Plataforma de comunicaciones B3G para medios de transporte

Iván Lequerica Roca
Telefónica I+D
Emilio Vargas 6, 28043 Madrid
Teléfono 913379436
ilr@tid.es

Carlos Miguel Nieto
Departamento de Ingeniería Telemática
ESTIT, Universidad politécnica de Madrid
Ciudad Universitaria s/n, 28040 Madrid
cmn@dit.upm.es

Resumen

La finalidad de este trabajo es presentar una plataforma de comunicaciones para transportes públicos como trenes de alta velocidad, aviones, autobuses y barcos. Dada su naturaleza móvil se requieren tecnologías de acceso inalámbrico capaces de soportar las velocidades, en muchos casos elevadas, de este tipo de transportes. Se ha optado por una solución mixta utilizando tres tecnologías diferentes: Redes satelitales, UMTS y WiMAX como backbone y WiFi para el acceso final de los usuarios. En cada momento se utilizará el enlace que más convenga en función de disponibilidad (cobertura), ancho de banda y coste manteniendo la calidad de servicio independientemente.

1. Introducción

Las redes denominadas de 4ª generación o B3G ("Beyond 3G") se basan en cuatro pilares; todo IP, movilidad, calidad de servicio (QoS) y AAA (Autenticación-Autorización-Accounting). [1], [2] y [3].

- La principal característica de una red 4G es la utilización de tecnología IP tanto en la red de acceso como en el núcleo para soportar todos los servicios

- Deberán disponer de mecanismos eficientes que permitan la movilidad de usuarios. Esto requiere mecanismos que soporten handover entre subredes bajo igual o distinta tecnología (handover horizontal y vertical) de forma eficiente. La principal propuesta de soporte de movilidad en redes IP son los protocolos Mobile IP aunque para este caso se ha desarrollado una alternativa que lo optimiza. Esta movilidad requiere interaccionar con los procesos de soporte de QoS y con los mecanismos de AAA en los handovers

- Deben soportarse mecanismos de autenticación y autorización para ofrecer mecanismos seguros de identificación de usuarios y acceso a los servicios. Este es el papel de los sistemas AAA, encargados de comprobar la identidad de los usuarios, dar acceso controlado a los servicios disponibles y tarificar por ello

- En estas redes también será necesario proporcionar mecanismos para asegurar la calidad de servicio, teniendo en cuenta parámetros como el ancho de banda, el retardo, el jitter manteniendo el tipo de servicio SLS ("Service Level Specification") contratado por el usuario

La mayoría de los sistemas 4G proponen un modelo de comunicación en el que la tecnología de acceso inalámbrica es variable. Esto provoca unos requisitos elevados de Hardware del usuario final, que deberá ser capaz de soportar varias tecnologías (UMTS, WiFi...) La solución propuesta en este estudio se basa en una sola tecnología de acceso que comunique al usuario final con un controlador de acceso móvil que soportará varias tecnologías inalámbricas. Esta plataforma está especialmente indicada para medios de transporte como trenes, autobuses, barcos e incluso aviones así como para equipos de refuerzos en situaciones de emergencia o desastres naturales.
En la mayor parte del tiempo estos sistemas se encontraran en movimiento y en exteriores siendo ideal la comunicación vía satélite. También pueden encontrarse en entornos cubiertos (como túneles y estaciones) dónde también se desea conectividad, para estos se ha pensado en UMTS y WiMAX, tecnologías que soportan altas velocidades y más baratas y sencillas que el uso de redes satelitales. Debido a la popularidad y rapidez con la que se ha extendido parece adecuado que el acceso de los usuarios sea mediante WiFi, aunque la arquitectura del sistema permite cambiar este acceso de forma sencilla a otras tecnologías incluidas redes LAN cableadas.

2. Descripción general de la solución

En la Fig. 1 se muestra un esquema muy general de la arquitectura de la plataforma. Se puede observar que los usuarios del sistema se conectarán a un interfaz del equipo móvil vía WiFi siendo transparente para ellos el enlace que utilice para comunicarse con el concentrador y finalmente con Internet. Estos enlaces se pueden ver como servicios IP que conectan los equipos móviles con Internet a través de túneles.

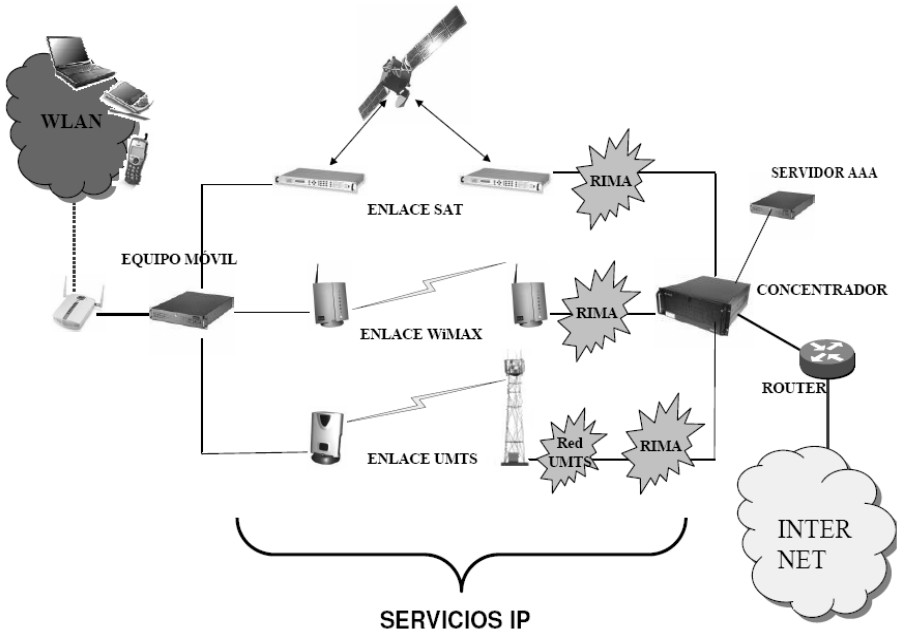

Figura 1. Arquitectura

La plataforma presenta una arquitectura compleja dadas las diferentes tecnologías que utiliza, veamos una descripción de cada uno de los elementos que la componen:

- Equipo móvil. Principalmente tiene tres funciones:
    - Controlador de acceso. Es el encargado de controlar el acceso de los usuarios finales soportando DHCP o configuración fija.
    - Encaminador. Decide por cual de los tres enlaces se comunicará con el exterior. Esta decisión será automática y se tomará en base a parámetros como cobertura, ancho de banda disponible y coste pudiendo incluso tener varios enlaces activos simultáneamente.
    - Marca los paquetes dependiendo del SLS contratado por cada usuario para proporcionar QoS.
- Concentrador.
    - Soporta la movilidad entre los diferentes enlaces según la decisión que tome el equipo móvil en cada momento.
    - Gestiona el provisionamiento de la plataforma. Debe disponer de mecanismos de control por cada tecnología para provisionar recursos asegurando así diferentes niveles de calidad de servicio según las marcas del equipo móvil.
- Servidor AAA. Es el encargado de la autenticación y tarificación de usuarios gracias a un servidor DIAMETER.
- Enlace Satélite. Consiste en túneles sobre una conexión satelital basada en DVB-S y DVB-RCS para el canal de retorno. Es necesario contratar el servicio con una operadora de satélite que conecte su infraestructura al concentrador y preparar los equipos móviles para utilizar esta tecnología en movimiento. Para esto, además del módem, las antenas deben disponer de mecanismos de apuntamiento dinámicos o ser del tipo "fase array" para mantener la comunicación en todo momento.
- Enlace UMTS. Utilizando la tecnología celular UMTS estandarizada por 3GPP se desarrollará un enlace mediante en un módem en el equipo móvil y un túnel sobre la red que proporcione conexión con el concentrador.
- Enlace WiMAX. El equipo móvil dispondrá de un CPE WiMAX, si se desea que funcione en movimiento deberá ser del estándar 802.16e. Las estaciones base estarán conectadas a la red privada del operador (por ejemplo RIMA) al igual que el concentrador.

3. Controlador de acceso

Hay varias formas de implementar un controlador de acceso para clientes Wifi, el que aquí se propone está basado en un conjunto de programas que se ejecutan en un PC bajo el sistema operativo LINUX. Dentro de este equipo generalmente coexisten modificaciones de productos de libre distribución con productos estándar y otros módulos desarrollados específicamente; servidores WEB y de aplicaciones, una base de datos, servidor DNS, DHCP, agente SNMP, servidor proxy...

Los principales elementos son el módulo de control, los demonios de facturación, el portal cautivo y el firewall dinámico. Veamos las funciones de cada uno de ellos:

El corazón del controlador de acceso lo constituye el módulo de control. Se trata de un módulo "kernel" que realiza las siguientes tareas:

- Marcado de paquetes: Según el estado del cliente (no identificado, identificado, validado, etc) y del tipo de contrato (estos datos los obtiene de la respuesta de la autorización enviada al servidor AAA) marca los paquetes de forma que el firewall dinámico los permita o los impida pasar

- Soporte de configuración cero de red: Se encarga de cambiar la dirección IP de los paquetes de las máquinas clientes que no usen DHCP

- Contabilidad en función de tiempo de conexión, tráfico, etc. Cortando el acceso cuando se acaba el crédito

El demonio de facturación está asociado al módulo y se encarga de leer las entradas de sesiones activas y enviar mensajes de facturación al servidor AAA. También lee las entradas desconectadas (por consumo de todo el crédito, tiempo de inactividad, etc) e informa al servidor AAA de esta desconexión actualizando los datos de tráfico y borrando las entradas de la tabla.

El portal cautivo y el firewall dinámico están basados en Iptables y Squid encargándose de las siguientes tareas:

- Capturar a los clientes cuando abran su navegador llevándoles a las páginas del portal independientemente de su página de inicio

- Soportar la configuración cero del navegador, mediante proxy transparente y NAT (Network Address Translation)

- Controlar el flujo de los paquetes basándose en la marca que les haya asignado el módulo de control

- Aplica NAT de salida a Internet (Masquerading)

- Funciones de "Firewall" estático para acceso a servicios locales, como DMZ y para proteger el propio equipo y los clientes de los posibles ataques del exterior

Otros elementos menos importantes dentro del equipo son; la base de datos necesaria para mantener información temporal de las sesiones cursadas; el agente SNMP para generar traps y notificaciones en caso de mal funcionamiento de algún proceso y las utilidades de carga remota encargadas de mantener actualizada la plataforma ante posibles cambios de código o mejoras.

4. Solución de movilidad

Dentro de la plataforma propuesta es imprescindible un mecanismo de encaminamiento que soporte no solo la movilidad del equipo móvil sino también el cambio de enlace por el que se accede a él.

A continuación se explican las dos posibilidades propuestas; Mobile IP [4] y una solución basada en direcciones privadas para cada enlace y solo una IP pública por cada equipo móvil.

4.1. Mobile IP

Mobile IP se diseña desde el IETF para permitir la movilidad en redes haciendo creer al resto de Internet que el equipo móvil siempre se encuentra accesible en su red origen (Home Network). Dentro de la red origen está el HA (Home Agent) que actúa como router con unas funciones especiales cuando el equipo móvil no se encuentra en su red origen.

Cuando el nodo móvil visita otra red (Foreign Network) necesita proveerse de una dirección IP de esta subred visitada, esta dirección se denomina care-of-address y es proporcionada por el FA (Foreign Agent); los paquetes que se envíen a esta dirección serán recibidos por el nodo.

Para comunicarse con otros equipos el nodo utiliza su Home Address, que puede permanecer invariable durante todo el proceso y su care-of-address para que el HA le haga llegar los paquetes. De la coordinación de todo esto se encarga Mobile IP creando un túnel desde la red origen hasta el FA.

Mobile IP se puede resumir en tres mecanismos separados pero relacionados entre sí:

- Anuncio de Servicio. Para que el nodo móvil pueda trabajar en la red visitada debe conseguir una care-of-address en dicha red. Para eso se ha especificado que los agentes puedan hacer broadcast anunciando CAs junto con otra información para los nodos móviles.

- Registro. Consiste en el proceso mediante el cual el FA comunica al HA que tiene al nodo móvil en su red. El HA confirma la información y apunta en su tabla de rutas que el nodo está accesible a través de la nueva care-of-address.

- Encapsulamiento. Una vez que el HA sabe como contactar con el nodo móvil, se crea un túnel entre el HA y el FA. Este último desencapsula los paquetes y los hace llegar al nodo móvil.

En la plataforma propuesta el HA sería siempre el concentrador y el equipo móvil actuaría como nodo y como FA. Puede trabajar como FA sabiendo de antemano las care-of-address que va a tener cada enlace. El proceso sería el siguiente;

1. El equipo arranca y por defecto se configura para que su care-of-address sea la correspondiente al satélite

2. Por este medio se registra en el concentrador (HA) informándole que los paquetes que vayan para él los tiene que enviar por el enlace satélite

3. A continuación se establece el túnel entre el concentrador y el equipo móvil a través del enlace satélite

4. Si se desea cambiar de enlace, el equipo móvil informa al concentrador de su nueva care-of-address (la correspondiente al enlace WiMAX o UMTS), el concentrador lo registra y se vuelve a crear un túnel por el enlace adecuado

Mobile IP es una tecnología estándar, bien probada y robusta pero puede no ser suficientemente rápida en los cambios de enlace y no permite tener varios enlaces operativos simultáneamente.

4.2. Solución ad-hoc propuesta

Otra solución alternativa a Mobile IP es una desarrollada expresamente para esta plataforma que define subredes con direccionamiento privado por cada enlace y una única dirección IP fija por cada equipo móvil.
La solución consiste en dos módulos kernel de Linux, uno en el equipo móvil y otro en el concentrador y un mecanismo de monitorización de los enlaces. A continuación se explican las funciones de cada uno de ellos:
El mecanismo de monitorización de enlaces es un elemento importante sobre el que se apoya este esquema ya que es el encargado de conocer en todo momento que enlaces están operativos y pueden ser utilizados para transmitir. Consiste en un demonio que periódicamente lanza ICMPs desde el equipo móvil a las direcciones privadas del concentrador para conocer que enlaces están activos. Dentro del ICMP se envía una estructura de datos que informa al concentrador de los enlaces que están activos en ese momento. De esta forma tanto el concentrador como el equipo móvil saben que enlaces están activos en cada momento. Esta solución permite definir enlaces unidireccionales de forma que se podría enviar información por un enlace y recibirla por otro.
Para optimizar el cambio de enlace, y dado que los equipos móviles van equipados con GPS, se ha pensado en el uso de mapas de coberturas. De esta forma cuando los equipos realicen trayectos conocidos, la plataforma irá comprobando el mapa de cobertura de los diferentes enlaces y podrá anticiparse a las perdidas de coberturas cambiando de enlace antes que el mecanismo de monitorización indique el nuevo enlace a utilizar.
Las funciones del módulo kernel del equipo móvil son:

- En PREROUTING cambia la dirección destino de los paquetes que le llegan del concentrador. Cambia la IP privada por la que le llega a la IP pública del equipo. De esta forma, internamente siempre le llegarán los paquetes a su IP pública independientemente del enlace que haya utilizado.

- Se define un bridge compuesto por los tres interfaces.

- Se elige el mejor camino por el que enviar los datos en cada momento basándose en los datos del mecanismo de monitorización de enlaces.

- En POSTROUTING se cambia la dirección MAC destino por la del módem del enlace elegido, de esta forma aunque todos los paquetes se envíen por el bridge solo llegarán al módem del enlace elegido.

- Cambia la IP de origen (SNAT) de todos los paquetes que salen (salvo los que lanza el demonio para comprobar los enlaces) de manera que todos salen con la IP pública independientemente del enlace elegido

- Actualiza el estado de los enlaces con los ICMPs del demonio

Las funciones del módulo kernel del concentrador son:

- Actúa como proxy-arp hacia el exterior, anunciando que todos los paquetes provenientes de Internet dirigidos a los equipos móviles se le envíen a él.

- Actualiza el estado de los enlaces con los ICMPs recibidos de los equipos móviles

- En PREROUTING cuando le llega un paquete de Internet con destino algún equipo móvil calcula el mejor enlace y se lo envía cambiando la IP de destino a la privada de ese enlace

Esta solución requiere de más esfuerzo de desarrollo y al no ser una tecnología estándar como Mobile IP es menos robusta, en cambio se tiene mayor control

sobre los enlaces permitiendo que el cambio sea mucho más rápido, también aporta mucha flexibilidad soportando varios enlaces simultáneos o enlaces unidireccionales.

5. Calidad de servicio

Uno de los requisitos principales de esta plataforma es la necesidad de proporcionar mecanismos de calidad de servicio eficaces que permitan ofrecer servicios de tiempo real, típicamente la voz, asegurando a los usuarios los mismos niveles de calidad que les ofrecen las arquitecturas basadas en conmutación de circuitos. Por calidad de servicio o QoS se entenderán los aspectos técnicos para proporcionar al usuario un servicio con determinados requisitos de ancho de banda, retardo, jitter...

Desde sus orígenes, las redes IP han centrado su funcionamiento en mecanismos del tipo best-effort, que consiste en que todos los paquetes reciben el mismo tratamiento, y la red se limita a encaminarlos hasta su destino final.

Las degradaciones del servicio en términos de ancho de banda, retardo y jitter afectan en el modelo best-effort a todos los servicios por igual, y esto puede no ser tolerable en la plataforma propuesta, en la que habrá tráfico perteneciente a servicios de naturaleza muy diferente y con requisitos muy distintos: aplicaciones no sensibles a retardos, como el correo electrónico o la transferencia de archivos, y aplicaciones basadas en el intercambio de flujos en tiempo real.

Es importante destacar las técnicas de señalización para el provisionamiento de recursos como RSVP (Resource ReSerVation Protocol) o más recientemente NSIS (Next Steps in Signaling). Estos protocolos de señalización permiten la comunicación con los elementos de red responsables del provisionamiento para pedir o liberar recursos en cada momento. En trabajos futuros se estudiarán estos aspectos en profundidad.

La plataforma deberá ser capaz de proporcionar y gestionar diferentes calidades de servicio independientemente del enlace utilizado en cada momento. Par ello se deberán desarrollar mecanismos de traspaso de sesión entre enlaces intercambiando información sobre los flujos de datos y la QoS de todos ellos. A continuación veremos las características principales de la tecnología sobre la que se basará la QoS.

DiffServ, estandarizada dentro de IETF, es la propuesta más completa entre todas las realizadas en los últimos años en el campo de QoS. La mayor aportación de esta tecnología viene dada por los mecanismos que introduce para manejar las políticas de prioridad de los flujos.

5.1. DiffServ

Gran parte de los esfuerzos realizados por la IETF en los últimos tiempos se han plasmado en la definición de arquitecturas, como IntServ o DiffServ, que permiten diferenciar entre sí los flujos que atraviesan una red en términos de prestaciones, de acuerdo a unas garantías (IntServ) o expectativas (DiffServ) de calidad. [5] y [6]

El grupo de trabajo DiffServ (Differenciated Services) propuso una arquitectura en la que el tratamiento se lleva a cabo sobre agrupaciones de flujos, de manera que se trata por igual a todos los flujos que requieren la misma clase de servicio. Así se consiguen evitar los problemas de escalabilidad de IntServ.

Por medio de un contrato de tráfico, la red se compromete a dar un determinado trato a los paquetes, con vista a ofrecer una calidad de servicio definida. El tratamiento viene determinado por el contenido del campo DS de la cabecera del paquete IP, que se corresponde con el campo TOS (Type Of Service), en el caso de IP, o con el campo traffic class, cuando se trata de IPv6.

Los paquetes entran en la red de tránsito con una determinada marca, indicativa de la calidad de servicio de que son acreedores, que va a condicionar el tratamiento que los nodos y enlaces les otorguen.

Todos los nodos del núcleo de la red (tanto los exteriores como los interiores) deben disponer de mecanismos de prioridad capaces de discriminar los paquetes en función de sus marcas (este es un requisito que cumplen la práctica totalidad de los equipos actuales). El tratamiento de los paquetes se concreta en lo que se conoce como PHBs (Per Hop Behaviours), que se corresponden con distintos niveles de prioridad:

- Prioridad de servicio. Determina qué paquete se atiende en primer lugar de todos los que están esperando a ser transmitidos por un enlace.

- Prioridad de descarte. En el interior de los nodos los paquetes son almacenados en buffers de tamaño finito. Como consecuencia de esto, cuando se agota su capacidad hay que proceder al descarte de uno o más paquetes. La prioridad de descarte permite determinar cuáles son los paquetes que se van a descartar cuando se produzca esta situación.

Durante su recorrido a través de la red, un paquete recibe distintos PHBs, en función del tratamiento de que sea acreedor, de manera que el servicio ofrecido a un flujo viene determinado por esa sucesión de PHBs. En este contexto, es necesario definir un conjunto de servicios extremo a extremo como sucesiones de PHBs.

La IETF se ha centrado en la especificación de tres tipos de PHBs distintos:

- EF (Expedited Forwarding). Define el tratamiento que se debe dar a los paquetes pertenecientes a flujos de servicios de tiempo real, permitiendo asegurar bajos retardos extremo a extremo, bajo jitter, baja

probabilidad de pérdidas y una tasa mínima garantizada.

- AF (Assured Forwarding). En este caso se definen cuatro prioridades de servicio diferenciadas, cada una de las cuales soporta tres niveles de prioridad ante descartes distintos. La diferenciación en niveles de calidad de servicio viene determinada por la reserva de recursos (ancho de banda y espacio en colas). Se trata de minimizar las congestiones a largo plazo mediante la inclusión de mecanismos activos de gestión de colas, como RED, RIO o WRED.

- BE (Best Effort). Afectaría a los paquetes de los flujos que no desean contratar una calidad de servicio mayor, además de a los paquetes no conformes pertenecientes a flujos de niveles de calidad superiores.

DiffServ se plantea como la solución más adecuada para ofrecer calidades diferenciadas en el seno de las futuras redes. Además es compatible y complementaria de la tecnología de transporte MPLS (Multiprotocol Label Switching) que dispone de mecanismos de ingeniería de tráfico y calidad de servicio basados en la utilización de etiquetas. Usando las dos de manera combinada se pueden aprovechar las capacidades de gestión de tráfico de la primera y las de ingeniería de tráfico de la segunda para ofrecer una cartera de servicios más amplia haciendo un uso más eficiente de los recursos.

El modelo DiffServ se limita a ofrecer expectativas de calidad a los flujos y no garantías absolutas, es decir, asegura que a unos flujos se les trata mejor que a otros, pero no garantiza unos parámetros de calidad concretos a cada grupo de flujos. En este sentido sigue siendo fundamental el realizar un dimensionado adecuado para cumplir con esos parámetros de calidad.

El control sobre los flujos de tráfico se realiza únicamente dentro del dominio IP del operador, pero no se tiene un control extremo a extremo de la comunicación. Sería necesario, por tanto, garantizar la coherencia entre la interpretación que distintos fabricantes de equipos y operadores de red realicen del mismo DS, es decir, que todos empleen las mismas correspondencias entre DS y PHBs, y esta es una tarea bastante difícil. También son muy importantes en este contexto los acuerdos de nivel de servicio (SLS) que el operador del dominio DiffServ tiene con los dominios con los que intercambia tráfico.

En resumen, el modelo Diffserv supone una herramienta simple para ofrecer servicios diferenciados, aunque sea necesario complementarla con otras herramientas de gestión o de dimensionado para explotar todas sus posibilidades. Por todo esto se ha elegido esta arquitectura como modelo de referencia de QoS de la plataforma, tanto el equipo móvil como el concentrador marcaran sus flujos de tráfico atendiendo a las diferentes clases Diffserv y serán los módems de las diferentes tecnologías los responsables de mapear estas clases a sus respectivos mecanismos de calidad.

Veamos las características generales de QoS de cada tecnología y una propuesta mapeo a las clases DiffServ.

5.2. QoS en DVB-S

Las redes satelitales presentan unas características especiales que habrá que tener en cuenta a la hora de planificar la calidad de servicio, como son; retardos elevados, LFN, ráfagas de errores producidas por ruido en el canal (condiciones climatológicas adversas), ancho de banda limitado y muy costoso, fuerte asimetría y accesibilidad intermitente.

Las funciones que intervienen en los mecanismos de QoS las podemos dividir en dos planos [7]:

- Plano C: funciones de señalización de reserva y asignación de ancho de banda

- Plano U: marcado de paquetes, clasificación y descartes

El ancho de banda y la prioridad en el uso de los recursos dependerá de la prioridad asignada al tráfico. La diferenciación del tráfico se realiza por tipo de aplicación en un número mayor de clases de tráfico (hasta un máximo de 8 clases distintas a nivel IP), incluyendo funcionalidad de marcado. El control de admisiones y el control de congestión se basan en el tipo de aplicación y en los recursos disponibles del sistema.

En este tipo de redes satelitales de gran ancho de banda, también conocidas como BSM (Broadband Satellite Multimedia), se definen 8 clases de servicio. Para encajar dentro de la plataforma propuesta, los módems DVB deberán ser capaces de mapear estas clases con los diferentes PHBs de DiffServ con los que marcan los paquetes tanto el concentrador como el equipo móvil. Aunque este tratamiento de QoS no está suficientemente maduro en BSM, en la Tabla 1 se presenta una tabla con una posibilidad de mapeo.

5.3. QoS en UMTS

En UMTS se definen cuatro clases diferentes de QoS (también denominadas clases de tráfico), cuya diferencia fundamental estriba en la sensibilidad de cada una de ellas frente al retardo, agrupando así las posibles aplicaciones a ofrecer [8]. Estas clases reciben el nombre de:

- Clase “conversational”: Pensada para aplicaciones de voz o vídeo “conversacionales”, es decir, una clase de tráfico de tiempo real con requerimientos estrictos de retardo unidireccional máximo o jitter, aunque se acepta una pequeña tasa de pérdidas.

Tabla 1. QoS en DVB-S

Clase de Servicio BSM	*DiffServ PHBs*	*Criterio*
0	EF	Servicios de emergencia y esenciales
1	EF	Aplicaciones de tiempo real, sensibles al jitter, alta interactividad (VoIP)
2	EF	Aplicaciones de tiempo real, sensibles al jitter, interactivas, de tamaño de paquete variable (Video en tiempo real)
3	AF11, AF12, AF21, AF22, AF31	Transacciones, servicios interactivos, señalización, ingeniería de tráfico, PEPs
4	AF13, AF23, AF22, AF32	Transaccciones, PEP, servicios interactivos
5	AF33, AF41, AF42, AF43	Pocas perdidas (Video Streaming)
6	BE	Sin muchas perdidas pero gran retardo
7	BE	Sin especificar, usado para tráfico broadcast o multicast de baja prioridad

- Clase "streaming": Pensada para aplicaciones de voz o vídeo unidireccionales, en las que el destinatario es un ser humano. También se trata de una clase de tráfico de tiempo real pero sin requerimientos estrictos para los parámetros de tiempo ya que se pueden compensar en el receptor a costa de aumentar el retardo unidireccional total. Se acepta una pequeña tasa de pérdidas.

- Clase "interactive": Para aplicaciones en las que un ser humano solicita información a un servidor remoto, como por ejemplo navegación web, aunque también contempla interacciones máquina-máquina. En estas aplicaciones es deseable que la respuesta desde el servidor remoto se produzca en un tiempo acotado y que la red transfiera la información de forma transparente, es decir, con una tasa de error mínima.

- Clase "background": El destinatario de la información no espera recibirla en un tiempo determinado, aunque si espera una tasa de error mínima. Ejemplos de aplicaciones son; MMS y e-mail.

Para mantener los requisitos de cada una de las clases descritas, se definen diversos mecanismos que trabajan en los dos planos:

1. El plano de control se encarga de proveer la QoS antes de establecer la conexión mediante funciones como la asignación de recursos o el control de admisión.
2. El plano de usuario se encarga de proporcionar y mantener la QoS una vez que se ha establecido la portadora, incorpora funciones tales como el control de potencia, la adaptación del enlace o la priorización de paquetes (packet scheduling).

En nuestra plataforma se podrán implementar dos esquemas para la provisión de recursos (ancho de banda y QoS). En la primera; el equipo móvil se encarga de comunicar al concentrador los requisitos de ancho de banda y calidad para las conexiones que está gestionando y este ordenará a la red que se los proporcione. En el segundo esquema es el módem de cada tecnología el encargado de gestionar los recursos.
Hay que recordar que el mecanismo elegido para dotar de QoS a la plataforma es DiffServ, con lo que el módem UMTS deberá mapear las clases de

Tabla 2. QoS en UMTS

Clase UMTS	*DiffServ PHBs*	*Criterio*
Conversational	EF	Garantías deterministas de ancho de banda, pocas pérdidas y bajo jitter
Streaming	AF11, AF12, AF21, AF22, AF31	Bajo jitter
Interactive	AF13, AF23, AF22, AF32, AF33, AF41	Baja latencia y pocas pérdidas
Background	AF42, AF43, BE	Best effort

tráfico de DiffServ con las clases UMTS en el equipo móvil, y la operadora deberá hacer el proceso inverso con los paquetes que salen de su red y pasan a la red RIMA que lleva al concentrador.

En la Tabla 2 se propone un sistema de mapeo entre aquellos PHBs que tienen requisitos de QoS similares a ciertas clases de tráfico en UMTS. El

grupo EF en DiffServ se utiliza cuando es necesario asegurar un cierto ancho de banda con pocas pérdidas y bajo jitter, parece lógico mapear este PHB con la clase "conversational" en UMTS. El grupo AF, más concretamente Afij, permite a un dominio DiffServ proveer diferentes garantías de calidad en base a 4 clases ($N = 4$, $1 \leq i \leq N$) con tres prioridades de descarte cada una ($M = 3$, $1 \leq j \leq M$). Un ejemplo de uso muestra que cuanto menor es el índice de la clase mayor es el nivel de servicio (platino=1, oro=2, plata=3, bronce=4) con baja, media y alta prioridad de descarte (j=1, 2, 3). De esta forma AF11 representa el mejor y AF43 el peor nivel de servicio. Parece lógico mapear los PHBs con las clases "streaming" e "interactive" de UMTS dejando las del tipo BE mapeadas con la clase "background".

5.4. QoS en WiMAX

A continuación detallaremos los mecanismos nativos de los que dispone WiMAX para proporcionar QoS y daremos una solución para nuestra plataforma basada en el mapeo entre las clases de servicio que proporciona esta tecnología y los PHBs de DiffServ. El estándar 802.16 especifica en la capa MAC diferentes tipos de servicios con el fin de proporcionar diferentes niveles de QoS [9]. Estos servicios son:

- UGS. (Unsolicited Grant Services). Está diseñado para proporcionar servicios que necesiten una tasa de transferencia constante como por ejemplo T1/E1 y VoIP sin supresión de silencios
- rtPS. (Real-Time Polling Services). Soporta servicios de tiempo real que generan paquetes de longitud variable como vídeo MPEG o VoIP con supresión de silencios
- nrtPS. (Non-Real-Time Polling Services). Soporta servicios que no transcurren en tiempo real pero requieren el manejo de paquetes de longitud variable
- BE. (Best Effort). Son los servicios típicos de la Internet actual sin ninguna garantía de QoS.

Todas las conexiones entre una estación base y un cliente tienen asignadas varias clases de servicio como parte del proceso de la conexión. Cuando los paquetes se clasifican, lo hacen atendiendo a las garantías de QoS que requiere la aplicación.

WiMAX proporciona a través de su clasificador de paquetes un mapeo entre las clases de servicio soportadas con varias tecnologías a diferentes niveles como pueden ser: TDM, ATM. IP, VLAN... Dado que nuestra plataforma se basa en el mecanismo DiffServ para proporcionar QoS, los CPEs deberán ser capaces de mapear los PHBs de DiffServ con las clases de servicio a nivel MAC que soporta WiMAX. Veamos una posibilidad de mapeo en la Tabla 3.

6. Autenticación, autorización y tarificación basado en DIAMETER

Para la autenticación, autorización y contabilidad (AAA) de la plataforma se ha pensado en un servidor DIAMETER. Diameter es un protocolo IETF que unifica las transacciones AAA [10]. Al

Tabla 3. QoS en WiMAX

Clase de Servicio 802.16	*DiffServ PHBs*	*Criterio*
UGS	EF	Garantías deterministas de ancho de banda, pocas pérdidas y bajo jitter
rtPS	AF11, AF12, AF21, AF22, AF31	Bajo jitter
nrtPS	AF13, AF23, AF22, AF32, AF33, AF41	Baja latencia y pocas pérdidas
BE	AF42, AF43, BE	Best effort

combinar funciones de contabilidad y autenticación, Diameter da soporte en entornos con IP móvil conservando la autenticación como un proceso sencillo al tiempo que minimiza los tiempos de respuesta y la información adjunta (overhead) en la red.
Las principales características de este protocolo son:

- Puede utilizar tanto UDP como TCP en la capa de transporte para los mensajes
- Soporta Mobile IP
- Permite enviar solicitudes de facturación en ambos sentidos
- Ofrece seguridad extremo a extremo con autenticación y cifrado
- Dispone de un mecanismo para informar a los controladores de acceso que está operativo o que va a dejar de estarlo

El esquema de funcionamiento es el siguiente:

1. El usuario, al conectarse a la red WiFi, se le presenta un portal cautivo (gracias al controlador de acceso del quipo móvil) y le pide autenticación.
2. El usuario envía su autenticación al equipo móvil dentro de un mensaje "AA-Request" y este la redirige por el enlace activo al concentrador, donde reside el servidor AAA.
3. Si la información de autenticación es válida, el servidor responde con un mensaje "AA-Response" al equipo móvil con la información de autorización; el tipo de facturación, el tiempo de sesión
4. permitido, los servicios a los que tiene acceso de acuerdo con el SLA del usuario; además se obtienen los parámetros de QoS con los que trabajará el usuario.
5. El controlador de acceso, gracias a unos demonios de facturación, envía mensajes de facturación en el formato estándar ADIF (Accounting Data Interchange Format)
6. El servidor DIAMETER responde con un mensaje de respuesta a la petición de facturación
7. Cuando el usuario se desconecta, el controlador de acceso informa al servidor DIAMETER que puede finalizar la facturación.

7. Funcionamiento global de la plataforma

Para describir el funcionamiento global de la plataforma se divide este apartado en dos secciones;

- Inicio de sesión. Referente a los procesos que se llevan a cabo cuando un usuario se conecta al sistema y entra en sesión.
- Handover. Funcionamiento de la plataforma y procesos que entran en juego cuando el equipo móvil decide cambiar de enlace.

7.1. Inicio de sesión

En este apartado veremos todos los procesos que se llevan a cabo cuando un usuario entra en sesión.

1. Enciende el equipo y se conecta a la red WiFi que controla el equipo móvil. El responsable del servicio deberá facilitar las

claves para una conexión segura con los puntos de acceso basada en WPA-2.

2. El controlador de acceso del equipo móvil le muestra al usuario el portal cautivo y no le permite salir al exterior sin autenticarse. Excepcionalmente se puede permitir "Walled Gardens", es decir, acceso a determinados contenidos sin necesidad de autenticación.
3. El usuario introduce su autenticación. El equipo móvil encamina estos datos por el enlace activo en ese momento hasta el concentrador.
4. El concentrador reenvía la petición al servidor AAA, y este le responde.
5. Si la autenticación es correcta se piden más recursos a la red del enlace activo, bien desde el concentrador (1) o desde el módem del equipo móvil (2). Si no fuera posible proporcionar los recursos necesarios para esta nueva sesión, se puede optar por degradar las demás sesiones para que tenga cabida la nueva o simplemente denegar el servicio informando al usuario de las causas.
6. Si se proporcionan los recursos, el concentrador informa al equipo móvil con un mensaje que contiene los datos de autorización de dicho usuario, es decir, el SLA contratado.
7. Con estos datos, el equipo móvil activa en su tabla al usuario y marca los paquetes de este usuario con los campos Diffserv atendiendo al SLS.
8. Empieza el servicio de tarificación. Desde el equipo móvil comienzan los demonios de tarificación para este usuario, comunicándose por el enlace activo con el servidor AAA tras el concentrador. El equipo móvil dispone de un sistema de tarificación local de forma que si hubiese algún problema con la comunicación con el servidor AAA, la plataforma seguiría tarificando al usuario normalmente y actualizaría los datos en el servidor cuando se restableciesen las comunicaciones
9. Por último, el usuario informa al controlador de acceso del equipo móvil que desea desconectar y este manda al concentrador un mensaje de fin de tarificación y libera los recursos de dicho usuario.

Veamos estos procesos descritos en un diagrama (Fig. 2), el color rojo indica que esos mensajes pueden viajar por cualquiera de los enlaces. Los trazos discontinuos indican varias posibilidades.

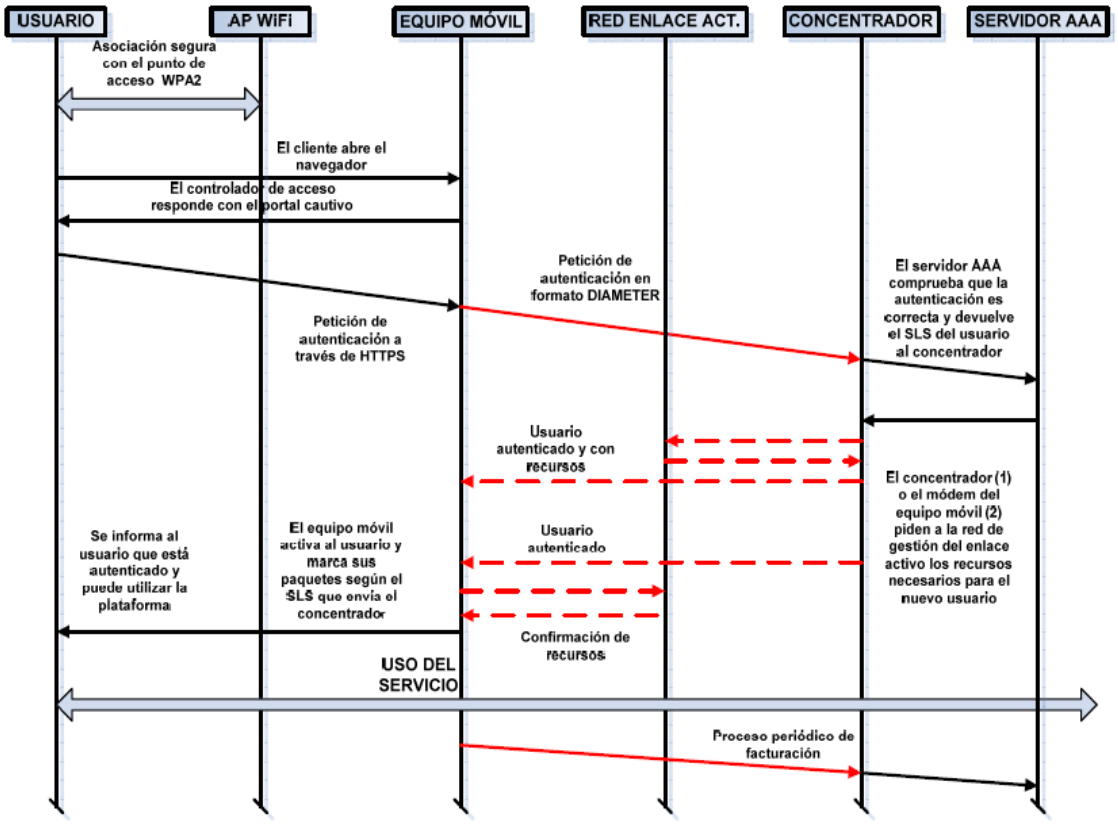

Figura 2. Inicio de sesión

7.2. Handover

De forma análoga al apartado anterior aquí se muestran los procesos que se producen cuando la plataforma cambia de enlace activo para comunicarse con el concentrador:

1. El equipo móvil basándose en el mecanismo de monitorización de enlaces, los mapas de cobertura y la tabla de prioridades (según ancho de banda disponible y coste del enlace principalmente) decide cambiar de enlace usado como backbone informando al concentrador de este hecho
2. Lo primero es conseguir los recursos necesarios en el nuevo enlace, el concentrador (1) o el módem del equipo móvil (2) informa a la red de sus necesidades, anchos de banda y diferentes valores de QoS que deberá proporcionar para la comunicación.
3. Se liberan los recursos disponibles del anterior enlace, si esto no es posible por haber perdido cobertura estos recursos se desactivarán pasado un cierto tiempo configurable para cada red.
4. Se deberá pedir una dirección IP y con ella activar la red privada virtual hasta el concentrador.
5. Una vez que el nuevo enlace está activo, el módem del nuevo enlace debe mapear las clases Diffserv que tienen asociados los paquetes de los diferentes usuarios en el equipo móvil, a los mecanismos de QoS equivalentes que usará en su enlace.
6. A partir de ese momento, todos los datos serán transportados por el nuevo enlace, incluidos los mensajes de tarificación. Dado que es el equipo móvil quien lleva el control de las sesiones de los usuarios, no es necesario una nueva autenticación por parte de estos, siendo transparente el cambio de enlace

Veamos estos pasos representados de forma gráfica en un esquema (Fig 3); el color rojo representa la transmisión por el enlace 1 y los verdes por el enlace 2. Los trazos discontinuos indican varias posibilidades para esos mensajes:

8. Conclusiones

La plataforma propuesta en este documento proporciona un sistema de comunicaciones móviles con las siguientes características:

- De banda ancha; pudiendo llegar en determinados entornos, gracias a la tecnología WiMAX, a los 50Mbps y permitiendo un gran

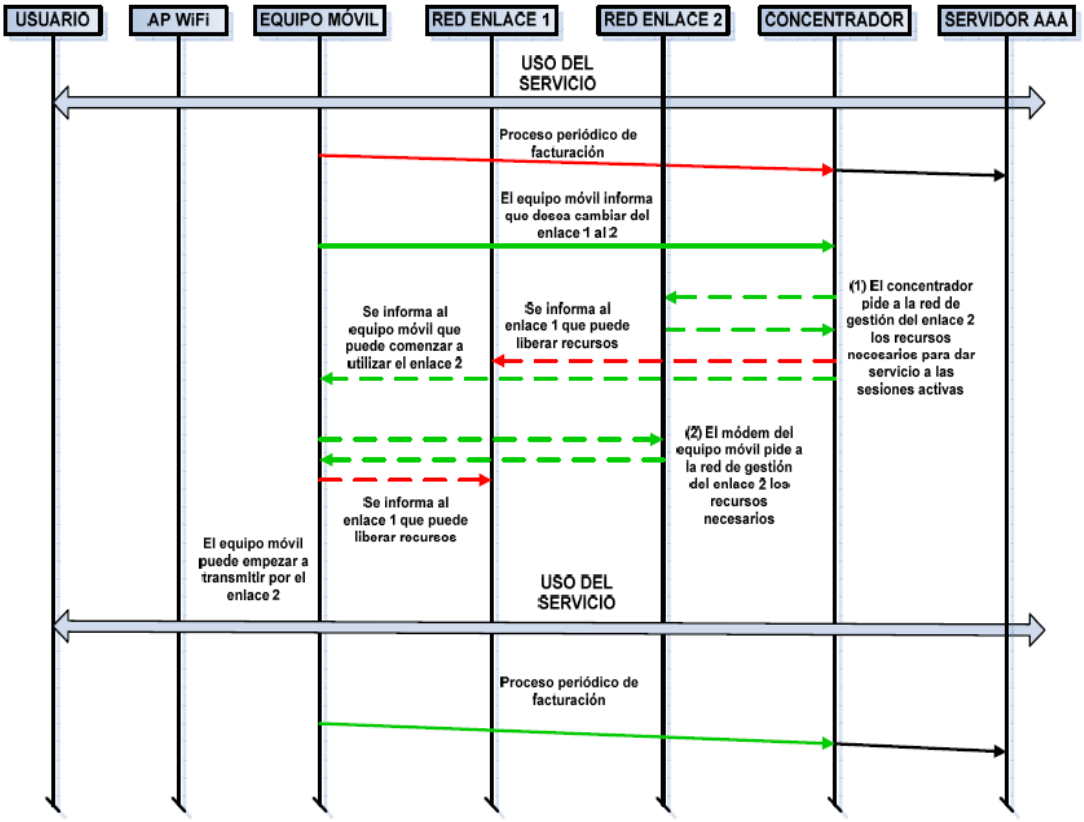

Figura 3. Handover

número de usuarios finales

- Seguro extremo a extremo, tanto en la autenticación basada en DIAMETER como en el cifrado usando IPSec en los túneles sobre las diferentes tecnologías

- Permite priorizar tráfico basado en la tecnología de QoS Diffserv atendiendo los SLS de los usuarios

- Además de conexiones con el exterior permite desplegar servicios locales, como video on demand, streaming de TV y radio en multicast, etc.

- Uno de las principales servicios que funcionarán sobre esta plataforma serán las comunicaciones VoIP, salvo en el enlace satélite en el que el retardo degrada sensiblemente la comunicación, se espera que la experiencia del usuario sea satisfactoria

- Los cambios de enlace se efectúan de forma rápida, siendo dichos cambios transparentes para el usuario

- Está basado en tecnologías estándar y suficientemente maduras

Se ha explicado como desplegar de una forma segura una plataforma de comunicaciones para dar servicio de voz y datos. Esta plataforma además de en medios de transporte se podrá utilizar en:

- Zonas dónde se han producido desastres naturales con sistemas habituales caídos.
- Apoyo a equipos de emergencias como bomberos o rescates de montaña.
- Aplicaciones de consulta en entornos rurales para médicos, veterinarios...
- Como apoyo a sistemas habituales en circunstancias excepcionales con picos de tráfico, conciertos, eventos deportivos...

Referencias

[1] An IP-based QoS architecture for 4G operator scenario. Janusz Gozdecki, Piotr Pacyna, Victor Marques, Rui L. Aguiar, Carlos Garcia, Jose Ignacio Moreno, Christophe Beaujean, Eric Melin, Marco Liebsch.

[2] QoS en redes móviles de cuarta generación. Carlos García, Pedro Antonio Vico. Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid

[3] An all IP solution for QoS mobility management and AAA in 4G mobile networks. L. Dell'Uomo, E. Scarrone; Telecom Italia Lab

[4] RFC 2002. Mobile IP. C. Perkins (IBM)

[5] A Policy Framework for Integrated and Differentiated Services in the Internet. Raju Rajan (AT&T Labs), Dinesh Verma (IBM T. J. Watson Labs), Sanjay Kamat (Bell Labs)

[6] Las telecomunicaciones de Nueva Generación. Telefónica I+D (2004)

[7] Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia (BSM) Services and Architectures QoS Functional Architecture. Draft ETSI TS 102 462 V0.4.2 (2006-01)

[8] QoS Support in the UMTS/GPRS Backbone Network Using Diffserv. Farshid Agharebparast, Victor C. M. Leung. Department of Electrical and Computer Engineering, The University of British Columbia

[9] Providing Integrated QoS Control for IEEE 802.16 Broadband Wireless Access Systems. Jianfeng Chen, Wenhua Jiao, Qian Guo. Lucent Technologies, Bell Labs Research China

[10] http://www.diameter.org