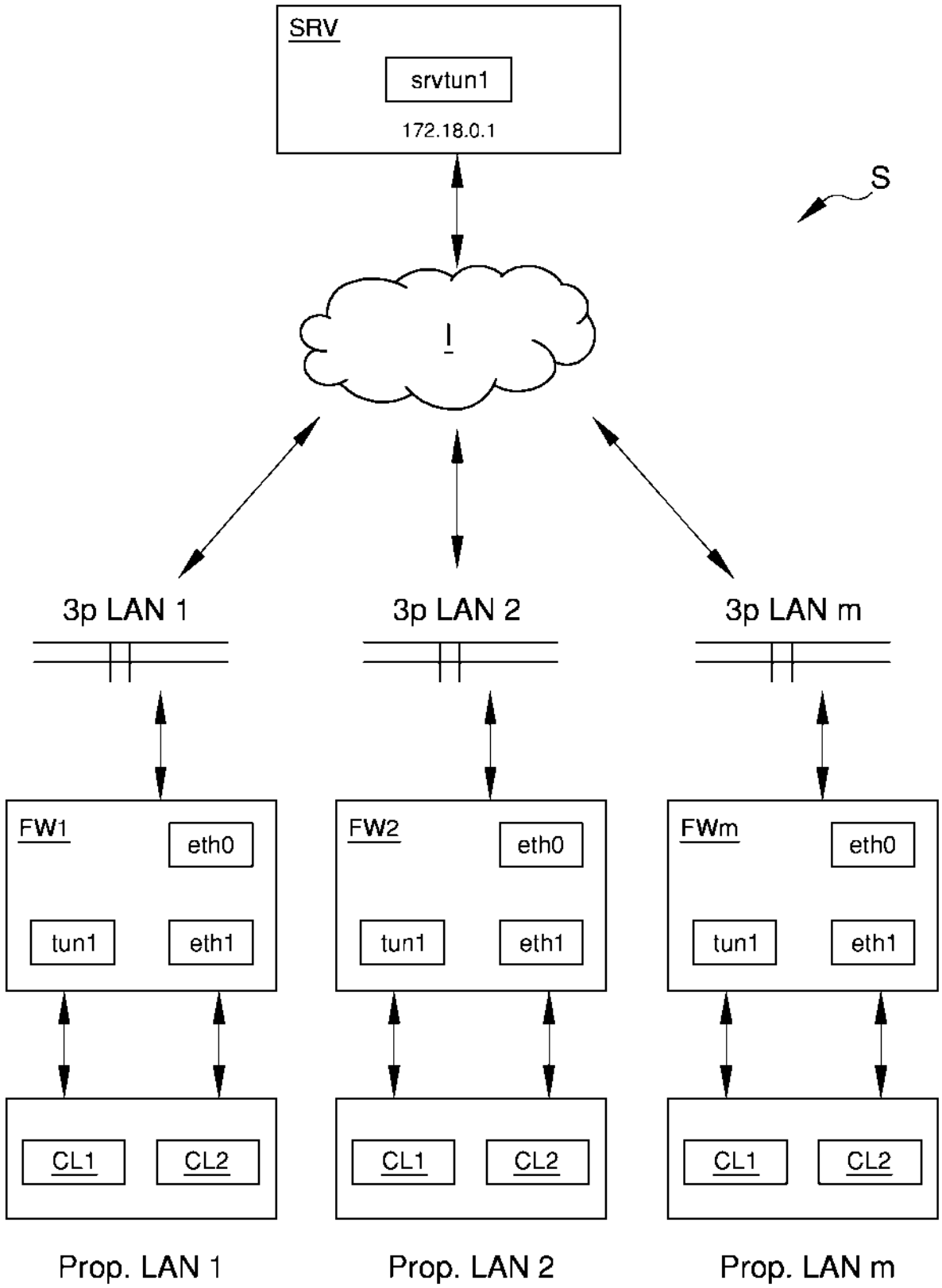

SRV
srvtun1
172.18.0.1
S
I
3p LAN 1
3p LAN 2
3p LAN m
FW1
eth0
tun1
eth1
FW2
eth0
tun1
eth1
FWm
eth0
tun1
eth1
CL1
CL2
CL1
CL2
CL1
CL2
Prop. LAN 1
Prop. LAN 2
Prop. LAN m

Fig. 2

Fig. 3

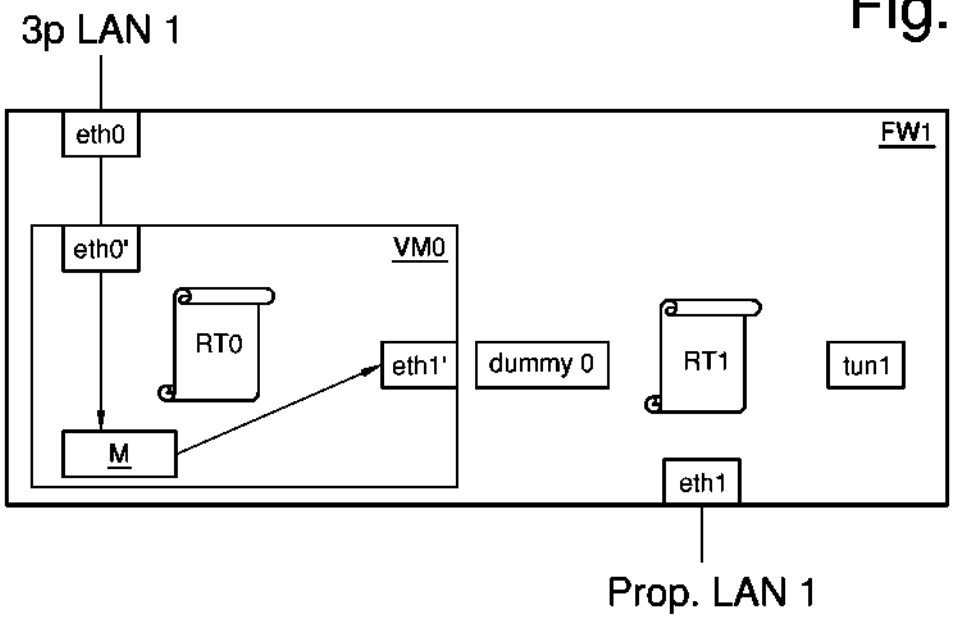

3p LAN 1
eth0
FW1
eth0'
VM0
RT0
eth1'
dummy 0
RT1
tun1
M
eth1
Prop. LAN 1

Fig. 4

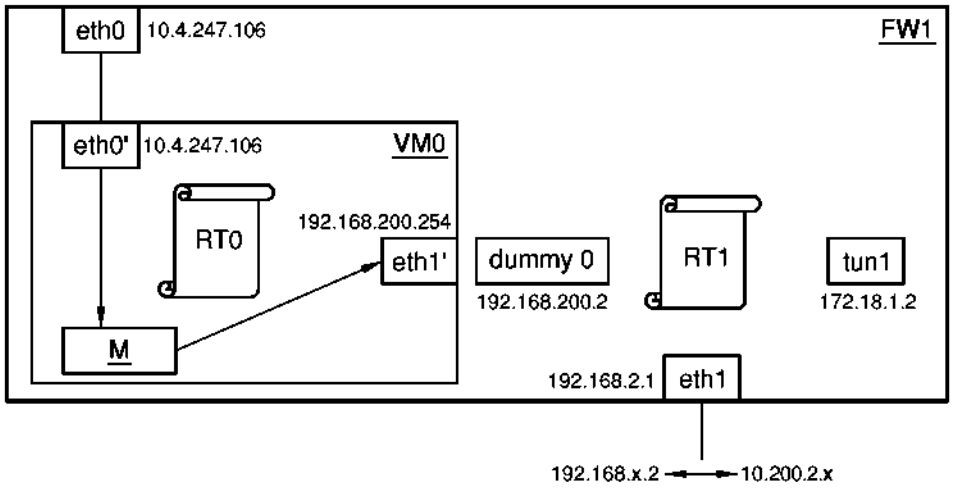

eth0
10.4.247.106
FW1
eth0'
10.4.247.106
VM0
RT0
192.168.200.254
eth1'
dummy 0
192.168.200.2
RT1
tun1
172.18.1.2
M
192.168.2.1
eth1
192.168.x.2
10.200.2.x

Fig. 5

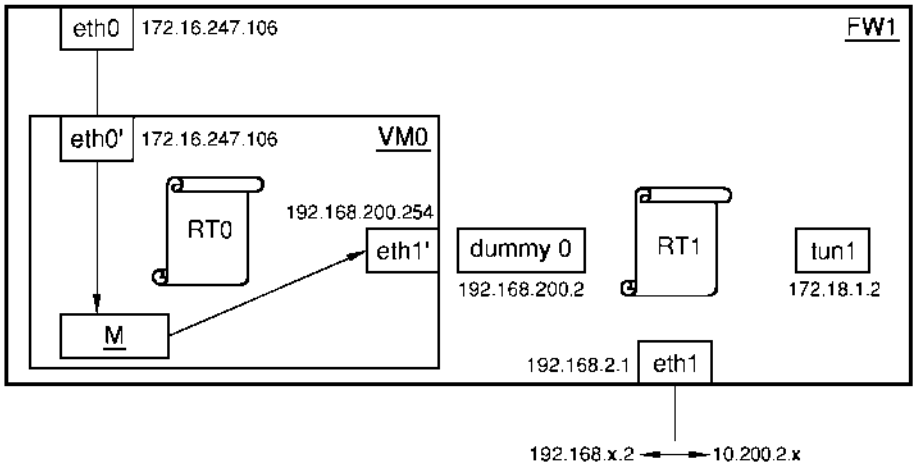


Fig. 6

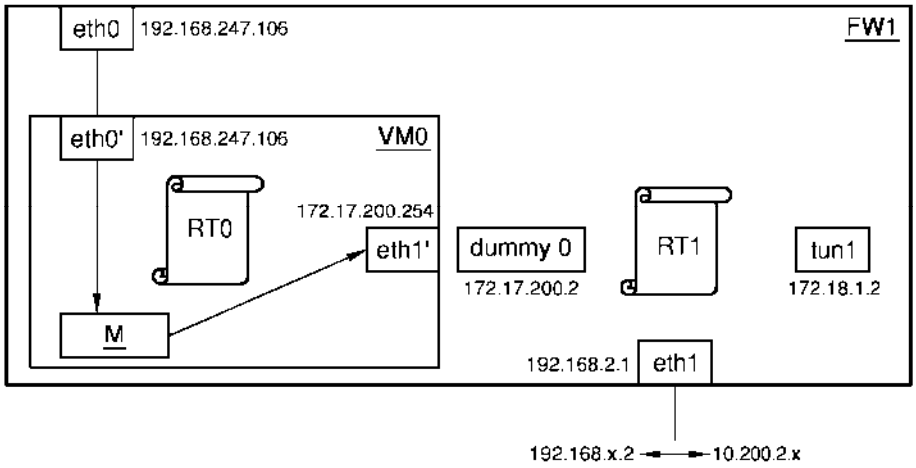
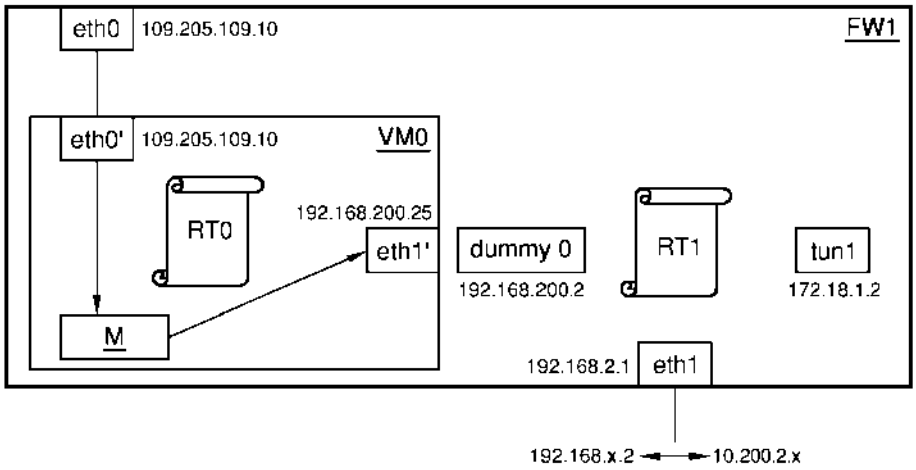


Fig. 7



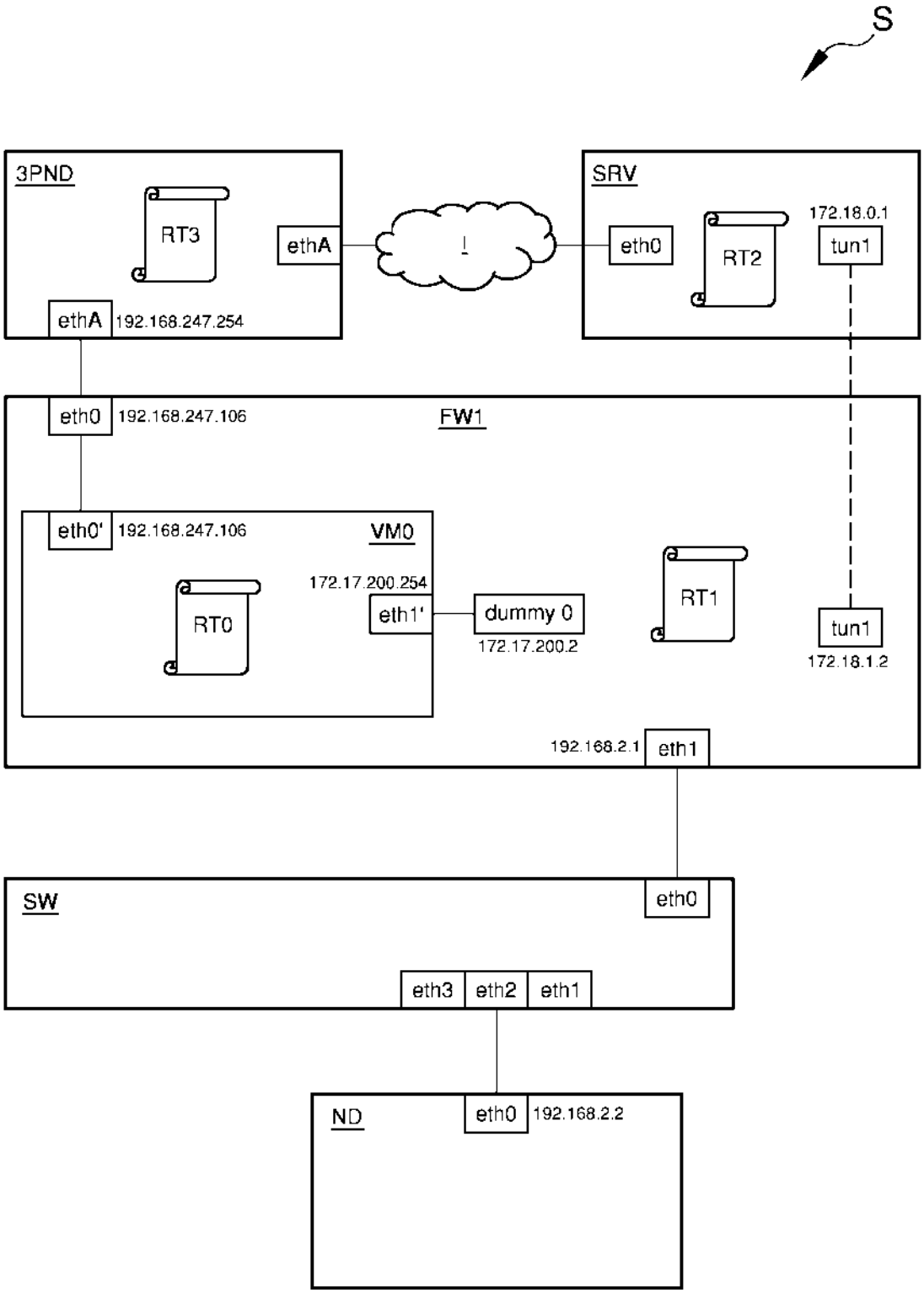

S
3PND
RT3
ethA
192.168.247.254
!
SRV
eth0
RT2
172.18.0.1
tun1
eth0
192.168.247.106
FW1
eth0'
192.168.247.106
VM0
172.17.200.254
eth1'
dummy 0
172.17.200.2
RT0
RT1
tun1
172.18.1.2
192.168.2.1
eth1
SW
eth0
eth3
eth2
eth1
ND
eth0
192.168.2.2

Fig. 8

Destino	Puerta	Genmask	Banderas	Métrica	Ref	Uso	Iface	MSS	Ventana	irtt
0.0.0.0	192.168.247.254	0.0.0.0	UG	0	0	0	eth0	0	0	0
172.17.200.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1	0	0	0
192.168.247.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0	0	0	0

Fig. 9

Destino	Puerta	Genmask	Banderas	Métrica	Ref	Uso	Iface	MSS	Ventana	irtt
0.0.0.0	172.17.200.254	0.0.0.0	UG	0	0	0	br1	0	0	0
10.0.0.0	172.18.0.1	255.0.0.0	UG	0	0	0	tun1	0	0	0
172.17.200.0	0.0.0.0	255.255.255.0	U	0	0	0	br1	0	0	0
172.18.0.1	0.0.0.0	255.255.255.255	UH	0	0	0	tun1	0	0	0
192.168.2.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1.2	0	0	0
192.168.3.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1.3	0	0	0
192.168.4.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1.4	0	0	0
192.168.5.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1.5	0	0	0
192.168.6.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1.6	0	0	0
192.168.10.0	0.0.0.0	255.255.255.0	U	0	0	0	eth1.1	0	0	0

Fig. 10