(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 281 945**

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Número de solicitud europea: **99113243 .2**
(86) Fecha de presentación : **06.07.1999**
(87) Número de publicación de la solicitud: **0991232**
(87) Fecha de publicación de la solicitud: **05.04.2000**

(54) Título: **Procedimiento y dispositivo para la determinación de la ruta en una red de comunicaciones.**

(30) Prioridad: **01.10.1998 DE 198 45 331**

(45) Fecha de publicación de la mención BOPI:
01.10.2007

(45) Fecha de la publicación del folleto de la patente:
01.10.2007

(73) Titular/es: **Siemens Aktiengesellschaft**
Wittelsbacherplatz 2
80333 Munich, DE

(72) Inventor/es: **Ruban, Thomas;**
Puhl, Alfons;
Grimminger, Jochen y
Bokaemper, Martin

(74) Agente: **Carvajal y Urquijo, Isabel**

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín europeo de patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre concesión de Patentes Europeas).

Venta de fascículos: Oficina Española de Patentes y Marcas. Pº de la Castellana, 75 – 28071 Madrid

DESCRIPCIÓN

Procedimiento y dispositivo para la determinación de la ruta en una red de comunicaciones.

La invención se refiere a un procedimiento para la determinación de la ruta, llamada también "Routing", en redes de comunicaciones y redes de datos IP orientadas a paquetes.

Un proveedor de un servicio de información pone informaciones a la disposición de los usuarios en una red orientada a paquetes. Estas informaciones pueden ser procesadas y seleccionadas, por ejemplo, en forma de contenidos de bases de datos o de páginas Web. Para poder utilizar un servicio de información, un usuario debe utilizar, en general, un servicio de conmutación. Este servicio conmuta paquetes de datos en la red de paquetes y de esta manera establece el acceso al servicio de información.

Hasta ahora, un usuario puede seleccionar entre diferentes servicios de conmutación. En un instante puede reclamar solamente un servicio de conmutación, todos los paquetes de datos son enviados a este servicio de conmutación, que los distribuye entonces posteriormente. En el caso de una modificación de la comunicación en una red de datos orientada a paquetes, por ejemplo con un proveedor de información (como Compuserve o AOL) o con una red privada de empresa, debe establecerse una nueva comunicación de datos.

Si un usuario no se encuentra en la red, a la que desea obtener acceso, entonces debe establecer en primer lugar una comunicación con un servicio de conmutación. Esto se lleva a cabo, por ejemplo, desde su PC por medio de un módem a través de la red telefónica de línea conmutada y con un protocolo especial, como SLIP o PPP. Si el usuario quiere cambiar el servicio de conmutación, entonces debe terminar la comunicación establecida y establecer una nueva comunicación con un servicio de conmutación siguiente.

De esta manera, se pierden todos los parámetros ajustados durante la primera comunicación.

Un caso especial del servicio de acceso se llama PoP (Punto de Presencia) Virtual. En este caso, se permite desde un servicio de conmutación a otros servicios de conmutación la utilización del mismo punto de acceso. Los usuarios de este segundo servicio de conmutación no se dan cuenta de que se encuentran en un punto de acceso "extraño".

El documento US 5.610.910 describe un procedimiento para el control de un acceso a servicios de la red utilizando un módulo de control de acceso. El procedimiento comprende la extracción de un contenido de información sobre paquetes de datos en el módulo de acceso como un nodo de la red. Además, se determinan una o varias redes adecuadas de acuerdo con el contenido de información extraído y se conducen los paquetes de datos de una manera correspondiente hacia una o varias redes adecuadas. El módulo de acceso comprende una base de datos local o puede tener acceso a una base de datos distante, estando memorizadas informaciones en la base de datos correspondiente, que se refieren a un perfil de usuario.

El documento WO 98/41043 describe un módulo de acceso y procedimientos de acceso para una red telefónica, en la que se posibilita a aparatos locales un acceso a redes telefónicas públicas.

El cometido de la invención es indicar una posibilidad para que un usuario pueda seleccionar, con una comunicación existente con una red de datos orientada a paquetes, entre diferentes proveedores de servicios de conmutación y de información, sin tener que adaptar esta comunicación en cada caso a ello.

Este cometido se soluciona a través de un procedimiento de acuerdo con la reivindicación 1.

En el procedimiento de acuerdo con la invención de la determinación de la ruta de tráfico (designada a continuación también como Routing) se analizan todos los paquetes de datos en la red a través de un nodo seleccionado de la red y se manipula la trayectoria de los paquetes hacia la dirección de destino de acuerdo con las previsiones. En este caso, se utilizan en primer lugar informaciones, que están contenidas en el paquete de datos (a través del usuario, que puede ser también un programa). Además, se utilizan segundas informaciones para la ruta, que están a la disposición del nodo de la red, o bien en una base de datos propia o también en varias tablas, que pueden estar presentes distribuidas en la red, que pueden ser llamadas por él. Se determina un nodo de transferencia (por ejemplo, servicio de conmutación) adecuado para las demandas.

De esta manera, el usuario puede seleccionar diferentes servicios de conmutación y de información, sin que deba liberarse la comunicación visible para él en ningún instante. Se asegura que se seleccione una ruta adecuada, por ejemplo cuando a través del usuario se requiere una seguridad elevada o cuando el destino en una red privada de empresa (Red Corporativa) debe ser accedido a través de una ruta exclusivamente a través de esta red privada de empresa.

La decisión sobre la ruta del paquete de datos se puede tomar, por ejemplo, de acuerdo con los siguientes procedimientos:

1. se determina desde el paquete de datos la dirección fuente (o también la dirección del remitente del usuario, 1ª información).

2. se asocia la dirección fuente a un usuario,

3. se determinan los proveedores, accesibles para el usuario, de servicios de conmutación o de servicios de información (2ª información),

4. entre los servicios de conmutación accesibles para el usuario se seleccionan aquéllos que ofrecen un transporte del paquete de datos hacia la dirección de destino deseada,

5. se determinan otros parámetros marginales (por ejemplo, límites de costes, calidad mínima), a partir de datos adicionales en el paquete de datos o a partir de informaciones adicionales asociadas al usuario, que pueden limitar adicionalmente la selección del servicio de conmutación o de información,

6. entre los servicios de conmutación seleccionados se selecciona aquel cuyos parámetros marginales coinciden mejor con los del usuario,

7. se asocian al servicio de conmutación seleccionado finalmente, por lo tanto, direcciones de destino accesibles a partir del perfil del usuario en la base de datos, por ejemplo a través de la fijación de reglas.

La transmisión del paquete se puede llevar a cabo entonces o bien de acuerdo con el principio ya conocido hasta ahora, por ejemplo con la ayuda de DNS en Internet.

A continuación se explican otras posibilidades.

El cometido se soluciona a través de un dispositivo de acuerdo con la reivindicación 19.

El dispositivo contiene:

- medios (routing engine) para la recepción, procesamiento y transmisión de paquetes de datos (IP),
- medios para la memorización de informaciones sobre el usuario y los servicios (usuario actual e información del servicio) y
- medios para el procesamiento de las primeras informaciones determinadas a partir del paquete de datos, y segundas informaciones adicionales disponibles sobre las posibilidades de rutas subyacentes (HW y SW) a partir del Routing Engine, y terceras informaciones memorizadas sobre usuarios y servicios (módulos de información de ruta) que intercambian informaciones como interfaz con Routing Engine y llevan a cabo conversiones de las informaciones transmitidas, si es necesario,

en el que estas informaciones pueden contener datos sobre facturaciones, por ejemplo después de la terminación de la comunicación o después de la finalización de un servicio así como informaciones de selección de rutas, como reglas, dirección de destino, siguiente nodo de la red y tipo de la comunicación seleccionada (por ejemplo, PVC, canalización...), y

- medios para la determinación de la reproducción de nombres lógicos de ordenador en direcciones de la red (DNS Proxy Server),
- medios para la administración del sistema (módulos de gestión del servicio),
- otros medios externos para la memorización de informaciones sobre usuarios (servidor de gestión del servicio), que pueden intercambiar datos con los medios de memoria internos a través de protocolos de comunicación, que son adecuados para la transmisión de datos de administración (como por ejemplo RADIUS).

Otras configuraciones y desarrollos se indican en las reivindicaciones dependientes.

Los paquetes de datos son enviados desde el elemento de la red hacia un punto de transferencia, que está establecido, Esto se lleva a cabo habitualmente por vías discrecionales, por ejemplo con un llamado túnel para paquetes de datos a través de la red (como con la ayuda del protocolo GRE, Encapsulación genérica de la ruta), PPTP, protocolo de canalización punto a punto o L2TP, protocolo de canalización de capa 2).

En una forma de configuración, se establece de la misma manera desde el nodo de la red la ruta hacia el nodo fijado. Esto es ventajoso, puesto que de esta manera se pueden activar criterios de control ya determinados, por ejemplo criterios de seguridad, para impedir que sean conducidos los paquetes de datos a través de redes "extrañas". Una trayectoria de datos de este tipo puede ser, por ejemplo, una comunicación directa (PVC, SVC). La trayectoria del paquete de datos se puede realizar también a través de una entrada explícita de la ruta en cada paquete (canales lógicos en ATM). En el caso de TCP/IP existe a tal fin el llamado "Source Routing" o también RSVPO (Resource ReSerVation Protocol, RFC 2205).

Las informaciones adicionales contenidas en el paquete de datos y analizadas por el nodo de la red pueden ser de diferente tipo. Además de datos concretos sobre los nodos de transferencia y los nodos de destino deseados, pueden pertenecer a ellos también datos concretos de la trayectoria. Además, son convenientes informaciones sobre fuente y destino del paquete de datos y características de la transmisión de los datos deseadas por el usuario, como costes, calidad, seguridad, velocidad. Estas informaciones se pueden determinar de una manera explícita a partir del contenido (cabecera) del paquete de datos o también de una manera implícita. Estos datos se pueden utilizar para el procesamiento posterior de una manera individual o también en combinación.

Las informaciones de dirección sobre fuente y destino de un paquete de datos pueden estar constituidas por varios componentes (componentes e la dirección). Entre ellos se encuentran, por ejemplo direcciones TCP/IP, que se pueden ampliar y refinar a través de una indicación exacta de un término lógico de la comunicación (el llamado número de puerto). En otros tipos de direcciones, a través de una ampliación de la dirección se puede activar también, por medio de números de puertos, un punto de conexión con una instalación de hardware.

Existen diferentes motivos para que no se pueda transmitir un paquete de datos desde el nodo de la red.

Por una parte, posiblemente los paquetes están mal direccionados. La dirección indicada podría no ser resulta de forma correcta, por ejemplo por el DNS Proxy, de manera que no se puede determinar ninguna dirección de destino y, por lo tanto, ningún nodo siguiente de la red, al que debe transferirse el paquete de datos.

Por otra parte, la dirección de destino es correcta, pero no se ha podido determinar ningún servicio de conmutación desde el nodo central de la red, que pueda transmitir el paquete de datos a la dirección de destino deseada. Otra posibilidad de error consiste en el hecho de que el usuario debe anunciarse en primer lugar en un servicio de conmutación o de información. Cuando el usuario selecciona un servicio, para el que no ha registrado ninguna autorización de utilización, no se pueden transmitir tampoco paquetes de datos.

Los paquetes de datos, que no se pueden transmitir, son borrados ("desechados"), en general, en una red de datos orientada a paquetes. En una forma de configuración de la invención, todos estos paquetes de datos que no pueden ser suministrados, son transmitidos a un nodo de la red adecuado ("por defecto") o son transferidos a un proceso lógico, que genera entonces una reacción. Esta reacción puede consistir, por ejemplo, en un mensaje de error, que se envía de retorno al emisor, y que contiene una indicación del motivo por el que no se ha realizado con éxito la emisión de los paquetes de datos (confirmación negativa). Otra solución sencilla sería la generación de respuestas ICMP (Protocolo de Mensaje de Control de Internet) ("ordenador central no accesible"). Además, esta reacción puede contener una ayuda acerca de cómo se podría evitar la aparición de errores en la transmisión de datos (por ejemplo; es necesaria una solicitud en el caso de un servicio de conmutación, errores en la dirección, ...). Estas instrucciones pueden ser tan detalladas en determinadas circunstancias que se ofrece al menos una acción concreta y se ofrece la posibilidad de que el usuario se decida por una de estas acciones, puede rechazarlas o también puede iniciar una reacción alternativa. Además, en el caso de una solicitud confusa (varios servicios de conmutación posibles son "igualmente buenos") se puede conseguir a través de otras consultar a través del nodo de la red una selección del servicio de conmutación o de información.

Los paquetes de datos, que son enviados como paquetes de respuesta desde la dirección de destino de retorno a la dirección fuente, deben recorrer los mismos nodos establecidos (es decir, el mismo servicio de conmutación) que los paquetes originales. Por lo tanto, en el recorrido de ida y vuelta es necesario que desde el nodo de la red sean manipuladas las entradas de las direcciones fuente y las direcciones de destino. Para poder asociar paquetes de datos entrantes de una manera unívoca como paquetes de respuesta, se memorizan en este caso registros sobre las comunicaciones virtuales, con el fin de poder modificar de nuevo las direcciones posiblemente manipuladas. Esto corresponde a los métodos conocidos para paquetes de datos IP de la Traducción de Direcciones de la Red (RFC 1631). Por ello se entiende por ejemplo mascarada, DNAT (Traducción de Direcciones de Redes Distribuidas), NAR (Reutilización de Direcciones Negociadas) o RAT (ver a este respecto también los Internet Drafts, por ejemplo en http://www.ietf.org/).

De esta manera, el usuario (es decir, el emisor de los paquetes originales y el receptor de los paquetes de respuesta) puede asegurar que también estos paquetes de datos cumplan los criterios deseados por él. Esto es aplicable a los costes de la transmisión y a la calidad de la transmisión de la misma manera que a la garantía de una seguridad de la transmisión.

En el caso de que la trayectoria para la ruta de retorno con la dirección fuente del paquete de datos original no sea conocida en la red, en cambio el servicio de conmutación propiamente dicho puede ser accedido desde "ambos lados" (emisor y receptor, usuario y servicio de información), se puede inducir a éste para que aprenda la ruta a través de protocolos estándar de una manera selectiva desde el nodo de la red central.

De esta manera, se define cada parte de la ruta de la transmisión para el paquete de datos, desde el usuario hacia el servicio de conmutación, desde el servicio de conmutación hacia el servicio de información y de nuevo de retorno. En el caso de que la ruta hacia el servicio de conmutación desde el nodo de la red central deba dedicarse para los mensajes, o bien es posible NAT sobre distintas direcciones fuente, para que el servicio de conmutación pueda acceder al nodo de la red central también sobre vías diferentes. Además, el nodo de la red central se puede comunicar también directamente con el nodo que sirve de base y de esta manera puede intercambiar informaciones de rutas.

En otra forma de realización de la invención se permite al usuario cambiar entre diferentes proveedores de servicios durante una comunicación con una segunda red de datos con las diferentes fuentes de datos accesibles. En este caso, se determina de una manera individual el recorrido para cada paquete de datos. El usuario puede seleccionar entre servicios de conmutación individuales, pero en cada caso solamente es activo un servicio de conmutación para determinadas redes o servicios de información. Esto es importante, por ejemplo, para la facturación. Los servicios de conmutación para redes corporativas / proveedores de servicios (redes generales) se pueden utilizar en paralelo.

Para la elevación de la seguridad es posible también codificar los paquetes de datos antes de la emisión con los mecanismos de codificación usuales a través del usuario o desde el elemento de la red (SG)Esto es ventajoso sobre todo cuando deben enviarse paquetes de datos sensibles a la seguridad y las trayectorias de datos que están disponibles conducen a través de redes extrañas.

Un usuario puede anunciarse en la red en diferentes servicios (servicios de conmutación o de información) y entonces tiene allí una autorización de utilización. Además, en función del tipo de servicio, se pueden indicar propiedades de transporte adicionales para mensajes con atributos para los usuarios individuales (dirección fuente).

En este caso, se pueden definir, por ejemplo, las diferentes disponibilidades para un servicio, de la siguiente manera:

- "oculto"

  el usuario no tiene la posibilidad de reclamar un servicio.

- "abonable"

  el usuario puede utilizar este servicio, pero debe registrarse con anterioridad

- "abonado"

  el usuario se ha registrado ya en un servicio y puede activarlo en adelante

- "activado"

  el usuario tiene abierto en este instante un acceso al servicio

Cada usuario tiene un estado básico determinado con relación a los servicios de conmutación y de información. Este estado básico se puede designar también como perfil del usuario. El perfil se puede modificar por el usuario durante una sesión. Este perfil del usuario puede estar memorizado en el elemento de la red central, pero también es posible tomar, en caso necesario, estos perfiles del usuario a partir de una (o varias) bases de datos externas distribuidas.

En virtud de estos perfiles de usuario, el elemento de la red central puede calcular con rapidez qué usuario posee una autorización para qué servicio de conmutación. En el caso de que el usuario no pueda utilizar un servicio de conmutación, el elemento de la red central puede transmitir un paquete de datos correspondiente de forma inmediata a un nodo de la red adecuado para el tratamiento de errores.

El acceso a través del perfil del usuario puede estar protegido con una palabra de paso (Login).

Se puede tratar el caso de que un usuario no pueda utilizar un servicio de conmutación, porque no se ha registrado allí todavía.

En ambos casos es conveniente asignar una autorización adecuada al emisor de los paquetes de datos. Esta autorización debe contener una referencia al motivo por el que ha fracasado una transmisión correcta del paquete de datos. Para la realización de la ejecución de estos mensajes de error se pueden transmitir los paquetes de datos correspondientes (al menos uno de ellos) también a un elemento adecuado de la red, que asume el procesamiento posterior.

El tratamiento de errores puede estar configurado de una manera muy cómoda para el usuario, por ejemplo con superficies gráficas y con un control de usuario, que proporciona mensajes de retorno también sobre la eliminación posible de los errores constatados. A través de un llamado panel de ayuda se puede ofrecer al usuario también, después de la emisión de paquetes de datos, una posibilidad de ayuda, que le indica las opciones y acciones posibles para él.

Puesto que todos los paquetes de datos pasan a través del "routing engine", que es controlado por este nodo especial de la red, se puede realizar fácilmente una colección de datos para fines de registro de las tasas. En este caso, se puede facturar, por una parte, a los usuarios la utilización de los recursos ofrecidos. Por otra parte, se pueden facturar también las informaciones recolectadas por los proveedores de servicios. En este caso, los valores utilizados habitualmente para ello se refieren al volumen de los datos o a la duración de la comunicación existente para la transmisión (incluida la ocupación de recursos de la red). Además, se puede llevar a cabo también una facturación en virtud de datos sobre los servicios utilizados o el número de los paquetes de datos conmutados con éxito u otros datos.

Para conducir los paquetes de datos desde el nodo especial de la red (Routing Engine) hacia el nodo establecido (punto de transferencia o bien servicio de conmutación) debe establecerse una ruta. Esto se puede realizare de diferentes maneras:

- con la ayuda de métodos de NAT,
- "Encapsulación". Es decir, encapsulación de los paquetes de datos, por ejemplo con GRE (Encapsulación genérica de la ruta RFC 1701), utilizada también en "Tunneling", como con los protocolos PPTP (protocolo de canalización punto a punto, Microsoft) o L2TP (protocolo de canalización de capa 2), una ampliación del protocolo PPP),
- con PVC o SVC.

Adicionalmente a las informaciones memorizadas internamente sobre autenticación, acceso, perfil del usuario o facturación en una base de datos (por ejemplo, UMS, sistema de gestión del usuario), pueden existir también bases de datos externas, que ponen a disposición informaciones de este tipo en toda la red. Puesto que se puede tratar de datos sensibles para la seguridad, se plantean requerimientos elevados con relación a la seguridad de los datos en el protocolo de acceso desde el nodo de la red central a esta base de datos externa. Un protocolo de acceso adecuado para ello es RADIUS (Servicio de marcación de usuario de autenticación remota, RFC 2138) o LDAP (Lightweight Directory Access Protocol, RFC 1777).

En otra forma de realización, el usuario propiamente dicho puede modificar las informaciones contenidas en la base de datos, por ejemplo su perfil de usuario. A tal fin, debe prepararse una interfaz, a través de la cual puede acceder a los datos con la superficie adecuada. A tal fin, se conocen muchas soluciones. Una posibilidad es el protocolo http (protocolo de transferencia de hipertexto) utilizado ya muchas veces con los navegadores habituales de la red (Netscape. Mosaic, Microsoft Explorer,...) como interfaz de usuario. También son concebibles versiones modificadas de este protocolo o de otros protocolos adecuados (por ejemplo, utilizar IP V6, también para Voice over IP), también en otros terminales del usuario, como teléfonos móviles (con o sin organizadores electrónicos, como por ejemplo el Comunicador NOKIA) o Palmpilots, que tienen una capacidad de memoria reducida y una interfaz de mando pequeña.

A través de esta interfaz se puede acceder también a una máquina de ayuda para el usuario. Ésta puede simplificar una transmisión correcta de los paquetes de datos con la ayuda de informaciones accesibles y otras consultas desde y hacia el usuario. La posibilidad de ayuda se puede realizar en diferentes formas de realización.

La ventaja esencial de la invención consiste en que por medio de la estructura modular es posible una utilización de muchos componentes estándar (parcialmente en forma modificada). Esto simplifica y acelera la realización.

A continuación se explica la invención con la ayuda de ejemplos de realización. En este caso:

La figura 1 muestra una estructura esquemática posible del dispositivo para la determinación de la ruta de tráfico de un paquete de datos.

La figura 2 muestra una representación esquemática de las trayectorias de datos posibles entre dos redes de comunicación separadas con servicios de conmutación y servicios de información.

La figura 3 muestra una representación esquemática de una red de comunicaciones con la sesión de un usuario.

La figura 4 muestra una estructuras detallada de una red ejemplar con componentes individuales de la red, y

Las figuras 5a y 5b muestran un diagrama de flujo, que describe la colaboración de los componentes individuales del dispositivo con la ayuda de un escenario sencillo.

La figura 1 muestra la estructura esquemática posible de un dispositivo (SG) para la determinación de las rutas de tráfico de un paquete de datos (IP). La estructura no muestra la configuración mínima, solamente están previstos diferentes componentes para la elevación de la facilidad de utilización por el usuario, sin embargo no son necesarios en sí para el modo de funcionamiento del dispositivo.

Totalmente a la izquierda (S) se encuentra un usuario o una aplicación, que genera o recibe paquetes de datos y los quiere transmitir a la red. A tal fin, transfiere estos paquetes de datos (IP) a un "Routing engine" (RE), que tiene el cometido de recibir estos paquetes de datos, procesarlos y transmitirlos posteriormente de una manera adecuada. El "Routing Engine" puede estar contenido en el dispositivo de diferente manera, por ejemplo en el Kernel de un sistema operativo (como INUX) o también como rúter "externo" separado.

Este Routing Engine (RE) intercambia datos, con un medio (módulo de información de ruta) para el procesamiento de primeras informaciones, que calcula a partir de los paquetes de datos recibidos, segundas informaciones sobre usuarios y servicios, que pueden ser seleccionadas a partir de bases de datos y terceras informaciones, que contienen datos sobre hardware y software de las redes y rúteres utilizados que sirven de base. Por ejemplo se intercambian reglas,

que han sido determinadas a partir de un perfil del usuario y que reglamentan el acceso a determinados servicios de conmutación o de información. También pueden ser informaciones más detalladas para el uso de protocolos para la emisión posterior de los paquetes de datos, como métodos de NAT (RFC 1632). También se puede tratar de datos de facturación.

La fuente más importante para la segunda información es el medio de memoria (usuario actual e información de servicio, UMS). Aquí se encuentran los perfiles de usuarios (actuales), que contienen, por ejemplo, las reglas y lo que se necesita todavía como información sobre los usuarios y los servicios.

Esta base de datos de información se puede completar todavía a través de una o varias fuentes de memorias externas (SMS, Sistema de gestión de sistemas), que suministra las informaciones de autentificación necesarias (perfil de autorización). Aquí se puede llevar a cabo una comunicación por medio de RADIUS (radius). RADIUS es un protocolo para la transmisión de información de autentificación, de autorización y de configuración entre un servicio de conmutación, que quiere autentificar sus comunicaciones, y un servidor de autentificación (distribuido).

Los datos, que están memorizados en (UMS), se pueden modificar en otra forma de realización también por los usuarios. Esto se lleva a cabo a través de una interfaz (IF), que es generada, por ejemplo, por un HTML "procesador de plantilla", realizado como JAVA Script ("Servlet", "Applet"). En este ejemplo se utiliza para la comunicación con el usuario http y HTML, incluida una interfaz de usuario gráfica como Netscape. Esto eleva la facilidad de utilización para el usuario, pero no es absolutamente necesario para la invención. En el caso de utilización de un teléfono móvil como terminal, se pueden utilizar también las instrucciones de control correspondientes.

Para la resolución de la dirección (nombre lógico en la dirección de la red) de los paquetes de datos en una red orientada a paquetes con TCP/IP se necesita DNS. Éste puede ser, en otras redes, otro servicio correspondiente. El DNS Proxy previsto para ello distribuye en este caso consultas DNS entrantes de acuerdo con las reglas memorizadas sobre usuarios y servicios en el servidor DNS competente propiamente dicho en la red.

Otro módulo no absolutamente necesario ofrece al usuario una posibilidad de ayuda (panel de ayuda). En este caso, es conveniente utilizar la misma interfaz de usuario que para la modificación de las informaciones. La función de ayuda puede estar configurada en este caso de una manera conocida por el técnico.

Tan pronto como el paquete de datos (IP) ha sido analizado y procesado de la manera descrita, se puede transmitir a la dirección de destino. El objetivo puede ser directamente un servicio de información (CP, proveedor de contenidos) o una red privada de empresa (Corp, red corporativa). Si debe emitirse el paquete de datos a otra red de comunicaciones, entonces es necesaria una transferencia a través de un servicio de conmutación (ISP, Proveedor de servicios de Internet).

La figura 2 muestra una estructura esquemática de dos redes de datos (Na y Nb) así como un elemento de la red (SG), a través del cual se transmiten paquetes de datos de usuarios a una y/u otra red de datos y las trayectorias de datos, que adoptan los paquetes de datos hacia los servicios individuales.

Los paquetes de datos son recibidos por el elemento de la red (SG). Por medio del procedimiento ya descrito y de informaciones adicionales procedentes de una base de datos (DB) se calcula la otra trayectoria en la primera red (Na). Los paquetes de datos se pueden transmitir, por ejemplo, por encapsulación a uno de los servicios de conmutación disponibles (A - F). En este caso, se distingue entre servicios directamente en el punto de transferencia (servicios de información, C - E) y servicios a distancia del punto de transferencia (A, B, F, también llamados Proveedores de servicios de Internet, ISP).

Los servicios de conmutación posibilitan el acceso a servicios de información (G, H) en una segunda red de comunicaciones (Nb). En este caso, se puede acceder a un servicio de información a través de varios servicios de conmutación (G, A, B, F) y un servicio de conmutación puede acceder a varios servicios de información (A, G, H). Solamente se puede activar cada vez un servicio de conmutación en un instante a un servicio de información.

Un servicio de información es accesible directamente (C, D, E). En un instante, pueden estar activados más de un servicio de información.

La figura 3 muestra, a partir de la figura 2, el desarrollo de una "sesión" posible de un usuario.

Un usuario (user) accede a través de una red (por ejemplo, una comunicación en una red telefónica) al nodo de la red (SG). Éste verifica su perfil de usuario (2) con la ayuda de informaciones que proceden de los paquetes de datos (1) transmitidos y de informaciones contenidas en una base de datos (DB). En un perfil de usuario no están contenidos servicios que se puedan activar de forma inmediata, sin duda algunos, lo mismo que proveedores de información libremente disponibles para todos.

El usuario intercambia paquetes de datos (3) con uno de estos servicios libremente disponibles (CP, proveedores de contenidos), por ejemplo su base de datos. En nuestro ejemplo se puede tratar, por ejemplo, de su esto de cuenta, o de consultas de transferencias o similares. Si en el servicio libremente disponible no es necesaria una identificación

del usuario, entonces se puede elegir el usuario (registro anónimo). En el marco de este tráfico de dato, el usuario recibe algunas informaciones interesantes (por ejemplo) sobre páginas Web en Internet. Pero puesto que hasta ahora no está activado ningún servicio de conmutación, este servicio de información no era accesible hasta ahora para él (4). El elemento de la red (SG) da entonces al cliente la posibilidad de seleccionar un servicio (5) a partir de una lista de servicios de conmutación.

El usuario se decide por un servicio de conmutación lento y económico (ISPA) y a continuación es posible el intercambio de datos con el servicio de información (S) en la segunda red de comunicaciones (Nb).

Después de algún tiempo, el usuario descubre en el servicio de información (S) un documento mayor, que le gustaría transmitir. Con este fin, conmuta a un servicio de conmutación (ISPB), que es más rápido, pero, por lo tanto, más caro (7). Durante el cambio se realizan las siguientes modificaciones:

- se borra la entrada para la ruta estándar para este usuario hacia el primer servicio de conmutación (ISPA),
- se borran las reglas Firewall, que permiten a los paquetes de datos la ruta hacia el primer servicio de conmutación (ISPA),
- cuando se aplican métodos de NAT sobre la dirección fuente (IP) para el usuario hacia el primer servicio de conmutación (ISPA), de borran de la misma manera estas reglas. (NAT es necesario en una cadena de transmisiones referidas a las fuentes. La mayoría de las veces no se utiliza cuando se aplica la canalización (Tunneling)
- se registran reglas NAT nuevas para el segundo servicio de conmutación (ISPB), en caso necesario,
- se registran reglas Firewall nuevas para permitir a los paquetes de datos la ruta hacia el segundo servicio de conmutación (ISPB), y
- se registra una nueva ruta estándar para paquetes de datos desde la dirección de usuario hacia el segundo servicio de conmutación (ISPB).

Se puede comenzar con la copia del documento.

Durante la realización de la copia, el usuario quiere acceder a otro servicio de información (Corp), por ejemplo a una red interna de empresa (8), para verificar allí su correo electrónico. Esto es posible sin problemas durante la fase de copia, tan pronto como ha terminado la transmisión, el usuario puede terminar también la comunicación a través del servicio de conmutación (ISPB), mientras existe todavía la comunicación con la red privada de empresa (Corp).

Después de que se ha resuelto la comunicación desde el usuario, se borran las activaciones de los servicios de conmutación y se retiran todas las reglas desde el elemento de la red y/o el Routing Engine (es decir, las activaciones de los servicios de conmutación individuales desde su base de datos). Después de cada terminación de un servicio y después de la interrupción de todas las comunicaciones se transmiten (9) las informaciones acumuladas sobre la facturación a un centro de facturación (AAA).

La figura 4 muestra una estructura ejemplar de una red de redes, en la que el usuario (Dailin User) puede intercambiar paquetes de datos sobre rutas diferentes y servicios de conmutación con una segunda red de comunicaciones (Internet). El usuario se comunica en este ejemplo a través de la red telefónica (PSTN), con la que se conecta, por ejemplo a través de un módem con el PC.

El elemento de la red se puede utilizar también como PoP Virtual (Punto de Presencia, punto de acceso a una red). Desde la red telefónica se transmiten los paquetes de datos enviados hacia el elemento siguiente de la red (puerto de acceso de servicio y/o Routing Engine). En este caso, existen diferentes posibilidades, por ejemplo a través de servidor RAS (Servicio de acceso remoto), que existe de los más diferentes fabricantes, como 3Com, Cisco o Ascend. Desde allí (por ejemplo, a través de Ethernet u otros protocolos de transmisión) se conducen los paquetes de datos hacia el elemento de la red (SG1 o SG2), que calcula con la ayuda de las informaciones como el perfil del usuario (SSM, Módulo de selección del servicio, PRM, Módulo Proxy Radius) una ruta hacia un punto de transferencia. Esta ruta puede ir en este ejemplo sobre una red orientada a paquetes, como una red IP principal. En este caso, los paquetes de datos son transmitidos por medio de técnica PVC, SVC o también a través de canalización (Tunneling).

Si la dirección de destino es un servicio de información o también una red privada de empresa (CP, proveedor de contenidos), entonces se puede conducir el paquete de datos directamente a través de un rúter adecuado (R) hacia allí.

Si debe demandarse un servicio de conmutación (ISP), entonces se transfiere un paquete de datos a otro elemento de la red o a un rúter (SG3, SG4). El cálculo de la vía posterior es asumido por un módulo de rúter (RM) en el elemento

de la red. El intercambio de datos de autentificación, de liquidación y de autorización se lleva a cabo, por ejemplo, con los servidores de autentificación de los servicios de conmutación (ISP x Radius, autentificación y contabilidad).

A través de los servicios de conmutación (ISP, ISP II, ISP III) es posible entonces un acceso a otra red, como Internet, pudiendo transmitirse los paquetes de datos. La facturación así como la acumulación de otras informaciones, como datos estadísticos, pueden ser asumidos en este caso por servidores de Radius que pertenecen a los servicios de conmutación.

También servidores de Radius (Radius) independientes pueden colgar en la red IP principal, que asumen, por ejemplo, la autentificación y la facturación en el caso de accesos a servicios de información (CP), que no se conducen sobre servicios de conmutación (ISP).

Además, puede estar prevista una gestión de la red (TMN). Ésta puede ser realizada por las compañías operadoras de la red. En este caso, se pueden administrar y supervisar comunicaciones cuando acceden a servicios de información y de conmutación con sus perfiles de usuario específicos. Los elementos especiales de la red presentes (puertos de acceso de servicio) necesitan diferentes informaciones, que deberían configurarse en común, con el fin de evitar inconsistencias. De acuerdo con el alcance de la red y el número de los elementos especiales de la red (puertos de acceso de servicio), el gasto de configuración sería entonces muy alto.

Se necesitan otras informaciones, por ejemplo, sobre:

- direcciones de dispositivos de canalización hacia los servicios
- direcciones de los puertos de acceso hacia la red principal
- direcciones de servidores RAS
- direcciones de sistemas de gestión de la red y sistemas de gestión de sistemas, informaciones sobre el estado del usuario, el estado de las tasas y el estado del sistema,
- informaciones, que deben enviarse a través de SNMP,
- informaciones, que deben enviarse a través de protocolos de ruta,
- reglas de seguridad.

Adicionalmente, se acumulan informaciones sobre los servicios ofrecidos:

- espacio de direcciones de los servidores y redes accesibles,
- comunicaciones (enlaces) URL (localizador de recursos uniformes)con el servicio,
- instrucciones sobre el estado del servicio con respecto a un usuario,
- servidor DNS (servicio de nombre de dominio)
- se utiliza NAT,

y muchos más.

La mayoría de las informaciones son idénticas en todos los elementos especiales de la red, a excepción de las informaciones, que se refieren al entorno específico de la red. La gestión de la red puede memorizar estas informaciones de forma centralizada y las puede modificar con los mecanismos habituales. Para la supervisión del sistema y de sus componentes se pueden procesar también informaciones como el régimen de trabajo de un nodo de la red o el número de los paquetes, que son procesados por un rúter, y se pueden utilizar con SNMP (protocolo de gestión de la red sencillo) en un sistema de gestión de la red como HP OpenView. Se puede conectar adicionalmente un monitor a una entrada prevista propiamente para ello, con el fin de representar informaciones de este tipo.

Las figuras 5aa y 5b muestran un diagrama de flujo, que muestra las llamadas, que se desarrollan entre un usuario (user) y los elementos de la red.

El usuario se inscribe a través de la red telefónica (PSTN, ISDN) en un servidor de traducción de direcciones de la red (NAS). Envía su identificación de usuario (login Id) y una palabra de paso.

El servicio NAS envía una solicitud de acceso (Access Request) por medio del protocolo RADIS, hacia un servidor especial (AAA), que contiene el “login Id”, la palabra de paso y un ID del interlocutor que llama.

El servidor AAA, por su parte, consulta (query) en un sistema de gestión de usuarios (UMS), que ha memorizado informaciones de usuario, con el fin de verificar la identidad del usuario. En el caso de que la consulta se realice con éxito, recibe un perfil de usuario (perfil de autorización). En otro caso, el servidor AAA es informado sobre el error.

Si la autentificación es realizada con éxito, entonces el servidor AAA es anunciado en el servidor NAS (acceso aceptado) junto con el perfil de autorización calculado a partir de la base de datos y también el perfil de autentificación, que puede contener también las direcciones de la red (dirección IP), que aquél recibe asignadas (usuario transparente). Si la autentificación no se realiza con éxito, esto es anunciado de la misma manera (acceso rechazado).

Después de la autentificación con éxito, el servidor NAS comunica algunas otras informaciones por medio de (Solicitud Acct Start) al servidor AAA, como dirección, ID del interlocutor que llama, ID de la sesión, que señaliza el comienzo de los registros de informaciones, que se utilizan también para la facturación.

El servidor AAA informa al mismo tiempo con estas informaciones que identifican al usuario al elemento especial de la red (SG) (Notificación). El servidor AAA envía una confirmación al servidor NAS (Acct-Start-Ack).

El elemento especial de la red (SG) memoriza los datos sobre servicios y usuarios, que han sido comunicados de retorno en el perfil del usuario (perfil de servicios). Esta lista puede contener también otros datos de direcciones para el procesamiento futuro. Con la ayuda de estos datos se modificar las reglas para la selección de las rutas (Routing) de una manera adecuada en el elemento especial de la red. De esta manera, se posibilita para el usuario el acceso a los servicios deseados (es decir, se anuncia o se activa).

La activación de servicios se puede realizar

- durante la inscripción, cuando entran los primeros paquetes de datos del usuario, o
- cuando el usuario lleva a cabo una acción (activación o desactivación de un servicio) o
- después del acceso a una dirección o página especial (“Hit”)

En este caso, se emiten, respectivamente, solicitudes Acct-Start, así como Stop-Ack. Las modificaciones son memorizadas en cada caso en el servidor UMS o bien en la base de datos (DB).

De esta manera, se establece una comunicación con el usuario, que tiene ahora acceso al elemento especial de la red, a sus datos y a los servicios activados y activables (Conectar).

Si se necesitan para estos servicios otras informaciones o autentificaciones, entonces éstas se realizan ahora (autentificación adicional, figura 5b).

El usuario puede acceder a servicios también a través del elemento especial de la red. Estos servicios le pueden ser ofrecidos, por ejemplo, por medio de una página Web http por el elemento de la red, de manera que solamente tiene que seleccionar el enlace correspondiente en esta página (acción adicional). En este caso se pueden utilizar otras reglas a partir de su perfil de usuario. Si esto es necesario, se inicia o bien se permite ahora una comunicación con una red, aquí Internet, a través de un servicio de conmutación adecuado.

Los paquetes de datos son enviados con la ayuda de las reglas para la selección de la ruta hacia su destino. En este caso, se pueden realizar desde el elemento especial de servicio (SG) también registros sobre la utilización de servicios individuales.

Si debe establecerse una comunicación con un segundo servicio de conmutación durante la comunicación, esto se puede realizar de la misma manera a través de la selección del “Enlace” correspondiente en la “Homepage”. Las configuraciones para el primer servicio son eliminadas, como se ha descrito anteriormente, en el caso de que se excluyan mutuamente los servicios, que son inscritos para el nuevo servicio. Con la solicitud Acct-Stop y la solicitud Acct-Start se pueden mantener o bien iniciar de nuevo cada vez los registros durante el cierre de un servicio antiguo y la apertura de un servicio nuevo.

Tan pronto como el usuario resuelve (interrumpe) la comunicación, desconectado, por ejemplo, su módem, se anulan de nuevo las entradas. El servidor NAS descubre la interrupción de la comunicación e informa al servidor AAA (solicitud Acct-Stop). Éste informa de nuevo al elemento especial de la red (notificación), que borra a continuación las entradas correspondientes en sus tablas y escribe de nuevo los perfiles de usuario y los perfiles de servicio en la base de datos (DB), si se ha modificado algo. Para terminar los registros, se emite una solicitud Acct-Stop para cada servicio activo y se confirma (Acct-Stop-Ack). Por último, el servidor recibe de la misma manera una confirmación. El servidor AAA termina los registros y envía de retorno una confirmación (Acct-Stop-Ack).

Índice de abreviaturas

AAA	Acceso a cuenta de autenticación
ATM	Modo de transferencia asíncrona
CP	Proveedor de contenidos
DB	Base de datos
DNS	Servicio de nombre de dominio
GRE	Encapsulación de ruta genérica
HTML	Lenguaje marginal de hipertexto
http	Protocolo de transferencia de hipertexto
IF	Interfaz
IP	Protocolo de Internet
ISP	Proveedor de servicios de Internet
L2TP	Protocolo de canal de capa 2
NAS	Servicio de acceso a la red
NAT	Traductor de direcciones de la red
NMS	Sistema de gestión de la red
POP	Punto de presencia
PPP	Protocolo punto a punto
PPTP	Protocolo de canal punto a punto
PRM	Modo de radio Proxy
PSTN	Red telefónica conmutada pública
PVC	Circuito virtual permanente
RADIUS	Servicio de marcación de usuario de autenticación remota
RAS	Servicio de acceso remoto
RM	Módulo de rúter
SG	Puerto de acceso de servicio
SLIP	Protocolo de Internet de línea en serie
SMS	Servidor de gestión del sistema
SMP	Protocolo de gestión de red sencillo
SSM	Módulo de selección de servicio
SVC	Circuito virtual conmutado
TMN	Red de gestión de telecomunicaciones
UMS	Sistema de gestión de usuarios
VPoP	Punto virtual de presencia
WWW	Internet

Índice de literatura

RFC 1055

Nonstandard for transmission of IP datagrams over serial linea (SLIP)

J. Romkey, Junio de 1988

RFC 1171

Point-to-Pint for the transmission of multiprotocoldatagramms over Point-to-Point links (PPP), D. Perkins, CMU, Julio de 1990

RFC 11631

The IP network-Address Translator (NAT)

K. Egevang, Cray Communications, P. Francis, NTT, Mayo de 1994

RFC 1701

Generic Routing Encapsulation (GRE), S. Hanks, NetSmiths, Ltd.

T. Li, D. Farinacci, P. Traina, cisco Systems, Octubre de 1994

RFC 1777

Lightweight Directory Access Protocol (LDAP), W. Yeong. Performance Systems International, T. Howes, Universidad de Michigan, S. Kille, ISODE Consortium, Marzo de 1995

RFC 2138

Remote Authentication Dial in User Service (RADIUS)

C. Rigney, Livingston, A. Rubens, Merit, W. Simpson, Daydreamer S. Willens Livinston, Abril de 1997

RFC 2205

Resource ReSerVarion Protocol (RSVP), R. Graden, Ed., ISI, L. Zhang, UCLA, S. Berson, ISI, S. Herzog, IBM Research, S. Jamin, Universidad de Michigan, Septiembre de 1997.

DNS y BIND

Paul Albitz & Crcket Liu

Edición alemana, 1ª edición 1997, O'Reilly Verlag

Internet Engineering Task Force, INTERNET DRAFT

G. Montyenegro, Sun Microsystems, Inc.

Negotiated Address Reuse (NASR), 1 de Mayo de 1998,

Draft-montenegro-aatn-nar-00.txt

INTERNET DRAFT

Michael Borella, David Grabelsky, Ikhlaq Sidhu, Brian Petry 3Com Corp.

Distributed Network Address Translation, Abril de 1998,

Draft-norella-aatn-dnat-00.txt

REIVINDICACIONES

1. Procedimiento para la determinación de la ruta en una red de datos IP (IP: Protocolo de Internet) o en una red de redes de comunicaciones o de redes de datos IP, en el que se reciben paquetes de datos desde un nodo de red (SG) en la red y con la ayuda de primeras informaciones contenidas en el paquete de datos y a través de la asociación de estas primeras informaciones a segundas informaciones, que están a disposición (DB) en adelante del nodo de la red (SG), se determina para cada paquete de datos desde el nodo de la red (SG) de una manera individual una ruta a través de la red / las redes hacia una dirección de destino, en el que al menos uno de los nodos de la red recorridos en la ruta está fijado sobre la misma ruta sobre la base de la segunda información, y el paquete de datos es transmitido al nodo siguiente de la red sobre la ruta calculada hacia la dirección de destino.

2. Procedimiento de acuerdo con la reivindicación 1, **caracterizado** porque la ruta calculada del paquete de datos desde el nodo de la red (SG) hasta el nodo establecido (A - F) es fijada de una manera clara.

3. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque a partir de las informaciones contenidas en el paquete de datos, se puede calcular uno de los siguientes datos:

- usuario (dirección fuente)
- dirección de destino
- proveedor de servicios (punto de transferencia)
- calidad
- costes
- seguridad

de la transmisión deseada.

4. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la dirección fuente y/o la dirección de destino están compuestas por varios componentes de la dirección.

5. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la dirección de destino contenida en el paquete de datos es falsa o desconocida, y el paquete de datos es enviado hacia una instancia especial en la red y es procesado allí.

6. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque los paquetes de datos transmitidos en esta red desde la dirección fuente hacia la dirección de destino y los paquetes de respuesta emitidos desde la dirección de destino a la dirección fuente recorren el mismo nodo establecido (punto de transferencia).

7. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque en el paquete de datos en la ruta desde la dirección fuente hacia la dirección de destino se modifica la dirección fuente por el nodo de la red (SG).

8. Procedimiento de acuerdo con la reivindicación 7, **caracterizado** porque en un paquete de respuesta se inscribe sobre un paquete de datos original, en la ruta desde la dirección fuente (= dirección de destino original) hacia la dirección de destino (= dirección fuente modificada) desde el nodo de la red la dirección de destino correcta, es decir, que se anula de nuevo la modificación original de la dirección fuente.

9. Procedimiento de acuerdo con la reivindicación 6, 7 u 8, **caracterizado** porque se aplica sobre los paquetes de datos un método de Traducción de la dirección de la red (NAT).

10. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque las direcciones de destino se encuentran en una segunda red de comunicaciones (Nb), que es accesible a través de uno o varios puntos de acceso, pudiendo utilizarse en cada caso solamente uno de estos puntos de acceso en un instante.

11. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque la dirección de destino es un servicio de información (CP), en el que tiene que haberse anunciado un usuario, antes de que pueda utilizarlo, y porque puede utilizar en cada caso varios de estos servicios de información en un instante.

12. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque los paquetes de datos transmitidos están codificados.

13. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque para una dirección fuente están presentes en una base de datos central (DB) unas indicaciones que contienen un estado básico con relación a la autorización de utilización de servicios que están presentes en la red.

14. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque un usuario no está autorizado a utilizar un servicio (CP, ISP) existente en la red y en el caso de emisión de un paquete de datos del usuario no autorizado, este paquete de datos es enviado a una instancia específica en la red, que genera un mensaje de error adecuado.

15. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque un usuario no está autorizado a utilizar un servicio (CP, ISP) existente en la red y en el caso de emisión de un paquete de datos del usuario no autorizado, se genera un mensaje de error adecuado y se envía al usuario.

16. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque un usuario está autorizado a utilizar un servicio existente en la red y, sin embargo, no está registrado en este servicio, y en el caso de emisión de un paquete de datos del usuario no registrado, este paquete de datos es enviado a una instancia especial en la red, que genera un mensaje de error adecuado.

17. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque en virtud de las informaciones acumuladas durante la selección de la ruta de tráfico en el nodo de la red (SG), se puede llevar a cabo una facturación del usuario, en virtud de al menos uno de los siguientes criterios:

- tiempo
- volumen
- número de accesos
- servicios utilizados
- tipo de los paquetes de datos
- calidad de la transmisión.

18. Procedimiento de acuerdo con una de las reivindicaciones anteriores, **caracterizado** porque en virtud de las informaciones acumuladas durante la selección de la ruta de tráfico en el nodo de la red (SG) se puede llevar a cabo una facturación del proveedor del servicio, en virtud de al menos uno de los siguientes criterios

- tiempo
- volumen
- número de accesos
- servicios utilizados
- tipo de los paquetes de datos
- calidad de la transmisión.

19. Dispositivo para la determinación de las rutas de tráfico para paquetes de datos en una red de datos IP o en una de red de redes de comunicaciones y/o de redes de datos IP (SG),

- con medios (RE) para la recepción, procesamiento y transmisión de los paquetes de datos (IP), y
- con medios para la memorización de informaciones adicionales sobre usuarios y/o servicios existentes en las redes (UMS), y
- con medios para la memorización de informaciones de administración (Módulos de Gestión de Servicios), y
- con medios para la determinación de la reproducción de nombres de ordenadores lógicos en direcciones de la red y a la inversa (DNS Proxy Server), y
- con medios para la toma de una determinación de rutas de tráfico para cada paquete de datos individual (IP), tanto con la ayuda de las informaciones calculadas a partir del paquete de datos como también con la ayuda de las informaciones adicionales memorizadas (Módulos de Información de Rutas,

en el que al menos uno de los nodos recorridos en la ruta (punto de transferencia) está fijado claramente en esta ruta, y

- con una interfaz (IF) para la modificación de las informaciones adicionales memorizadas.

20. Dispositivo de acuerdo con la reivindicación 19, **caracterizado** porque se lleva a cabo una trayectoria clara hacia el nodo establecido (punto de transferencia) a través de una comunicación virtual.

21. Dispositivo de acuerdo con una de las reivindicaciones 19 ó 20, **caracterizado** porque es posible un acceso a un servidor, que contiene datos de autenticación y/o datos de acceso y/o datos de facturación (AAA, SMS).

22. Dispositivo de acuerdo con una de las reivindicaciones 19 a 21, **caracterizado** porque existe una interfaz (IF), a través de la cual se pueden modificar las informaciones adicionales memorizadas sobre usuarios y/o servicios existentes (http).

23. Dispositivo de acuerdo con una de las reivindicaciones 19 a 22, **caracterizado** por una posibilidad de ayuda para usuarios, que en el caso de que aparezcan errores durante el acceso a un servicio en la red, se emite un mensaje al usuario con informaciones sobre el error aparecido (http Helpdesk).

24. Dispositivo de acuerdo con la reivindicación 23, **caracterizado** porque la posibilidad de ayuda está configurada de tal forma que en el caso de que aparezcan errores durante el acceso a un servicio, se ofrece un servicio alternativo.

25. Dispositivo de acuerdo con una de las reivindicaciones 23 ó 24, **caracterizado** porque la posibilidad de acceso y/o la posibilidad de ayuda se realizan a través de una interfaz de usuario.

26. Dispositivo de acuerdo con la reivindicación 25, **caracterizado** porque la comunicación con la interfaz de usuario se lleva a cabo por medio de un protocolo adecuado (http).

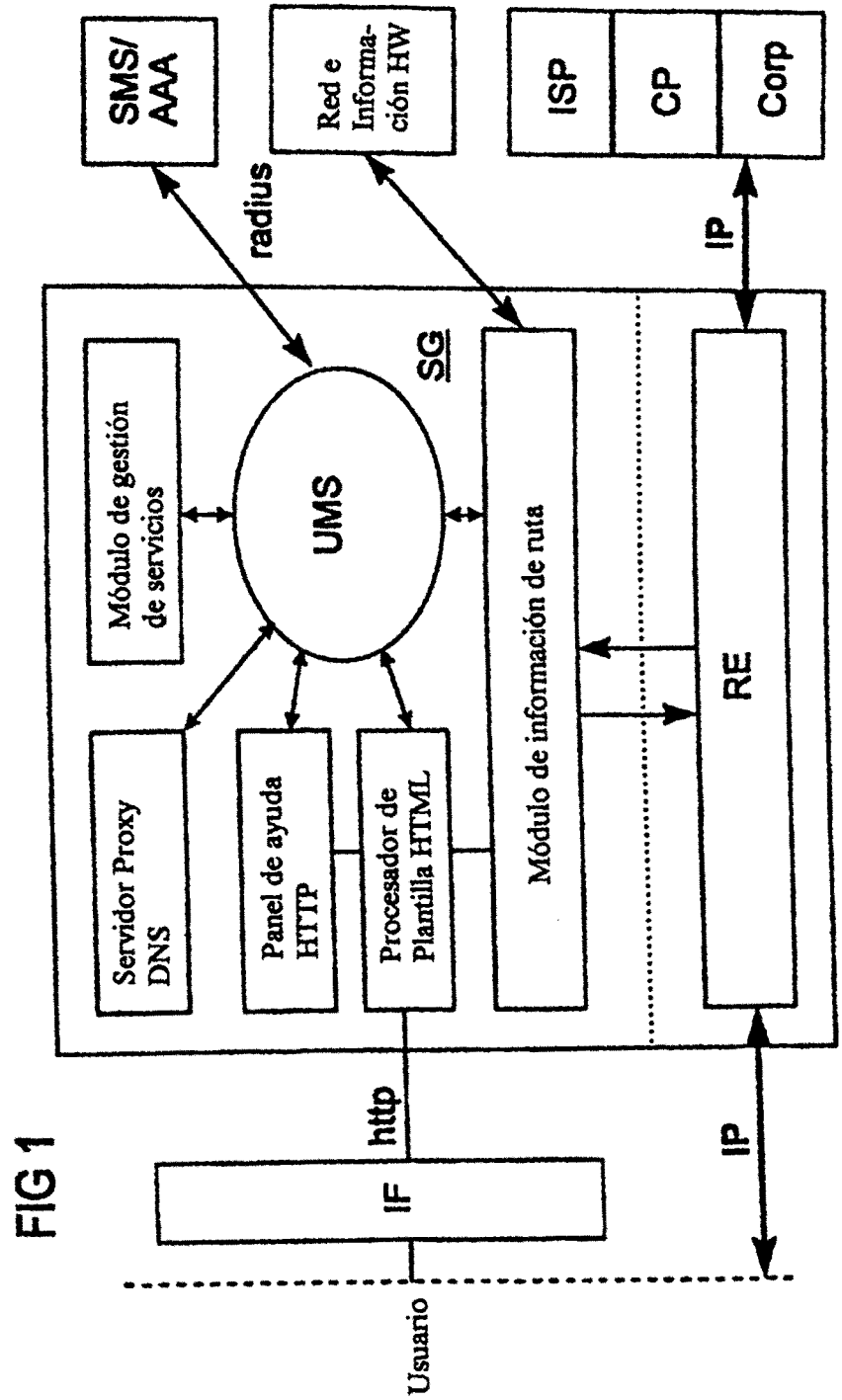
SMS/ AAA
Red e Informa-ción HW
ISP
CP
Corp
radius
IP
SG
Módulo de gestión de servicios
UMS
Módulo de información de ruta
RE
Servidor Proxy DNS
Panel de ayuda HTTP
Procesador de Plantilla HTML
http
IF
IP
Usuario

FIG 1

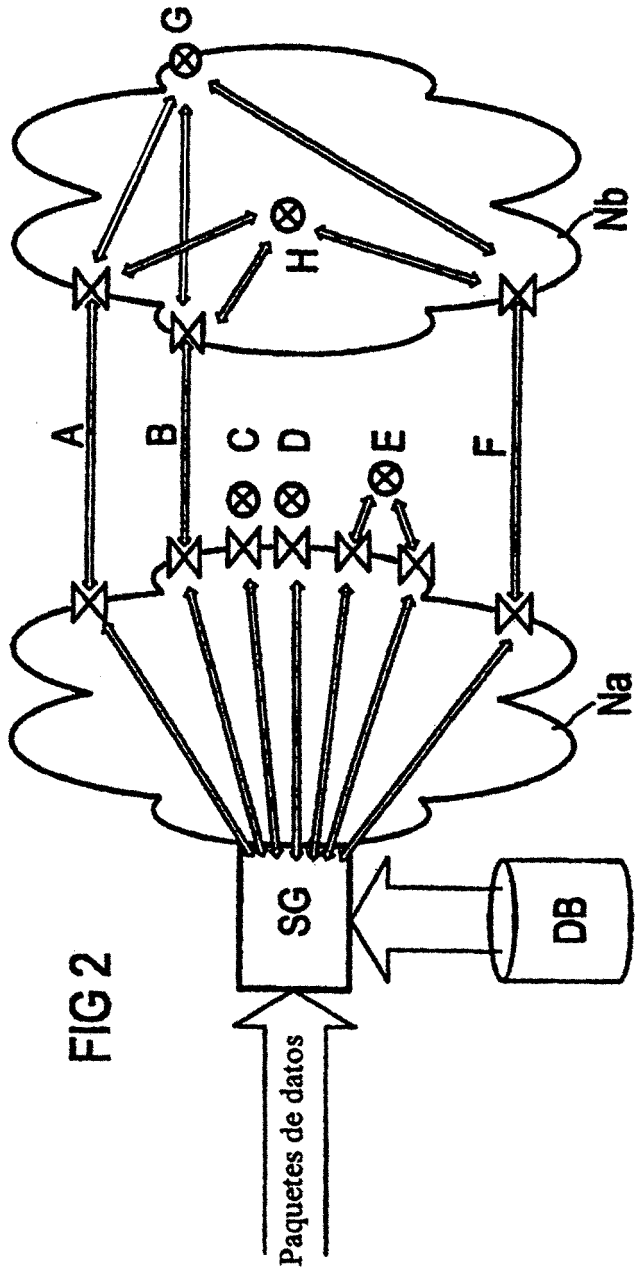

FIG 2

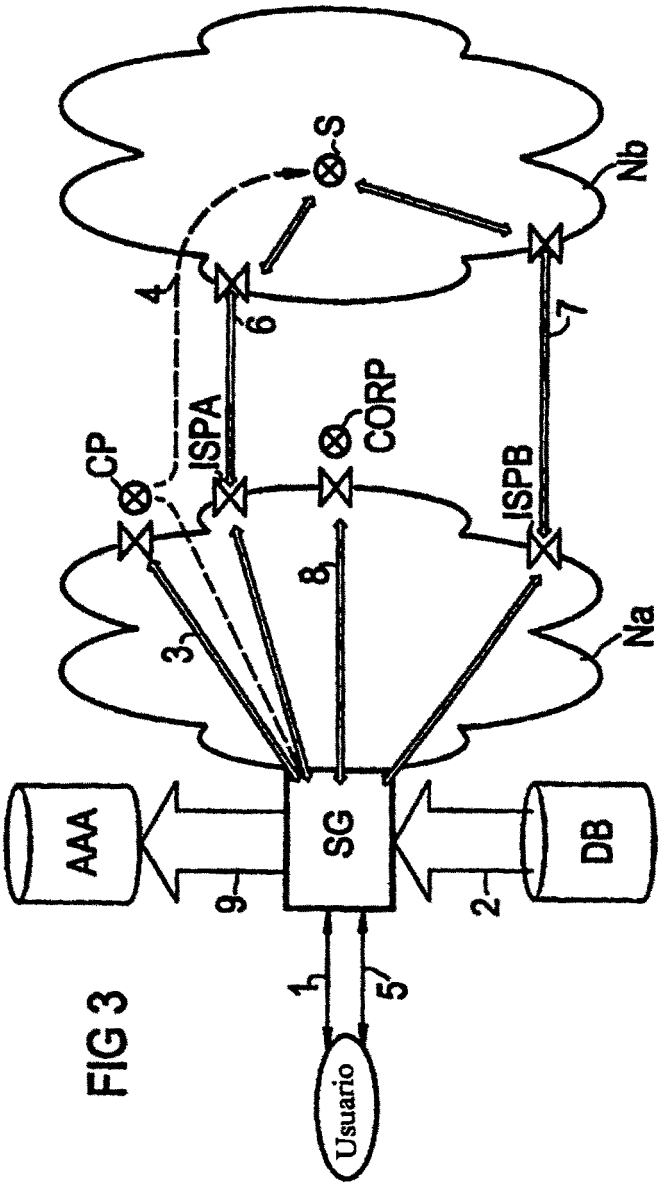

FIG 3

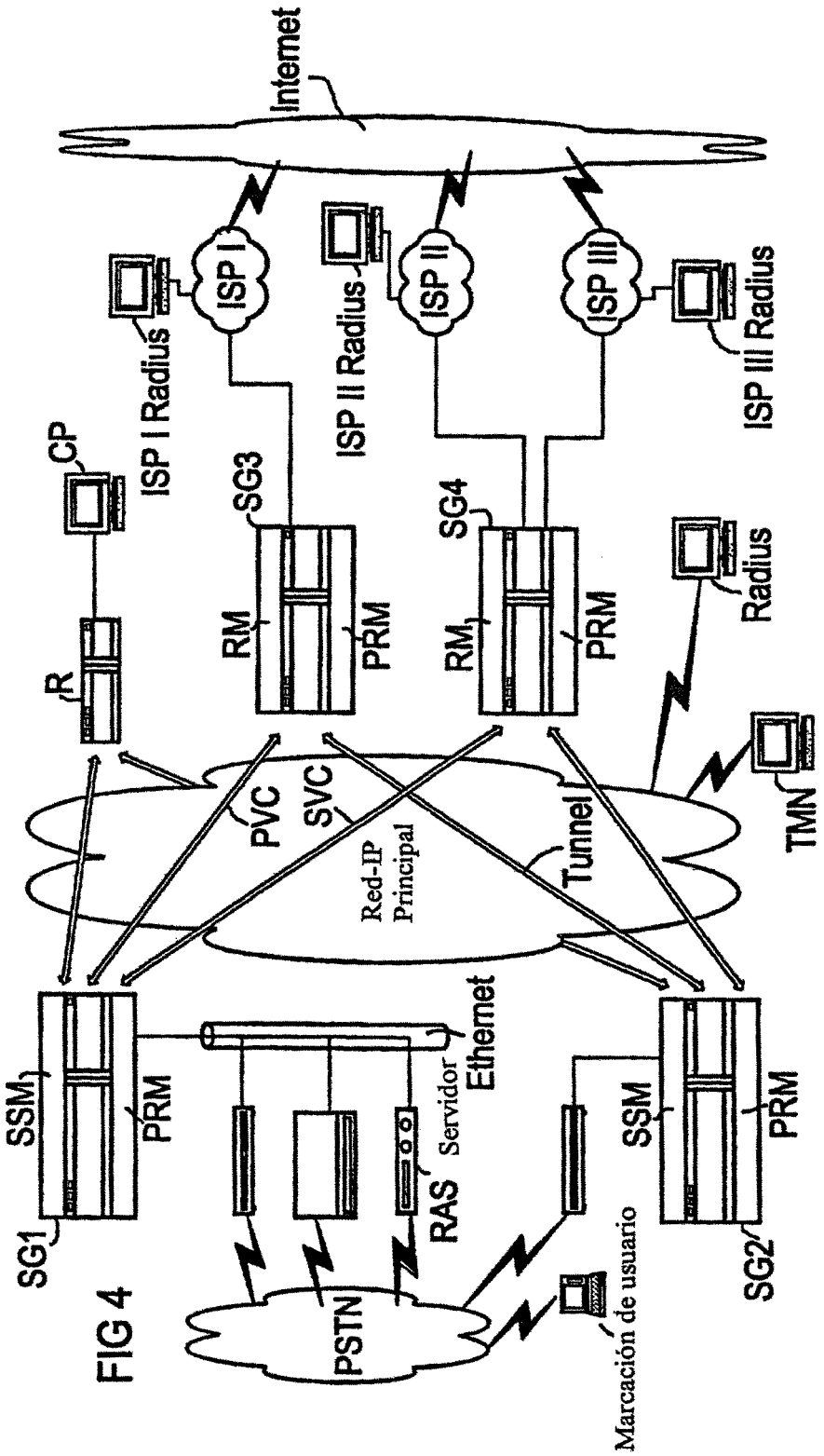
Internet
ISP I
ISP II
ISP III
ISP I Radius
ISP II Radius
ISP III Radius
CP
R
SG3
SG4
RM
PRM
Radius
PVC
SVC
Red-IP Principal
Tunnel
TMN
SSM
SG1
SG2
Ethernet
Servidor
RAS
PSTN
Marcación de usuario

FIG 4

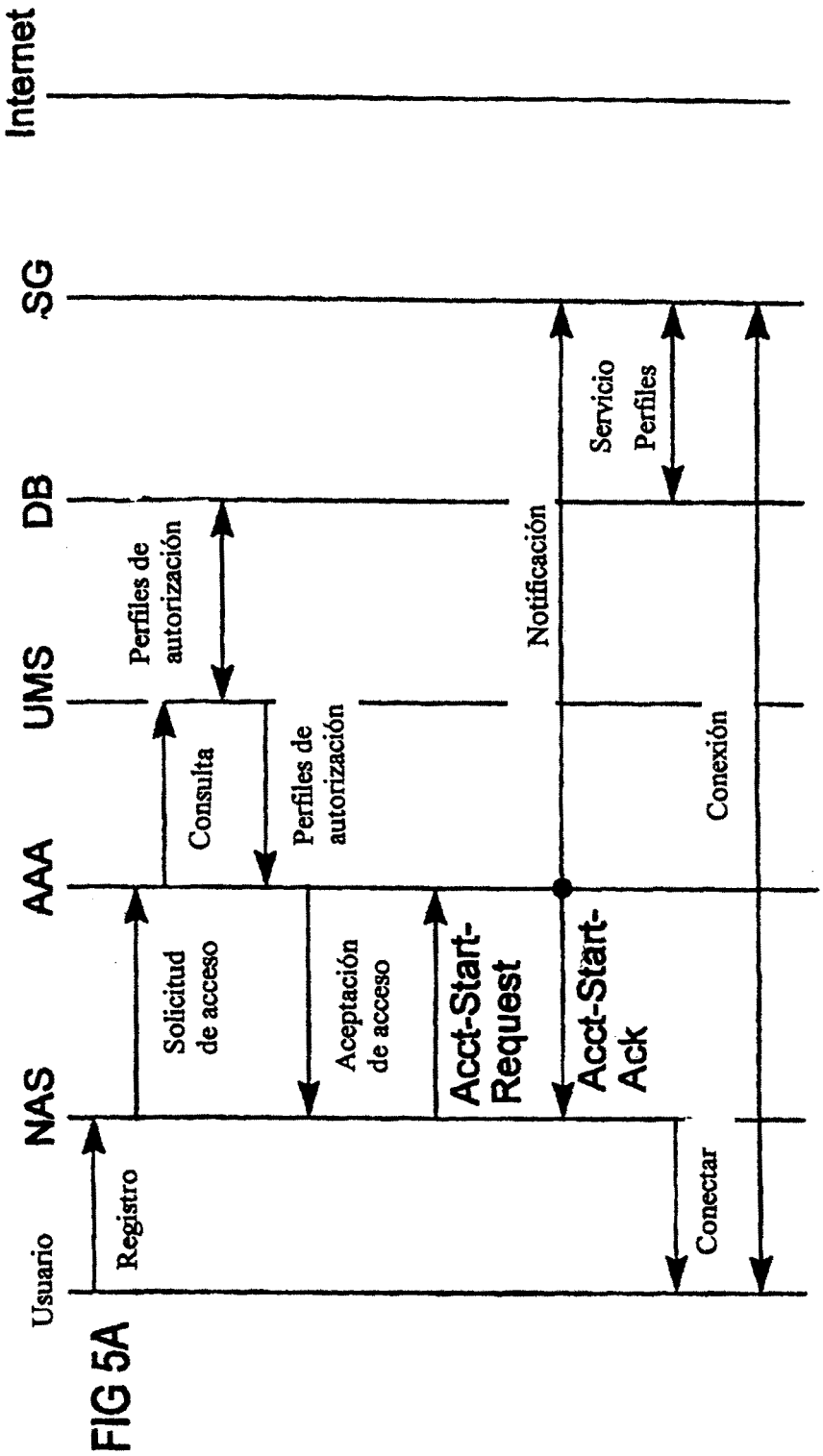
Usuario
NAS
AAA
UMS
DB
SG
Internet
Registro
Solicitud de acceso
Aceptación de acceso
Acct-Start-Request
Acct-Start-Ack
Conectar
Consulta
Perfiles de autorización
Perfiles de autorización
Notificación
Servicio Perfiles
Conexión

FIG 5A

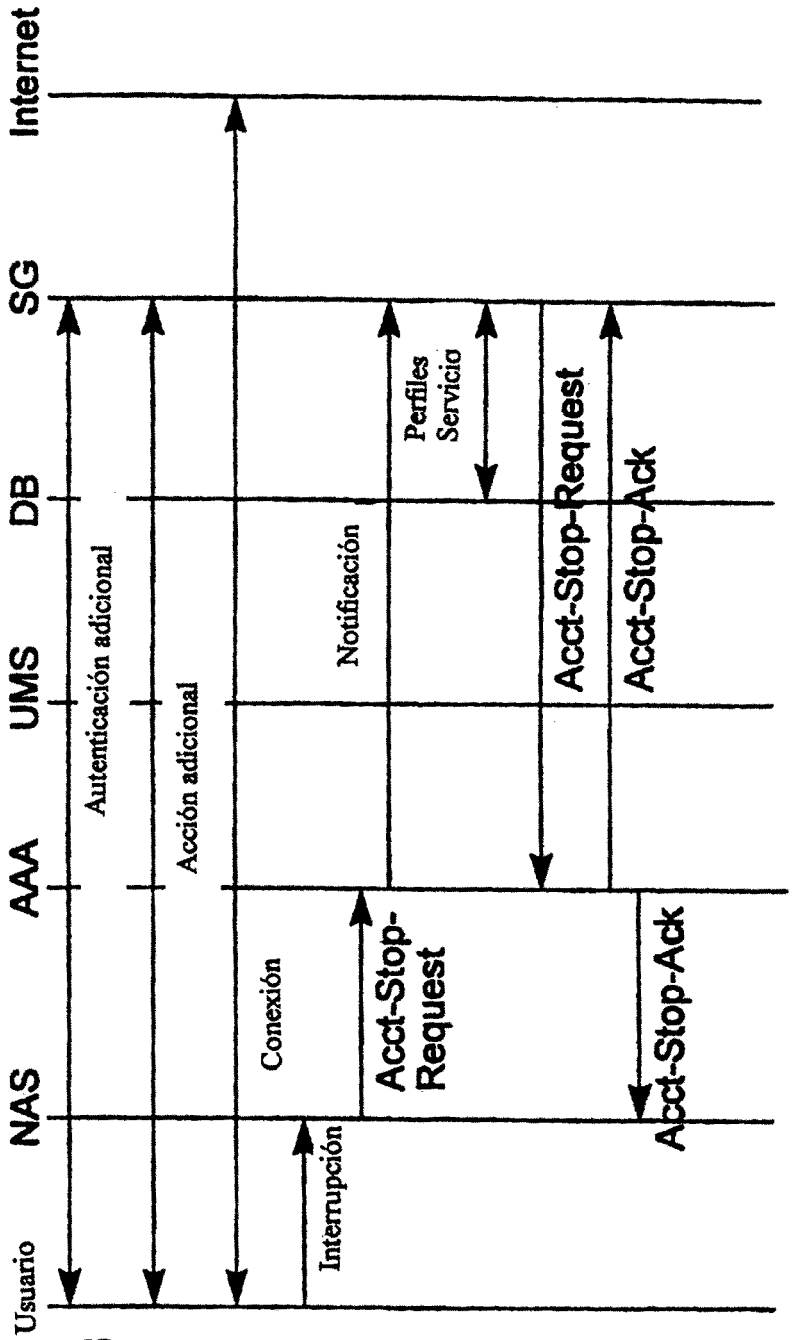
Usuario
NAS
AAA
UMS
DB
SG
Internet
Autenticación adicional
Acción adicional
Conexión
Interrupción
Acct-Stop-Request
Notificación
Perfiles Servicio
Acct-Stop-Request
Acct-Stop-Ack
Acct-Stop-Ack

FIG 5B