(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 362 885**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **05787057 .8**
(96) Fecha de presentación : **11.08.2005**
(97) Número de publicación de la solicitud: **1779637**
(97) Fecha de publicación de la solicitud: **02.05.2007**

(54) Título: **Procedimiento para la conmutación de paquetes IP entre redes de cliente y redes de proveedor IP a través de una red de acceso.**

(30) Prioridad: **19.08.2004 EP 04019739**

(45) Fecha de publicación de la mención BOPI:
14.07.2011

(45) Fecha de la publicación del folleto de la patente:
14.07.2011

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

(72) Inventor/es: **Stademann, Rainer y**
Theimer, Thomas

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

DESCRIPCION

Procedimiento para la conmutación de paquetes IP entre redes de cliente y redes de proveedor IP a través de una red de acceso.

Objetivo de la invención

Las redes de acceso futuras para la conexión de abonados de banda ancha deben poner a disposición anchos de banda grandes con costes menores de lo que es posible con las redes de conexión basadas en ATM habituales en la actualidad. Por este motivo las redes futuras deben basarse más en la tecnología IP y de Ethernet que actualmente se establece como solución atractiva para redes metropolitanas en el mercado.

Mientras que la arquitectura de red para redes de acceso basadas en ATM ya se definió en el foro de DSL, los trabajos para redes de acceso basadas en IP y Ethernet aún se encuentran en un estadio inicial. Se requiere una nueva arquitectura de red para la agregación basada en IP y Ethernet de conexiones de abonados de banda ancha que cumpla con los siguientes requisitos de manera óptima:

- Acceso de red dinámico con autentificación y control de acceso
- Coste de administración mínimo para configurar abonados nuevos
- Buena escalabilidad
- División de tráfico entre conexiones de abonado individuales
- Selección dinámica de diferentes servicios o clases de servicios
- Selección dinámica de diferentes proveedores de servicios
- Agregación de muchos abonados en pocos túneles lógicos específicos del servicio
- Soporte de calidad de servicio
- Alta resistencia frente a diversos ataques sobre la integridad y función de la red

El objeto de esta invención es una solución de agregación novedosa según las reivindicaciones 4 y 22 para su aplicación en particular en redes de acceso de banda ancha orientadas a Ethernet. La invención debe posibilitar sesiones IP simultáneas de un cliente final a través de una red de acceso de Ethernet a varias redes IP diferentes de proveedores de servicios IP diferentes, sin necesitar para ello PPPoE. Los operadores de red IP independientes no tienen que coordinar sus espacios de direcciones IP entre sí, los espacios de direcciones de diferentes operadores de red IP pueden solaparse o ser idénticos. Con la invención debe posibilitarse que puedan establecerse redes económicas con IP sobre Ethernet y un control de sesión basado en DHCP, mientras que al mismo tiempo puedan soportarse varios operadores de red IP independientes mediante una red de acceso.

Ejemplo del objetivo según la invención

Un ejemplo de un escenario de red en el que puede aplicarse esta invención de manera muy ventajosa se muestra en la figura 1. Este escenario contiene tres redes 110, 120, 130 de cliente. A modo de ejemplo se considera en primer lugar la red 110 de cliente. La red 110 de cliente contiene dos terminales (por ejemplo PC) 112 y 113. Éstos están conectados a un encaminador 111 IP de cliente. El encaminador 111 está conectado con una terminación 114 de red (NT). La terminación 114 de red está conectada a través de una línea 115 de acceso con el “puerto a”, 119, del nodo 140 de acceso. El nodo de acceso está conectado a través de dos enlaces 141 y 142 ascendentes con dos nodos 161 y 162 de agregación. A través de nodos 163 y 164 de agregación opcionales adicionales pueden alcanzarse finalmente dos redes 150 y 170 IP de dos operadores de red IP. Los nodos de acceso y los nodos de agregación pertenecen a la red 160 de acceso de un operador de red de acceso.

En el ejemplo existe ahora el objetivo de transportar, durante la duración de una sesión IP, paquetes IP entre el encaminador 111 del cliente y el operador 150 de red IP a través de la red de acceso, para lo cual el operador de red debe adjudicar al encaminador del cliente en primer lugar una dirección IP (en el ejemplo Ia1). Para ello el operador 150 de red debe utilizar protocolos conocidos, como por ejemplo DHCP, y elementos auxiliares adicionales, como por ejemplo un servidor 151 DHCP.

De manera correspondiente, en el ejemplo, el operador 170 de red debe poder adjudicar al encaminador 121 del cliente en la red 120 de cliente, igualmente para la duración de una sesión IP, una dirección IP Ib2 y los paquetes IP deben transportarse a través de la red 160 de acceso entre el encaminador 121 del cliente y el operador 170 de red. Las direcciones IP Ia1 e Ib2 deben poder concederse a este respecto de manera completamente independiente entre sí.

También debe ser posible que a una red de cliente se le puedan adjudicar varias direcciones IP de diferentes operadores de red IP al mismo tiempo. Se muestra un ejemplo de la red 130 de cliente. Ésta contiene dos

encaminadores 131 y 132 de cliente, estando conectados ambos por ejemplo a través de una red de Ethernet a la misma terminación 133 de red. En este caso el operador 150 de red IP debe poder adjudicar al encaminador 131 una dirección IP Ic1, mientras que al mismo tiempo el operador 170 de red IP debe poder adjudicar al segundo encaminador 132 en la misma red de cliente una dirección IP Ic2. Los paquetes IP deben poder transportarse simultáneamente a través de la red 160 de acceso por un lado entre el encaminador 131 y el operador 150 de red IP y por otro lado entre el encaminador 132 y el operador 170 de red IP.

Solución para el objetivo según la invención

La solución según la invención consiste en un procedimiento para la conmutación de los paquetes de datos mediante los datos asignados a una sesión IP. En concreto esto significa:

• Para paquetes en la dirección desde la red de cliente a un operador de red IP: los paquetes recibidos se asignan mediante su dirección de capa 2 de origen así como la dirección IP de origen a una sesión IP (en el ejemplo: M1 y Ia1). Todos los paquetes de una sesión IP se retransmiten a la dirección de capa 2 del operador de red IP asignada a la sesión (en el ejemplo: M7).

• Para paquetes en la dirección desde un operador de red IP a la red de cliente: los paquetes recibidos se asignan mediante su dirección de capa 2 de origen así como la dirección IP de destino a una sesión IP (en el ejemplo: M7, Ia1). Todos los paquetes de una sesión IP se retransmiten a la dirección de capa 2 de la red de cliente asignada a la sesión (en el ejemplo: M1).

Objetivo adicional según la invención

Además del objetivo de la invención mencionado se obtiene en muchas redes un objetivo adicional, relacionado con el mismo, que a continuación se denomina también objetivo adicional.

Para clientes de empresas, los operadores de red ofrecen a menudo servicios de red continuos en la capa 2. Ejemplos son servicios ATM (por ejemplo servicios de circuito virtual permanente (PVC, *permanent virtual circuit*), servicios de línea arrendada TDM (por ejemplo, servicios E1/T1) y recientemente servicios de Ethernet metropolitanos, como especifica por ejemplo Metro Ethernet Forum (MEF). En estos servicios se transportan células o tramas de capa 2 de los protocolos respectivos entre los puntos de traspaso del cliente de empresa generalmente sin modificar a través de la red del operador.

Para clientes privados estos servicios basados en capa 2 a menudo no son necesarios, porque en el caso de los clientes privados se trata en la mayoría de los casos de servicios de acceso a Internet o de servicios de acceso a aplicaciones basándose en el protocolo IP, como por ejemplo aplicaciones de vídeo o VoIP. Estas aplicaciones requieren el transporte de paquetes IP del cliente privado a uno o varios operadores de red IP, dado el caso también el acceso simultáneo a varios operadores de red IP. Para estos servicios es suficiente el transporte de paquetes IP entre la red de cliente y el operador de red IP respectivo. Si bien para ello basta con un servicio basado en capa 2, sin embargo, no es necesario. Puesto que en particular con Ethernet como capa 2 están asociados tanto problemas de escalado (por ejemplo, sólo 4096 etiquetas VLAN) como riesgos de seguridad diversos (por ejemplo suplantación de identidad de dirección MAC, inundación de direcciones MAC), en particular para los clientes privados es ventajoso terminar la capa 2 en el nodo de acceso y transportar los propios paquetes IP al operador de red IP. Así son especialmente ventajosas soluciones que no transportan las tramas de Ethernet completas desde la red de cliente al operador de red IP, sino sólo su contenido de capa 3, concretamente el paquete IP.

Soluciones conocidas hasta ahora para el objetivo adicional mencionado

a) La arquitectura para redes de acceso de banda ancha basadas en ATM con soporte de QoS se describe por ejemplo en las especificaciones TR-058 y TR-059 del foro de DSL. Estas redes se basan en conexiones virtuales de ATM configuradas de manera fija (PVC) entre la conexión de abonado y un nodo de acceso de red IP central (servidor de acceso de banda ancha (BAS)). El BAS (*Broadband Access Server*) asume el control de acceso y la autentificación de los abonados así como la selección del servicio. Esta arquitectura tiene diferentes desventajas:

• Las conexiones (PVC) entre abonados y BAS deben configurarse tanto en la red ATM como en el BAS.

• Por cada clase de QoS se requiere en cada caso un PVC de ATM propio

• El tráfico entre abonados debe pasar siempre a través del BAS

• Los productos BAS actuales no permiten servicios económicos con tasas de transmisión de datos elevadas (por ejemplo varios canales de vídeo por cada abonado)

b) Un procedimiento que para redes de acceso a Ethernet reduce parcialmente el problema de seguridad se ha dado a conocer en el borrador de IETF draft-melsen-mac-forced-fwd-02.txt con el título “MAC Forced Forwarding: An ARP proxy method for ensuring traffic separation between hosts sharing an Ethernet Access Network” de T.Melsen y S.Blake. En este procedimiento el nodo de acceso comprueba la dirección de destino MAC en el lado del abonado utilizada en las tramas de Ethernet con respecto a su admisibilidad. Un proxy ARP en el nodo de acceso devuelve

adicionalmente, en el caso de peticiones ARP en el lado del abonado, sólo direcciones MAC admisibles. Este procedimiento no soluciona el problema del acceso simultáneo a diferentes redes IP independientes.

c) Se conoce otro procedimiento con el nombre de "(Virtual) MAC Address Translation". (Véase por ejemplo ITU Contribution COM 13 - D 447 - E de ZTE Corporation de febrero de 2004). En este enfoque las direcciones MAC de los puntos de extremo de capa 2 en el lado del abonado se convierten por el nodo de acceso unívocamente en direcciones MAC "virtuales", que determina el operador de red de acceso. Las direcciones MAC de los puntos de extremo de capa 2 en el lado de red se mantienen sin modificar durante el paso de las tramas de Ethernet a través del nodo de acceso. En particular, en este enfoque de solución es desventajoso que para cada dirección MAC en el lado del abonado se requiere una dirección MAC virtual adicional en la red. Este procedimiento tampoco soluciona el problema del acceso simultáneo a diferentes redes IP independientes.

d) En un procedimiento adicional, que corresponde al estado de la técnica, una función de encaminador IP en el nodo de acceso termina la capa 2 y encamina los paquetes IP de la capa 3 mediante las direcciones IP (encaminamiento IP). En esta solución se producen las siguientes desventajas:

i. El operador de red de acceso debe convertirse en operador de red IP

ii. Las direcciones IP no pueden concederlas operadores de red IP independientes

iii. El número de encaminadores IP aumenta aproximadamente un orden de magnitud de uno a dos en comparación con las redes IP actuales por lo que aumenta considerablemente el esfuerzo para operar la red IP.

iv. El encaminador IP debe dominar protocolos de encaminamiento complejos.

e) Una solución conocida adicional utiliza el protocolo PPPoE o PPPoA entre la red de cliente y el operador de red IP. En este caso se establecen túneles PPP hacia la red IP respectiva, en la que se transportan los paquetes IP. En esta solución son desventajosos los altos costes para la terminación de PPPoE/ PPPoA en un servidor de acceso de banda ancha (BAS) así como problemas de seguridad en redes de acceso basadas en Ethernet.

El documento WO/03/067821 A1 describe la asignación de proveedores de servicios a redes de cliente en un sistema de acceso con ayuda de direcciones MAC dinámicas.

Solución del objetivo adicional según la invención

La figura 2 muestra esquemáticamente el funcionamiento de un nodo de acceso, que según la invención funciona como conmutador de servicio IP (*IP Service Switch*). En la red 260 de acceso para cada operador de red IP soportado se implementan una o varias "conexiones de servicio IP" entre uno o varios nodos de acceso y uno o varios encaminadores de borde IP (*IP Edge Router*) de los operadores de red IP. En el ejemplo de la figura 2 una conexión 242 de servicio IP está configurada entre los nodos 240 y 241 de acceso y el encaminador 250 de borde para el operador 1 de red. De manera correspondiente una conexión 243 de servicio IP adicional está configurada entre los mismos nodos 240 y 241 de acceso y el nodo 270 de borde IP.

Las conexiones de servicio IP vienen dadas en el caso más sencillo únicamente por una dirección de destino de capa 2 de la interfaz en la red de acceso a un encaminador de borde IP del operador de red IP respectivo. Se trata en el ejemplo de la figura 2 de las direcciones M7 y M8 de capa 2. En redes de Ethernet, M7 y M8 son las direcciones MAC de la interfaz de Ethernet en los encaminadores 250 y 25 de borde. Característico de una conexión de servicio IP en el sentido de esta invención es el transporte de paquetes IP entre uno o varios conmutadores de servicio IP por un lado y uno o varios encaminadores de borde por otro lado, que mediante direcciones de capa 2 pueden alcanzarse por el elemento de red según la invención (conmutador de servicio IP) (el propio conmutador de servicio IP no requiere para ello una dirección IP propia). Como las conexiones de servicio IP están definidas por tanto sobre la capa 2, las direcciones IP de los paquetes IP transportados entre diferentes conexiones de servicio IP pueden seleccionarse independientemente entre sí.

Por motivos de seguridad y para poder garantizar de manera más sencilla calidades de servicio específicas en la red de acceso, a menudo es ventajoso utilizar atributos de capa 2 adicionales para implementar conexiones de servicio IP. En redes de Ethernet puede utilizarse para ello por ejemplo ventajosamente la técnica VLAN según la norma IEEE 802.1q. Para ello el conmutador 240 de servicio IP en el ejemplo de las figuras 2, 3, 4 coloca junto a la dirección MAC de destino M7 o M8 la etiqueta 2011 ó 2022 VLAN de la conexión de servicio IP. Esto es ventajoso porque así pueden adjudicarse recursos de la red de acceso a una conexión de servicio IP en los conmutadores L2 posteriores del operador de red de acceso sólo mediante la etiqueta VLAN. Ésta es una función muy extendida en muchos conmutadores de capa 2. También son concebibles realizaciones de conexiones de servicio IP mediante MPLS (trayecto de conmutación de etiquetas, *Label Switched Path*) o la técnica IP (por ejemplo L2TP, RFC 2661).

Adicionalmente en la figura 2 se muestra cómo el nodo de acceso conmuta paquetes IP entre sesiones IP del puerto en el lado del cliente por un lado y las conexiones de servicio IP por otro lado. Por ejemplo los paquetes IP entrantes de la sesión IP en la línea 215 de acceso (correspondiente al puerto 1 en la figura 1) se conmutan a la conexión 242 de

servicio IP y, a la inversa, los paquetes IP entrantes en la conexión 242 de servicio IP con dirección IP Ia1 se conmutan a la sesión IP de la línea 215 de acceso.

En el ejemplo de la línea 235 de acceso se supone que los paquetes IP de las dos sesiones IP diferentes entre los encaminadores 231 y 232 de cliente por un lado y el nodo 240 de acceso por otro lado, se transportan por ejemplo a través de una VLAN de Ethernet distinta en cada caso (por ejemplo “1001” y “1002”) según la norma IEEE 802.1q o por ejemplo a través de distintos PVC de ATM. Los paquetes IP entrantes en tramas de capa 2 de la línea 235 de acceso con dirección de capa 2 M3 de origen y procedentes de la VLAN “1001” pertenecen a una sesión IP y se conmutan a la conexión 242 de servicio IP y los paquetes IP entrantes de la línea 235 de acceso con dirección de capa 2 M4 de origen y procedentes de la VLAN “1002” se conmutan a la conexión 243 de servicio IP. A la inversa, los paquetes IP procedentes del nodo de acceso en la conexión 242 de servicio IP con dirección IP Ic1 se empaquetan en tramas de capa 2 con VLAN “1001” y dirección de capa 2 M3 de destino y se conmutan a la línea 235 de acceso. Los paquetes IP entrantes en la conexión 243 de servicio IP con dirección IP Ic2 se conmutan en tramas de capa 2 con VLAN “1002” y dirección de capa 2 M4 de destino de la línea 235 de acceso.

Son características de una sesión IP en el sentido de esta invención

a) al menos una dirección de capa 2, con la que puede alcanzarse un equipo en una red de cliente, y

b) al menos una dirección IP asociada a esta dirección de capa 2 mencionada.

En la mayoría de los casos es ventajoso para la caracterización de una sesión IP añadir adicionalmente uno o varios puertos físicos del elemento de red según la invención a través de los cuales puede alcanzarse el equipo mencionado en la red de cliente mencionada. Por ejemplo, diferentes equipos pueden emplear por tanto las mismas direcciones de capa 2 si éstas pueden alcanzarse a través de diferentes puertos físicos.

Las especificaciones para la conmutación IP basada en sesión pueden mantenerse por el nodo de acceso en forma de tabla. Un ejemplo se muestra en la figura 3. En esta tabla se asignan sesiones IP en el lado del cliente final a conexiones de servicio IP en el lado de la red.

Se definen sesiones IP en el ejemplo mediante un puerto físico en el lado del cliente en el conmutador de servicio IP (en el ejemplo a, b o c) y mediante una dirección de capa 2 en el lado del cliente y la dirección IP asignada. Adicionalmente, atributos adicionales pueden definir una sesión IP. Entre éstos se encuentra, por ejemplo, una etiqueta VLAN en el lado del cliente (en la figura 4 en la columna “C-VLAN” de la tabla).

Se definen conexiones de servicio IP en el ejemplo mediante una dirección de capa 2 en el lado de la red de un punto de extremo de la conexión de servicio IP. En el ejemplo de la figura 3 son las direcciones M7 y M8 de los puntos de extremo en los encaminadores 151 y 171 de borde IP de los dos operadores 150 y 170 de red IP. Opcionalmente otros atributos pueden caracterizar una conexión de servicio. En el ejemplo de la especificación de conmutación de la figura 3 están asignadas en cada caso una etiqueta VLAN (en la figura 4 en la columna “S-VLAN” de la tabla) según IEEE 802.1q a una conexión de servicio.

Con ayuda de las especificaciones de conmutación predefinidas en la tabla de la figura 3 pueden realizarse las conversiones de dirección y atributo necesarias por el conmutador de servicio IP. Además de estas conversiones pueden tener lugar comprobaciones adicionales del tráfico, para garantizar por ejemplo la integridad y la seguridad de la red. Por ejemplo pueden rechazarse paquetes IP de un cliente final, si éstos no llevan la dirección IP fuente predefinida en una especificación de conmutación. Las especificaciones de conmutación pueden predefinirse administrativamente completa o parcialmente o se aprenden automáticamente en el establecimiento de una sesión IP mediante aplicación de protocolos para la autenticación, autorización y concesión de direcciones IP tal como 802.1x, DHCP, RADIUS en el nodo de acceso.

La figura 4 muestra, para el caso de Ethernet como protocolo de capa 2, en una forma ventajosa de la invención cómo se usan las especificaciones de conmutación de la figura 3 por un elemento de red para convertir las direcciones de capa 2 y los atributos de las tramas de Ethernet en la conmutación de los paquetes entre la sesión IP y la conexión de servicio IP.

A diferencia del planteamiento de solución conocido 1d), en esta forma ventajosa del procedimiento según la invención pueden correlacionarse diferentes direcciones M1 a M4 MAC en el lado del abonado con la misma dirección de red M6. En el ejemplo de la figura 4 se sustituye la dirección M1 fuente en la trama 301 en el conmutador de servicio IP por la dirección MAC M6 en la trama 302. Al mismo tiempo se sustituye la dirección M5 de destino en el conmutador de servicio IP por la dirección M7 de destino del encaminador 250 de borde. A la inversa, en el ejemplo de la figura 3 en sentido inverso (tramas 311, 312, 313) la dirección M7 fuente en la trama 312 se sustituye por la dirección M5 fuente del conmutador de servicio IP, antes de enviar la trama al encaminador 111 del cliente. De manera correspondiente se sustituye la dirección M6 de destino en la trama 312 por la dirección M1 del encaminador 111 del cliente.

De este modo se aumenta la escalabilidad, ya que la red de acceso no tiene que aprender las direcciones MAC M1 a M4 en el lado del abonado. Asimismo se rechazan ataques tales como “inundación de direcciones MAC” en la red de acceso. En sentido inverso, las direcciones MAC M7 y M8 en el lado de la red de los encaminadores 250 y 270 de borde

no se retransmiten a los abonados sino que se sustituyen por una dirección M5 MAC del conmutador de servicio IP. De este modo también se aumenta la seguridad de la red, ya que de este modo las direcciones de los encaminadores de borde permanecen ocultas para los abonados.

También es ventajoso que en el conmutador 240 de servicio IP en dirección a la red se coloque como atributo adicional de la conexión de servicio IP una etiqueta VLAN (en el ejemplo de la figura 4 la etiqueta VLAN “2011”). Mediante esta etiqueta VLAN pueden reservarse en un conmutador de capa 2 posterior recursos tales como por ejemplo ancho de banda en una línea de conexión. En dirección al cliente final se elimina la etiqueta VLAN “2011” del conmutador de servicio IP. Son posibles otras implementaciones de conexiones de servicio IP por ejemplo mediante trayectos MPLS (LSP, *Labeled Switched Path*) y se trata tan sólo de variaciones de esta invención.

La figura 5 muestra en una forma ventajosa adicional cómo puede utilizarse la norma IEEE 802.1x para determinar una primera parte de la especificación de conmutación. El usuario se autentifica y autoriza en primer lugar según el estado de la técnica mediante los protocolos 802.1x y RADIUS, así como una base de datos AAA (*Authentication, Authorization, Accounting*; autenticación, autorización, contabilidad). A este respecto el usuario puede indicar, por ejemplo mediante indicación de un nombre de dominio plenamente calificado (FQDN, *Fully Qualified Domain Name*) el servicio y el operador de red IP deseados. Mediante el FQDN se retransmite la petición RADIUS a través del proxy 501 al servidor 502 AAA del operador de red IP. Éste comprueba las credenciales (por ejemplo contraseña) y devuelve en caso de éxito un mensaje RADIUS, que contiene información sobre el servicio solicitado (*service profile*; perfil de servicio). Con ayuda de esta información, el conmutador 503 de servicio IP puede determinar la conexión de servicio IP correspondiente, que viene dada en el ejemplo mediante la dirección de capa 2 M7 y la S-VLAN “2011”. El puerto físico (c), la C-VLAN (1001) y la dirección de capa 2 del terminal del cliente final se derivan por el conmutador de servicio IP a partir de las tramas 504, 505 y 506 802.1x.

La figura 6 muestra cómo puede emplearse en el conmutador de servicio IP un perfil de servicio (en el ejemplo de la figura 5 el perfil de servicio S1 del mensaje 507) para ejecutar de manera controlada para la respectiva sesión IP una política de tráfico. Para ello, el conmutador de servicio IP tiene por ejemplo una tabla tal como en la figura 6, en la que se definen diferentes perfiles de servicio. Así, el perfil S1 define un servicio IP con una clase de tráfico “mejor esfuerzo” y “tiempo real”, liberándose en cada caso los anchos de banda máximos indicados por el conmutador de servicio IP para una sesión IP con el perfil S1. De manera correspondiente, S2 define un perfil con sólo una clase de tráfico “mejor esfuerzo” con los anchos de banda máximos indicados.

La figura 7 muestra, para el caso de IPv4 cómo se emplean mensajes DHCP para establecer una sesión IP. Aquí, se usa en el conmutador de servicio IP un agente de retransmisión DHCP, a través del cual se dirigen todos los mensajes DHCP entre los usuarios del servicio y la red. A partir del intercambio de mensajes 601 a 608 el agente de retransmisión puede deducir la especificación de conmutación necesaria y rellenar con ello la tabla 610. Opcionalmente en la especificación de conmutación puede contenerse el tiempo de arrendamiento DHCP y supervisarse por el conmutador de servicio IP. En el ejemplo el tiempo de arrendamiento tiene una duración de 1500 s.

La figura 8 muestra cómo, una vez transcurrido el tiempo de arrendamiento, el conmutador de servicio IP libera la sesión IP. Para ello el agente de retransmisión envía mensajes *DHCP Release* al terminal y al servidor DHCP en el lado de la red. Adicionalmente se borran en la tabla de las especificaciones (710) de conmutación los datos de la sesión IP. A continuación no se retransmite ningún paquete IP con la dirección Ic1 de origen desde este puerto de sesión en la red.

La figura 9 muestra cómo se responden, en el caso de IPv4, peticiones ARP del usuario 801 o peticiones ARP del encaminador 803 de borde IP por el conmutador de servicio IP. En ambos casos y para cada una de las direcciones IP “any”, el conmutador de servicio IP responde a peticiones ARP con su respectiva dirección MAC. Se trata de M5 en el caso de la respuesta 802 ARP y M6 en el caso de la respuesta 804 ARP. Estas respuestas garantizan que tanto el equipo 810 en el lado del usuario como el encaminador 811 IP en el lado de la red usan las direcciones MAC del conmutador de servicio IP para transmitir los paquetes IP.

La figura 10 muestra la estructura de la dirección IP para el caso especial IPv6. Aquí, surge el problema de que la dirección IP contiene un identificador de interfaz (*interface identifier*) que adjudica el propio cliente. El identificador de interfaz puede corresponder a la dirección de capa 2 del cliente, aunque también puede elegirse aleatoriamente. Por tanto surge el problema de que también en caso de ID de interfaz idénticos de varios clientes debe generarse una dirección IP unívoca. Según la invención este problema se resuelve de modo que el propio conmutador de servicio IP puede adjudicar un prefijo IP local que se elige en cada caso individual de modo que se genere una dirección IP unívoca. A cada conmutador de servicio IP en una subred se le deben adjudicar por tanto varios prefijos locales, de modo que la combinación de prefijo local y global siempre dé una dirección IP unívoca, independientemente del respectivo identificador de interfaz. El cliente obtiene esta asignación o bien a través de DHCP o bien mediante *stateless address autoconfiguration* (configuración automática de dirección sin estado) (*router discovery*, descubrimiento de encaminador).

Ventajas que se derivan de la solución del objetivo de la invención

a) Conmutación IP basada en sesión en lugar de encaminamiento IP en el conmutador de servicio IP. Con ello, el operador de red de acceso no tiene que ser al mismo tiempo operador de red IP, es decir no necesita direcciones IP

propias para los abonados. Al mismo tiempo, pueden soportarse varios operadores de red IP en la misma red de acceso. Un abonado puede mantener también simultáneamente varias sesiones IP con diferentes operadores de red IP. Además se evita que el número de nodos IP aumente de uno a dos órdenes de magnitud en comparación con las redes IP habituales actuales.

b) La invención posibilita una arquitectura de red para redes de acceso basadas en IP/Ethernet, que transfiere la función del BAS a la red de acceso y la modifica de modo que el control de acceso pueda realizarse con métodos basados en IP/ Ethernet. Por un lado ya no existe de este modo la necesidad de un BAS separado, lo que lleva a ahorros de costes significativos. Por otro lado, el control de acceso se acerca más al abonado, con lo cual se obtiene una alta seguridad de red y se posibilita un mejor soporte de QoS.

Ventaja que se deriva de la solución del objetivo adicional de la invención

Terminación de capa 2. En particular al usar Ethernet como capa 2 se conocen una pluralidad de posibles ataques a la función y la integridad de la red. Mediante la terminación de la capa 2 en el conmutador de servicio IP estos ataques se reducen en gran medida para los nodos de red situados tras el conmutador de servicio IP.

REIVINDICACIONES

1. Procedimiento para la conmutación de paquetes IP entre redes (110, 120, 130) de cliente y redes (150, 170) de proveedor IP a través de una red (160) de acceso, según el cual

a) las redes de cliente están conectadas a puertos de nodos de acceso (conmutador de servicio IP) de la red de acceso,

b) se definen sesiones IP entre las redes de cliente y las redes de proveedor IP mediante la asignación de direcciones IP a las direcciones de capa 2 asignadas a las redes de cliente en los puertos de acceso de los nodos de acceso,

c) se definen conexiones de servicio IP entre los nodos de acceso de la red de acceso y las redes de proveedor IP mediante direcciones de capa 2 asignadas a las redes de proveedor IP,

d) se asigna una sesión IP activa al menos a una conexión de servicio IP

e) pueden asignarse varias sesiones IP activas a la misma conexión de servicio IP,

caracterizado porque

en la conmutación, debido a la asignación mencionada entre sesiones IP y conexiones de servicio IP,

- se sustituyen (una) dirección (direcciones) de capa 2 y/o atributos de tramas, en los que se transmiten paquetes IP de una sesión IP a los nodos de acceso, completa o parcialmente por la(s) dirección (direcciones) de capa 2 y/o atributos asignados a la conexión de servicio IP respectiva, y/o

- se sustituyen (una) dirección (direcciones) de capa 2 y/o atributos de tramas, en los que se transmiten paquetes IP de conexiones de servicio IP a los nodos de acceso, completa o parcialmente por la(s) dirección (direcciones) de capa 2 y/o atributos asignados a la sesión IP respectiva.

2. Procedimiento según la reivindicación 1, caracterizado porque el nodo de acceso aprende la asignación de una sesión IP a una conexión de servicio IP durante el establecimiento de la sesión IP con ayuda de mensajes de establecimiento de sesión.

3. Procedimiento según la reivindicación 1, caracterizado porque la asignación de una sesión IP a una conexión de servicio IP se modifica después del establecimiento de sesión mediante mensajes de modificación de sesión.

4. Procedimiento según la reivindicación 1, caracterizado porque un paquete IP viene dado por un paquete IPv4 o un paquete IPv6.

5. Procedimiento según la reivindicación 1, caracterizado porque una sesión IP se registra adicionalmente con ayuda de uno o varios puertos físicos del nodo de acceso.

6. Procedimiento según la reivindicación 1, caracterizado porque, independientemente de la dirección IP objetivo en paquetes IP entrantes de una sesión IP, todos los paquetes IP de una sesión IP se conmutan a la misma conexión de servicio IP o a las mismas conexiones de servicio IP.

7. Procedimiento según la reivindicación 1, caracterizado porque se determina una dirección de capa 2 mediante una dirección MAC de Ethernet.

8. Procedimiento según la reivindicación 1, caracterizado porque se determina una dirección de capa 2 mediante un par VPI/VCI de un tramo ATM.

9. Procedimiento según la reivindicación 1, caracterizado porque se determina una dirección de capa 2 mediante una o varias etiquetas MPLS de un tramo MPLS.

10. Procedimiento según la reivindicación 1, caracterizado porque se determina una dirección de capa 2 mediante un DLCI de un tramo *Frame Relay*.

11. Procedimiento según la reivindicación 1, caracterizado porque una sesión IP se caracteriza adicionalmente por direcciones IP adicionales (por ejemplo, una subred IP) y/o uno o varios de los siguientes atributos

a) una etiqueta VLAN de Ethernet

b) un punto de código .1p de Ethernet

c) un punto de código DSCP del paquete IP que va a conmutarse

d) una dirección de capa 2 del nodo de acceso.

12. Procedimiento según la reivindicación 1, caracterizado porque se determina una conexión de servicio IP adicionalmente mediante uno o varios de los siguientes atributos

a) una etiqueta VLAN de Ethernet

b) un punto de código .1p de Ethernet

c) un punto de código DSCP

d) una dirección de capa 2 del nodo de acceso.

13. Procedimiento según la reivindicación 1, caracterizado porque se establecen sesiones IP mediante mensajes *IPv6 Router Discovery / Stateless Address Autoconfiguration*.

14. Procedimiento según la reivindicación 1, caracterizado porque se establecen sesiones IP mediante mensajes DHCP.

15. Procedimiento según la reivindicación 1 y 2, caracterizado porque los mensajes de modificación de sesión vienen dados por mensajes *DHCP_Request*.

16. Procedimiento según la reivindicación 1, caracterizado porque en el establecimiento de sesión IP se utilizan adicionalmente mensajes 802.1x.

17. Procedimiento según una de las reivindicaciones 1 a 16, caracterizado porque el nodo de acceso realiza una ejecución de políticas ("*Policy Enforcement*") para una sesión IP basándose en información de los mensajes de establecimiento de sesión o de modificación de sesión.

18. Procedimiento según la reivindicación 14, caracterizado porque se supervisa un tiempo de arrendamiento DHCP por el nodo de acceso para las sesiones IP y, una vez transcurrido el tiempo de arrendamiento, se interrumpe la sesión IP.

19. Procedimiento según una de las reivindicaciones 1 a 18, caracterizado porque se implementa un *IPv6 Neighbor Discovery Proxy* en el nodo de acceso, mediante el cual se responde a peticiones *Neighbor Discovery* en el lado del cliente y de la red con una dirección de capa 2 del nodo de acceso.

20. Procedimiento según una de las reivindicaciones 1 a 18, caracterizado porque se implementa un *ARP-Proxy* en el nodo de acceso, mediante el cual se responde a peticiones ARP en el lado del cliente y de la red con una dirección de capa 2 del nodo de acceso.

21. Procedimiento según la reivindicación 1, caracterizado porque se asigna a una sesión IP además del prefijo de dirección IP global también uno local.

22. Nodo (140) de acceso de una red (160) de acceso, configurado de modo que

a) al mismo están conectadas redes (110, 120, 130) de cliente a través de puertos de la red de acceso,

y porque el nodo

b) registra sesiones IP entre las redes de cliente y las redes (150, 170) de proveedor IP mediante la asignación de direcciones IP a las direcciones de capa 2 asignadas a las redes de cliente en los puertos de acceso del nodo de acceso,

c) determina conexiones de servicio IP entre las redes de acceso y las redes de proveedor IP mediante las direcciones de capa 2 asignadas a las redes de proveedor IP,

d) asigna una sesión IP activa al menos a una conexión de servicio IP

e) puede asignar varias sesiones IP activas a la misma conexión de servicio IP,

caracterizado porque

el nodo (140) de acceso, debido a la asignación mencionada entre sesiones IP y conexiones de servicio IP,

- sustituye (una) dirección (direcciones) de capa 2 y/o atributos de tramas, en los que se transmiten paquetes IP de una sesión IP al nodo de acceso, completa o parcialmente por la(s) dirección (direcciones) de capa 2 y/o atributos asignados a la conexión de servicio IP respectiva, y/o

- sustituye (una) dirección (direcciones) de capa 2 y/o atributos de tramas, en los que se transmiten paquetes IP de conexiones de servicio IP al nodo de acceso, completa o parcialmente por la(s) dirección (direcciones) de capa 2 y/o atributos asignados a la sesión IP respectiva.

23. Nodo de acceso según la reivindicación 22, caracterizado porque aprende la asignación de una sesión IP a una conexión de servicio IP durante el establecimiento de la sesión IP con ayuda de mensajes de establecimiento de sesión.

24. Nodo de acceso según la reivindicación 22, caracterizado porque modifica la asignación de una sesión IP a una conexión de servicio IP después del establecimiento de sesión mediante mensajes de modificación de sesión.

25. Nodo de acceso según la reivindicación 22, caracterizado porque registra una sesión IP adicionalmente con ayuda de uno o varios puertos físicos del nodo de acceso.

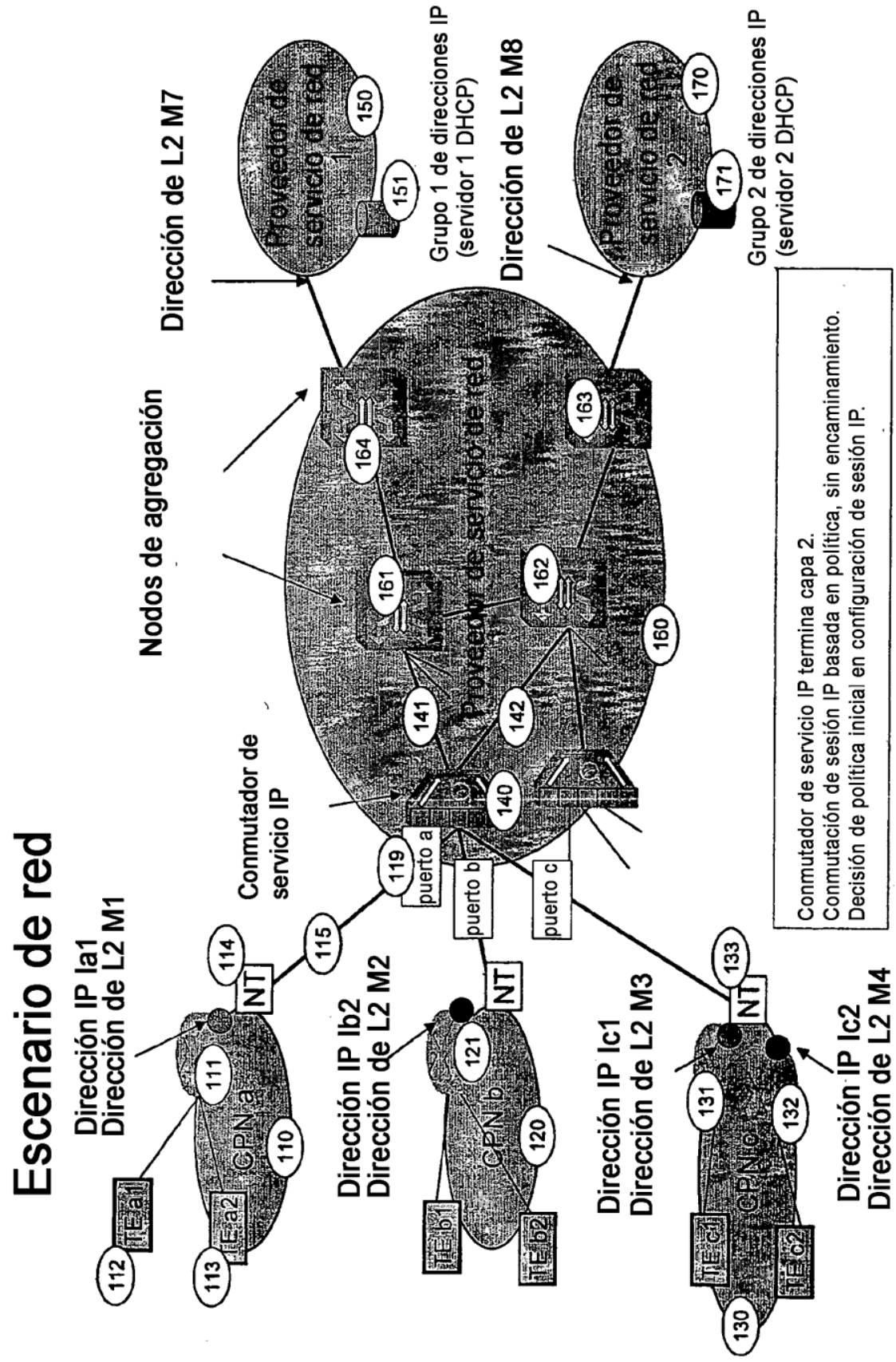

Escenario de red
Dirección IP Ia1
Dirección de L2 M1
Dirección IP Ib2
Dirección de L2 M2
Dirección IP Ic1
Dirección de L2 M3
Dirección IP Ic2
Dirección de L2 M4
Conmutador de servicio IP
Nodos de agregación
Dirección de L2 M7
Dirección de L2 M8
Proveedor de servicio de red 1
Proveedor de servicio de red 2
Grupo 1 de direcciones IP (servidor 1 DHCP)
Grupo 2 de direcciones IP (servidor 2 DHCP)
puerto a
puerto b
puerto c
NT
CPN a
CPN b
CPN c
IEa1
IEa2
IEb1
IEb2
IEc1
IEc2
Conmutador de servicio IP termina capa 2.
Conmutación de sesión IP basada en política, sin encaminamiento.
Decisión de política inicial en configuración de sesión IP.

Figura 1

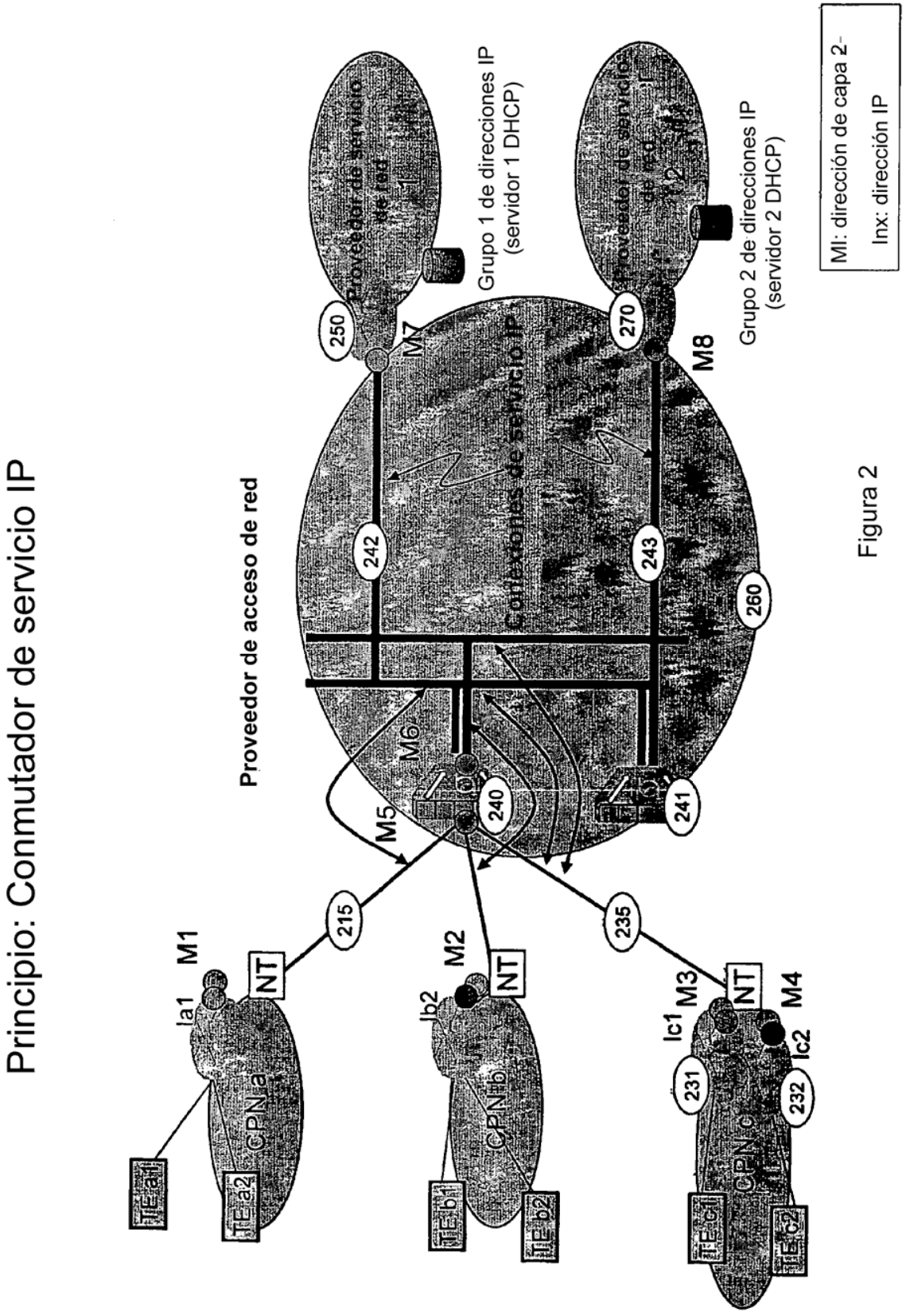

Principio: Conmutador de servicio IP
Proveedor de acceso de red
Conexiones de servicio IP
Proveedor de servicio de red 1
Proveedor de servicio de red 2
Grupo 1 de direcciones IP (servidor 1 DHCP)
Grupo 2 de direcciones IP (servidor 2 DHCP)
M1
M2
M3
M4
M5
M6
M7
M8
NT
CPN a
CPN b
CPN c
TE a1
TE a2
TE b1
TE b2
TE c1
TE c2
la1
lb2
lc1
lc2
215
235
240
241
242
243
250
260
270
231
232
MI: dirección de capa 2
Inx: dirección IP

Figura 2

Principio: Conmutador de servicio IP

Sesión					
Puerto físico	**C-VLAN**	IP(usuario)	Dirección de capa 2 (usuario)	**S-VLAN**	**MAC (NSP)**
a	**-**	**Ia1**	**M1**	**2011**	**M7**
b	**-**	**Ib2**	**M2**	**2022**	**M8**
c	**1001**	**Ic1**	**M3**	**2011**	**M7**
c	**1002**	**Ic2**	**M4**	**2022**	**M8**

Figura 3

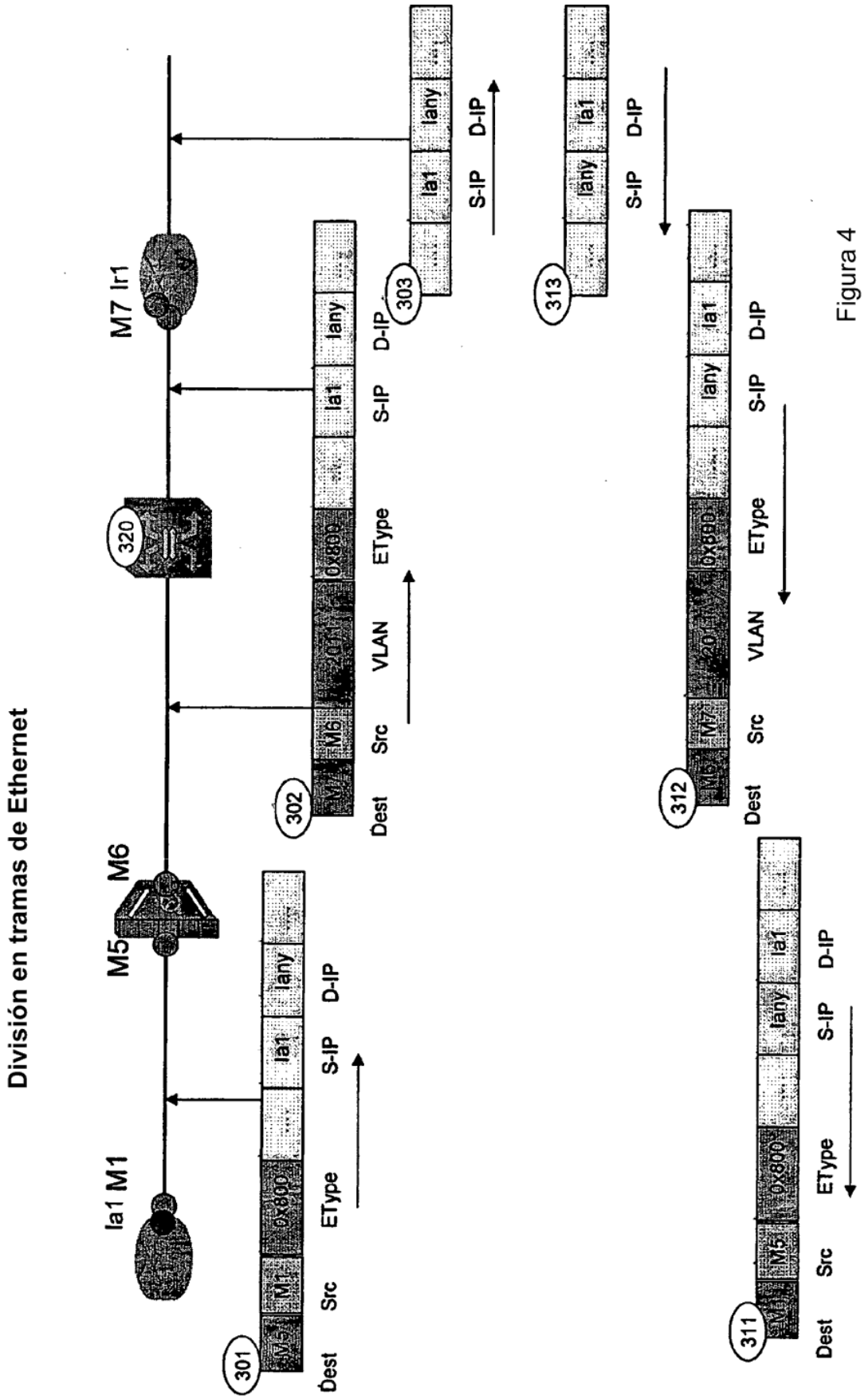

División en tramas de Ethernet
Ia1 M1
M5
M6
M7 Ir1
320
301
302
303
311
312
313
Dest
Src
VLAN
EType
S-IP
D-IP
0x800
Ia1
Iany

Figura 4

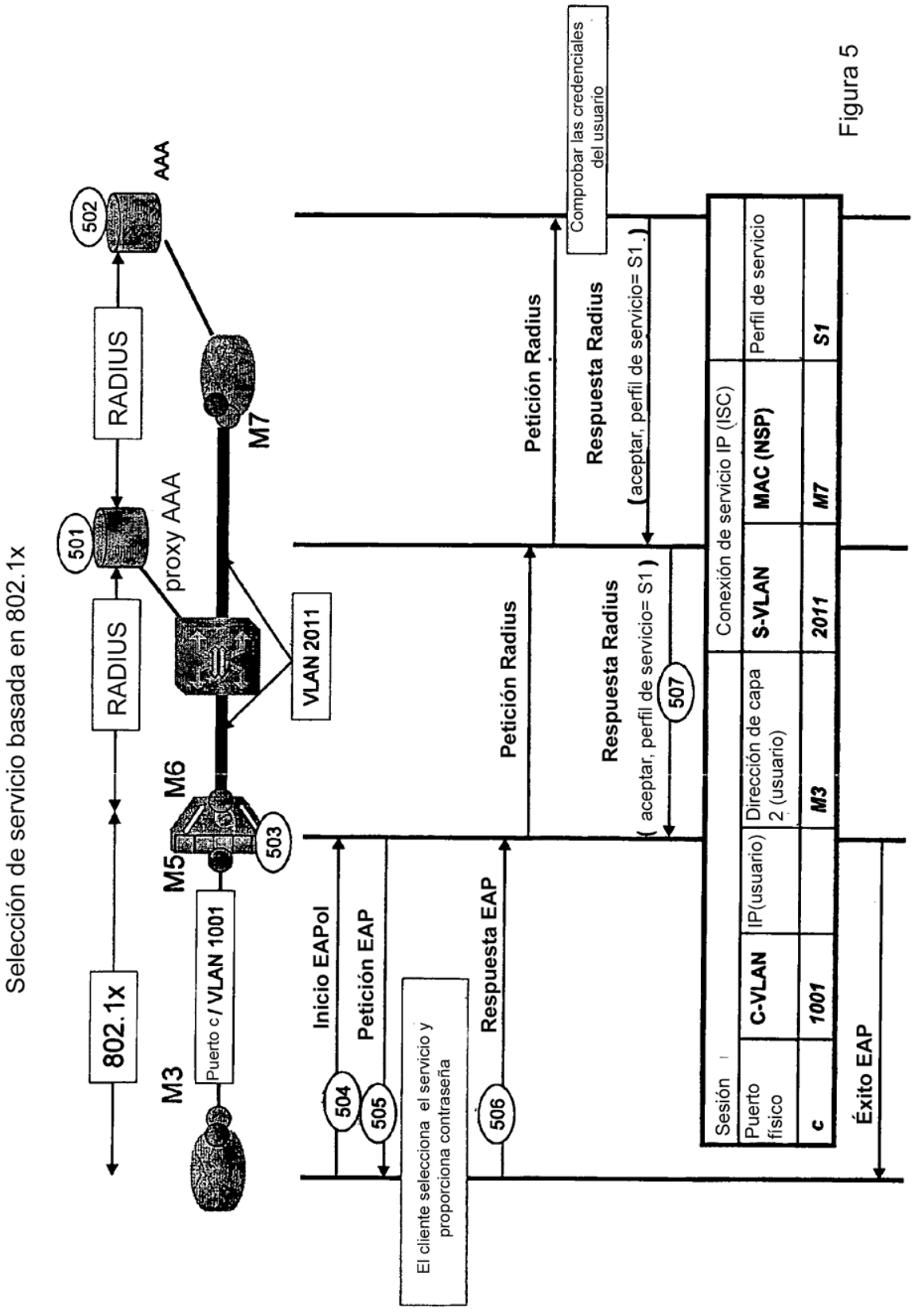
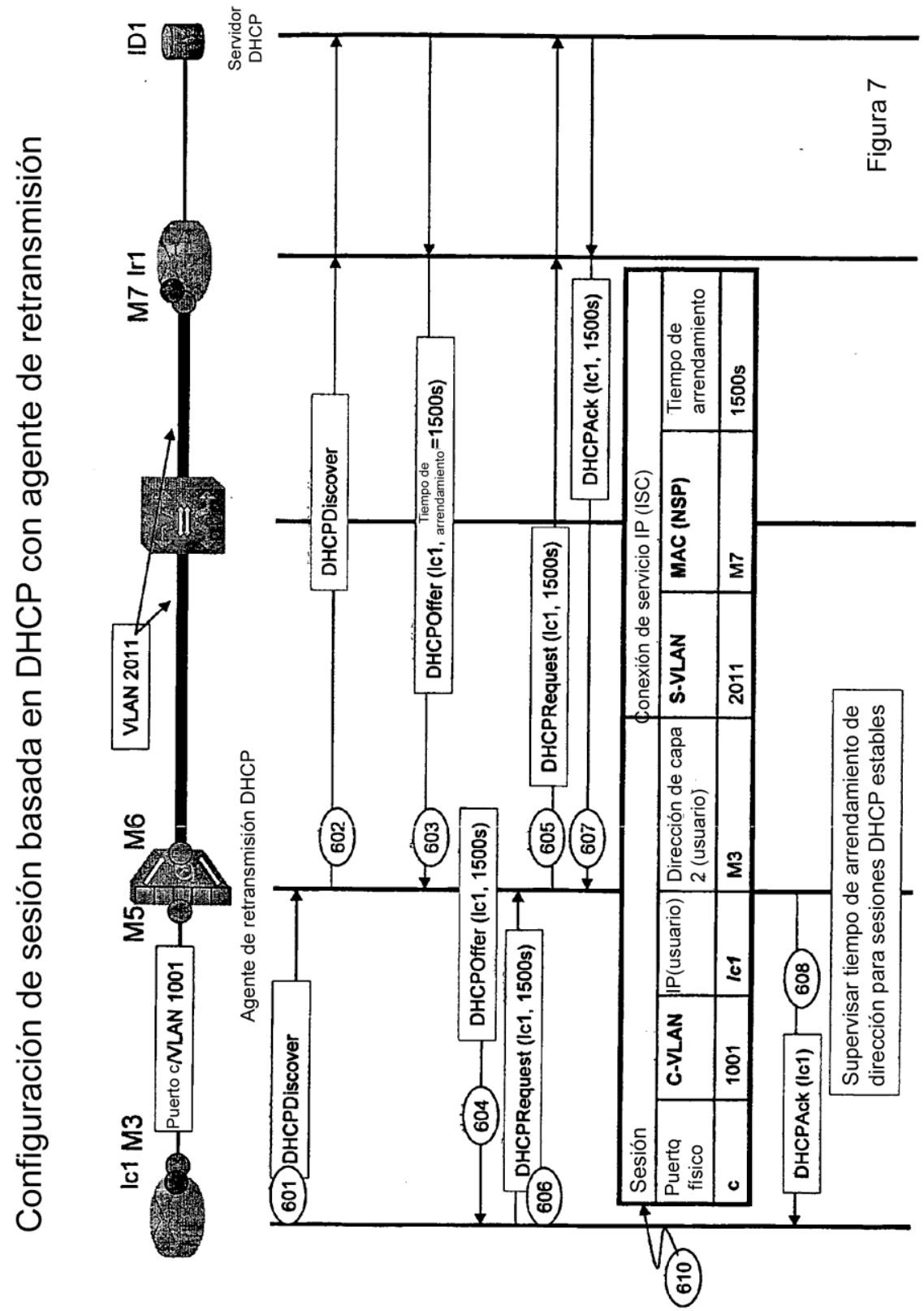

Selección de servicio basada en 802.1x
AAA
502
RADIUS
501
RADIUS
proxy AAA
M7
VLAN 2011
M6
M5
503
802.1x
M3
Puerto c / VLAN 1001
Petición Radius
Comprobar las credenciales del usuario
Respuesta Radius
(aceptar, perfil de servicio= S1)
Petición Radius
Respuesta Radius
(aceptar, perfil de servicio= S1)
507
Conexión de servicio IP (ISC)
Inicio EAPol
Petición EAP
Respuesta EAP
504
505
506
El cliente selecciona el servicio y proporciona contraseña
Sesión
Puerto físico
C-VLAN
IP(usuario)
Dirección de capa 2 (usuario)
S-VLAN
MAC (NSP)
Perfil de servicio
c
1001
M3
2011
M7
S1
Éxito EAP

Figura 5

Ejecución de políticas basda en perfil de servicio

Perfil de servicio	Ancho de banda (ascendente)	Ancho de banda (descendente)	Clase de servicio
S1	**0,5 Mbps**	**1,0 Mbps**	mejor esfuerzo
	0,2 Mbps	**0,2 Mbps**	tiempo real
S2	**0,5 Mbps**	**2,0 Mbps**	mejor esfuerzo

Figura 6


Configuración de sesión basada en DHCP con agente de retransmisión
Ic1 M3
Puerto c/VLAN 1001
M5
M6
VLAN 2011
M7 Ir1
ID1
Servidor DHCP
Agente de retransmisión DHCP
601 DHCPDiscover
602 DHCPDiscover
603 DHCPOffer (Ic1, Tiempo de arrendamiento =1500s)
604 DHCPOffer (Ic1, 1500s)
605 DHCPRequest (Ic1, 1500s)
606 DHCPRequest (Ic1, 1500s)
607 DHCPAck (Ic1, 1500s)
608 DHCPAck (Ic1)
610
Conexión de servicio IP (ISC)
Sesión
Puerto físico
C-VLAN
IP(usuario)
Dirección de capa 2 (usuario)
S-VLAN
MAC (NSP)
Tiempo de arrendamiento
c
1001
Ic1
M3
2011
M7
1500s
Supervisar tiempo de arrendamiento de dirección para sesiones DHCP estables
Figura 7

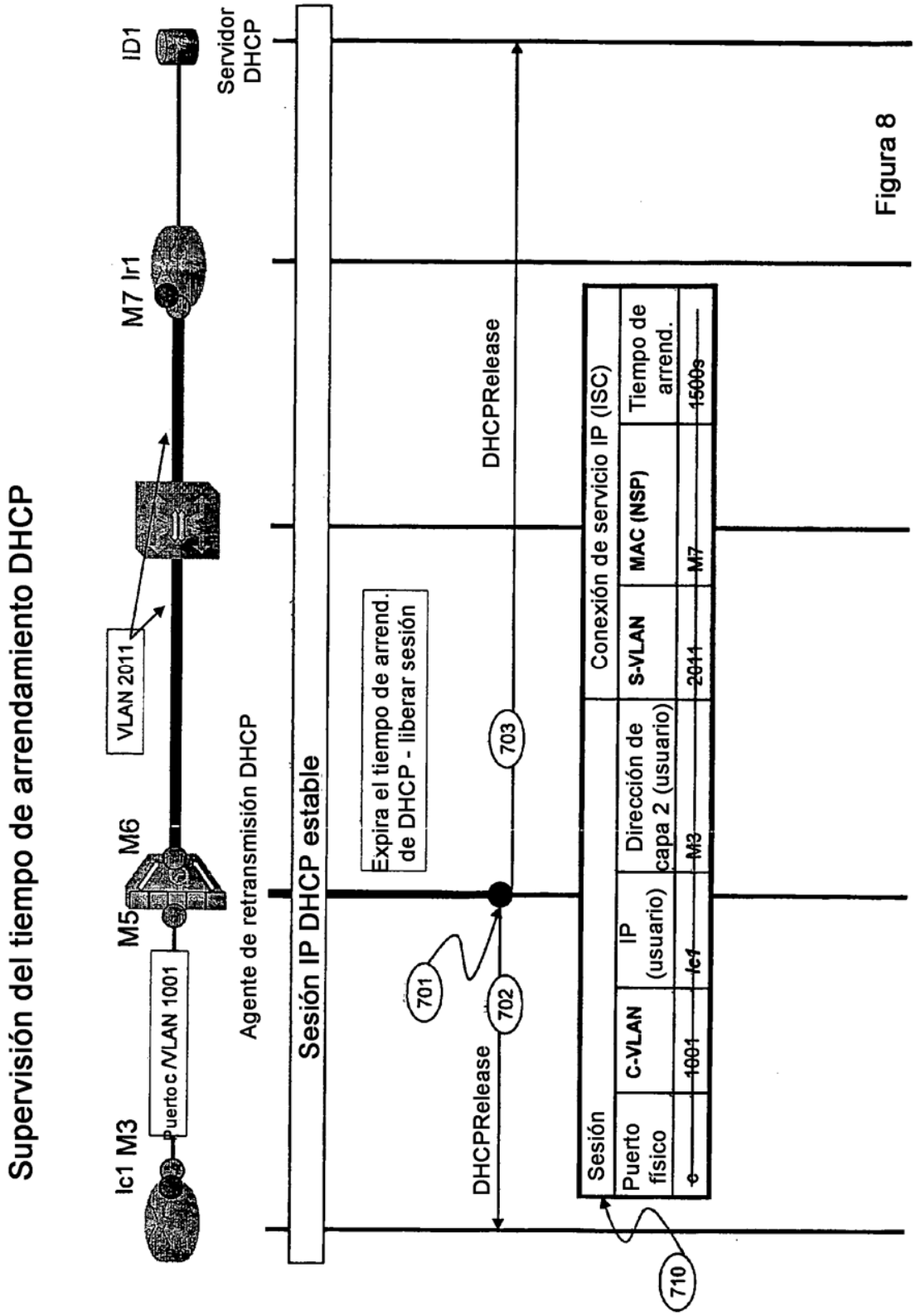

Supervisión del tiempo de arrendamiento DHCP
Ic1 M3
Puerto c /VLAN 1001
M5
M6
VLAN 2011
M7 Ir1
ID1
Servidor DHCP
Agente de retransmisión DHCP
Sesión IP DHCP estable
Expira el tiempo de arrend. de DHCP - liberar sesión
DHCPRelease
DHCPRelease
701
702
703
710
Conexión de servicio IP (ISC)
Sesión
Puerto físico
C-VLAN
IP (usuario)
Dirección de capa 2 (usuario)
S-VLAN
MAC (NSP)
Tiempo de arrend.
0
1001
Ic1
M3
2011
M7
1500s

Figura 8

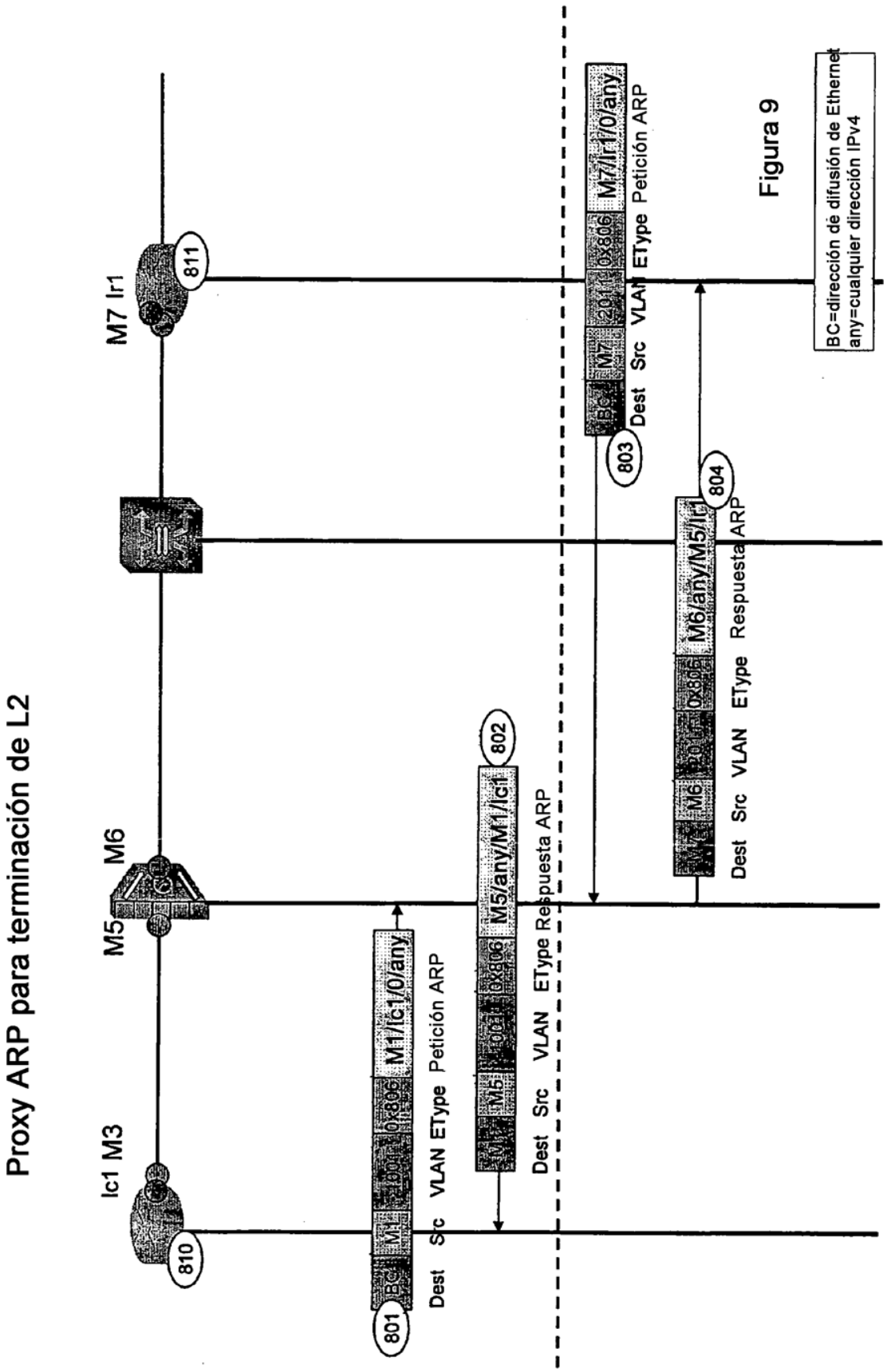

Proxy ARP para terminación de L2
Ic1 M3
M5
M6
M7 Ir1
810
811
801
802
803
804
Dest Src VLAN EType Petición ARP
Dest Src VLAN EType Respuesta ARP
BC=dirección de difusión de Ethernet
any=cualquier dirección IPv4

Figura 9

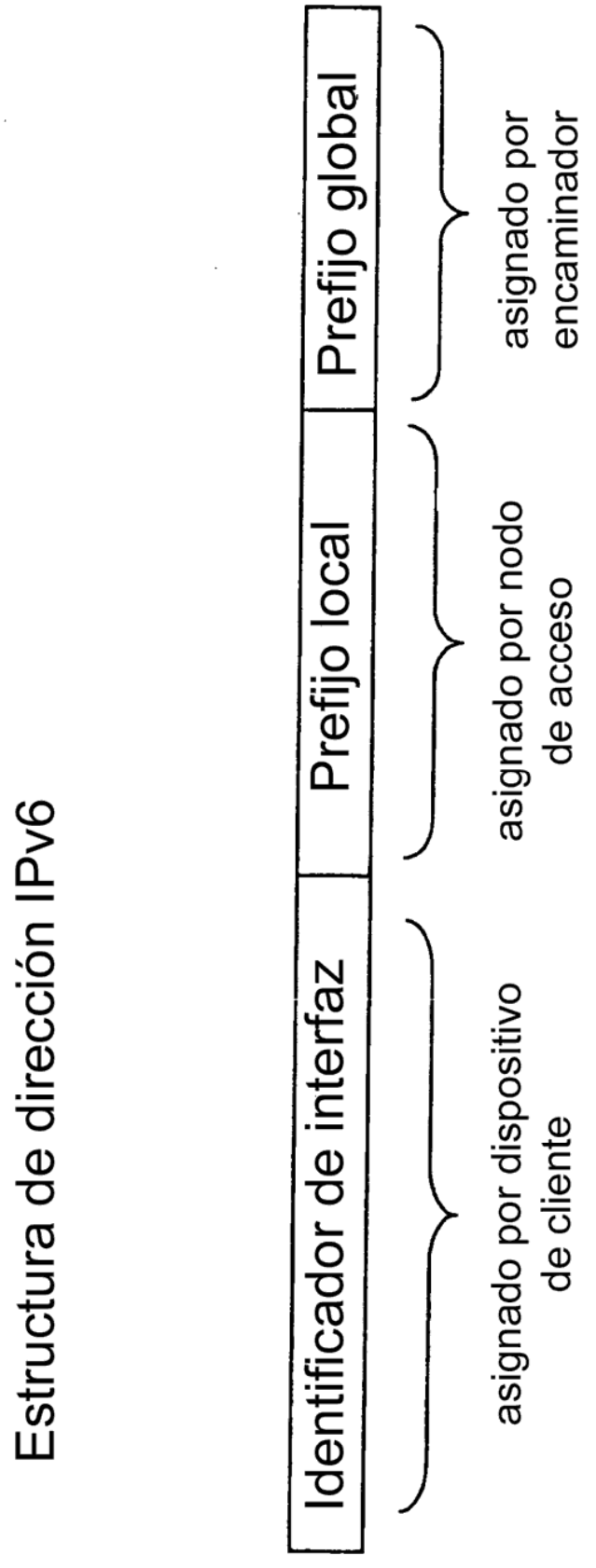

Estructura de dirección IPv6
Identificador de interfaz
Prefijo local
Prefijo global
asignado por dispositivo de cliente
asignado por nodo de acceso
asignado por encaminador

Figura 10