UNIVERSIDAD NACIONAL DE INGENIERIA

FACULTAD DE INGENIERIA ELECTRICA Y ELECTRÓNICA

" PROYECTO TV MOVIL "

INFORME DE INGENIERIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

BORIS PABLO MARTEL SILVA

PROMOCIÓN
1996 – II

LIMA – PERU
2005

PROYECTO TV MOVIL

A mis hijos Pablo y Piero.

A mi esposa Reyna

A mis padres Luz y Armando.

A mis hermanos Ivan, Larissa y Vania.

SUMARIO

El presente informe de ingeniería abarcan las distintas fases que se llevaron a cabo para implementar un servicio de videostreaming sobre una red celular, específicamente el proyecto TV Móvil, cuya aplicación permite a los usuarios móviles el acceso a los distintos canales de televisión por el celular, es decir, poder visualizar el contenido desde cualquier momento y en cualquier lugar donde se encuentre el usuario.

Al ofrecer este tipo de aplicaciones se debe considerar el impacto que puede tener una empresa si empieza a ofrecer servicios en tiempo real (videostreaming). Puesto que si bien obtendrían beneficios dado que los posicionarían como líderes tecnológicos, esto puede ser contraproducente si no se toman en cuenta los requisitos que deben tener estos tipos de aplicaciones en tiempo real, principalmente relacionados al flujo continuo y constante de datos para que se pueda ofrecer una calidad de servicio aceptable. También se deberá considerar la posible demanda que podría tener el servicio comercialmente, en este caso, se debería mantener una calidad aceptable del servicio pero con el menor costo y consumo de recursos posibles.

La investigación demuestra que es posible implementar soluciones en tiempo real en las redes celulares actuales 2G-GSM / 2.5G-GSM sin tener que esperar a redes de tercera generación (3G-GSM). Justamente, la factibilidad técnica para la implementación de estas aplicaciones, se basa en establecer mecanismos de medición y gestión del servicio, de tal forma de ofrecer servicios de streaming considerando los problemas y limitaciones existentes en las redes actuales por ejemplo, anchos de banda reducidos, asignación de canales en forma dinámica y variaciones del retardo entre otros.

INDICE

INTRODUCCION

La necesidad de implementar nuevos servicios de valor agregado para los clientes, obliga a las empresas u operadores en pensar en implementar servicios multimedia en tiempo real, dado que los posicionan como líderes tecnológicos. La aparición de estos servicios multimedia sobre redes en tiempo real, llamado también streaming, representa una de las aplicaciones más avanzadas que se brindan actualmente. Al hacer referencia al término de streaming se deben considerar requisitos de tiempo real que requieren estos servicios, es decir un flujo continuo y constante de datos para que se pueda ofrecer una calidad de servicio aceptable.

El presente informe de ingeniería hace un análisis de factibilidad para la implementación de este tipo de aplicaciones sobre las redes celulares actuales, es decir, se concluye que no es necesario esperar a redes de Tercera Generación Celular (3G) ó tener enlaces con anchos de banda dedicados para poder implementar estos tipos de aplicaciones. El proyecto esta basado en la implementación de un servicio de Televisión por celular, ó llamado también TV Móvil, a través de redes de 2.5G (GPRS), pero también podrían ser implementados en redes de 2G (HSCSD). A su vez, se proveen mecanismos para la medición del servicio, de tal forma de ofrecer aplicaciones de streaming tomando en cuenta los problemas y limitaciones existentes en las redes actuales (celular e Internet), por ejemplo, anchos de banda reducidos, asignación de canales en forma dinámica, actualizaciones del área de enrutamiento y variaciones del retardo entre otros.

Es importante resaltar que el sólo hecho de ofrecer el servicio de TV Móvil en tiempo real usando el celular, brindará a los usuarios la posibilidad de obtener la información desde cualquier lugar y en cualquier momento donde se encuentre. Estos servicios pueden generar mayores expectativas hacia los clientes por la novedad del servicio, pero puede

ser contraproducente sino se toma en cuenta los niveles de calidad que se les puede brindar a estos.

El informe de ingeniería consta esencialmente de 04 capítulos. El primero capítulo abarca el planteamiento del problema, es decir, se plantean los objetivos, hipótesis y la metodología empleada para el desarrollo de esta investigación. El segundo capítulo abarca el marco teórico, partiendo de un recuento sucinto de la historia de las comunicaciones móviles para luego entrar a los conceptos de una arquitectura de red GSM. Posteriormente, se presenta el Servicio General de Paquetes de Radio (GPRS), el protocolo de aplicaciones inalámbricas (WAP) y finalmente, se presentan los conceptos de videostreaming con sus correspondientes tratamientos de protocolos y técnicas de codificación y compresión El tercer capítulo abarca la solución propuesta, en ésta se presentan diferentes productos y soluciones (RealNetworks, Windows Media y QuickTime) para luego presentar el diseño y la arquitectura de la solución propuesta. El cuarto capítulo abarca la ingeniería del proyecto, en esta se presentan las diferentes configuraciones del servicio realizadas en todas las plataformas. A su vez, se presenta un sistema de métricas que permiten monitorear y gestionar estos tipos de servicios. Por último se presentan algunas pautas para la comercialización, los costos involucrados y los tiempos asociados a la implementación del proyecto total de TV Móvil

CAPITULO I
PLANTEAMIENTO DEL PROBLEMA

1.1 Formulación del Problema

Uno de los servicios más innovadores y que actualmente se ofrecen por Internet es el servicio de vídeo en demanda, el cuál permite por ejemplo, que los usuarios puedan acceder a un archivo multimedia para ver y/o escuchar el contenido previamente almacenado en un servidor de streaming.

Asimismo, las demandas de nuevos servicios sobre las redes celulares se están centrando en los contenidos multimedia. Las nuevas aplicaciones multimedia permitirán incrementar los beneficios por el mayor tiempo de uso y el valor agregado que estas aplicaciones ofrecen. Actualmente los servicios están basados en aplicaciones de envío y recepción de fotos y pequeños vídeos de móvil a móvil ó en servicios de descarga de contenido.

Existe una gran diferencia entre los servicios de descarga en comparación a los servicios de streaming, en el primero de ellos, se produce primero el envío de datos y solo después se accede a los contenidos. En cambio, con el servicio de streaming se necesita un flujo continuo, ya que el transporte y el tratamiento de los datos se producen de forma simultánea. Estos servicios pueden ser aplicados a una gran variedad de aplicaciones, tales como: entretenimiento (Música y TV), noticieros, capacitación, mensajes corporativos, soporte a clientes, campañas publicitarias, etc, mediante una transmisión en difusión ó bajo demanda.

Migrar estas aplicaciones hacia una red celular implica tomar en cuenta distintas dificultades en la implementación del servicio. Problemas como el alto tiempo de retardo, el ancho de banda variable, la asimetría del canal, la seguridad de la información, etc., imponen requisitos muy críticos que se deben considerar en el presente estudio. Además, es importante incluir mecanismos que permitan monitorear el sistema una vez lanzado el servicio.

El presente informe de ingeniería hace un análisis de factibilidad para la implementación de este tipo de aplicaciones sobre las redes celulares actuales, es decir, no es necesario esperar a redes de Tercera Generación Celular (3G) ó tener enlaces con anchos de banda dedicados para poder implementar estos tipos de aplicaciones. El proyecto esta basado en la implementación de un servicio de Televisión por celular, ó llamado también TV Móvil, a través de redes de 2.5G (GPRS), pero también podrían ser implementados en redes de 2G (HSCSD). Así como se proponen distintos mecanismos para la medición del servicio, donde su principal característica radica en que centra su atención en el carácter continuo de la información transmitida.

1.2 Objetivos

Los objetivos de la investigación son los siguientes:

- Desarrollar un prototipo de implementación para el servicio de Televisión sobre una Red Celular ó también llamado TV Móvil.
- Proveer herramientas necesarias que permitan medir y gestionar los servicios de streaming sobre estas redes.

1.3 Hipótesis

La arquitectura propuesta permitirá la implementación del servicio TV Móvil sobre una red celular, haciendo posible su medición y gestión.

1.4 Alcances y Limitaciones

El proyecto pretende implementar un prototipo de aplicación de videostreaming. Si bien es cierto, que existen diferentes tipos de software que pueden ser utilizados, el enfoque del proyecto se basa en utilizar el software de RealNetworks, puesto que algunos fabricantes de teléfonos celulares han incorporado el cliente RealPlayer dentro de sus menús de opciones.

A su vez, esta investigación solamente contempla una solución usando la tecnología GSM/GPRS/EDGE y no la tecnología CDMA1X.

1.5 Metodología

La Metodología esta basada en el acopio de información como se detalla a continuación:

- Revisión de documentación respecto a tecnologías de Streaming, incluyendo arquitecturas, protocolos, productos y servicios.
- Revisión de documentación respecto a los sistemas celulares.
- Estudio de estándares y protocolos de señalización y aplicación.
- Estudio para la integración de tecnologías de Streaming sobre una red celular.
- Revisión de documentación de métricas del servicio.
- Revisión de los manuales del servidor de streaming.
- Estudio del tipo de métricas a implementar.
- Ordenamiento y Sumarización de la información.
- Construcción del Prototipo.
- Observaciones y Conclusiones.

CAPITULO II
MARCO TEORICO

El presente capitulo tiene como objetivo describir el marco teórico que permite comprender como se implemento el servicio de TV Móvil en una red celular GSM. Primero se describe el funcionamiento de una red de telefonía celular enfocándose principalmente en la tecnología GSM, para luego explicar el funcionamiento de una red GPRS, que representa el nivel de transporte del servicio de TV Móvil y otras aplicaciones avanzadas. Luego, se describe el Protocolo de Aplicaciones Inalámbricas (WAP), el cuál es utilizado para el acceso al servicio de TV Móvil (control remoto para elección de los canales). Por último, se describe las características y funcionamiento de los servicios de streaming.

Las comunicaciones móviles celulares representan un punto importante en el proceso de evolución de las Telecomunicaciones, puesto que permiten emprender nuevas actividades principalmente debido a su movilidad, ya que donde exista cobertura y se tengan recursos disponibles en la red del operador, un abonado siempre será ubicado y podrá utilizar todos los servicios a los cuales se ha suscrito. A partir de un concepto básico, los sistemas inalámbricos han evolucionado hacia sistemas de uso masivos y complejos, compuestos por entidades muy diferentes utilizando a su vez distintos tipos de transmisión inalámbrica de datos.

Aunque existen muchos tipos de sistemas, actualmente sólo se utilizan tres tipos básicos de sistemas de modulación, los cuales son:

El sistema FDMA - Frequency Division Multiple Access (Acceso múltiple por división de frecuencias) transmite un circuito de voz por frecuencia. La información se transporta en formato analógico.

El sistema TDMA - Time Division Multiple Access (Acceso múltiple por división de tiempo) es un formato digital que "codifica" la señal analógica. El canal asignado se divide en varios intervalos de tiempo. Cada intervalo de tiempo puede transportar un circuito de voz.

Dependiendo del ancho de banda y del tipo de sistema, 3 o más circuitos de voz pueden reemplazar un circuito de voz analógico.

El sistema CDMA - Code Division Multiple Access (Acceso múltiple por división de código) es una tecnología digital de espectro expandido. CDMA asigna uno de 4,4 billones de códigos disponibles a cada circuito de voz digital. La unidad receptora decodifica sólo la señal que se le envió. Esto permite enviar varias conversaciones por la misma frecuencia.

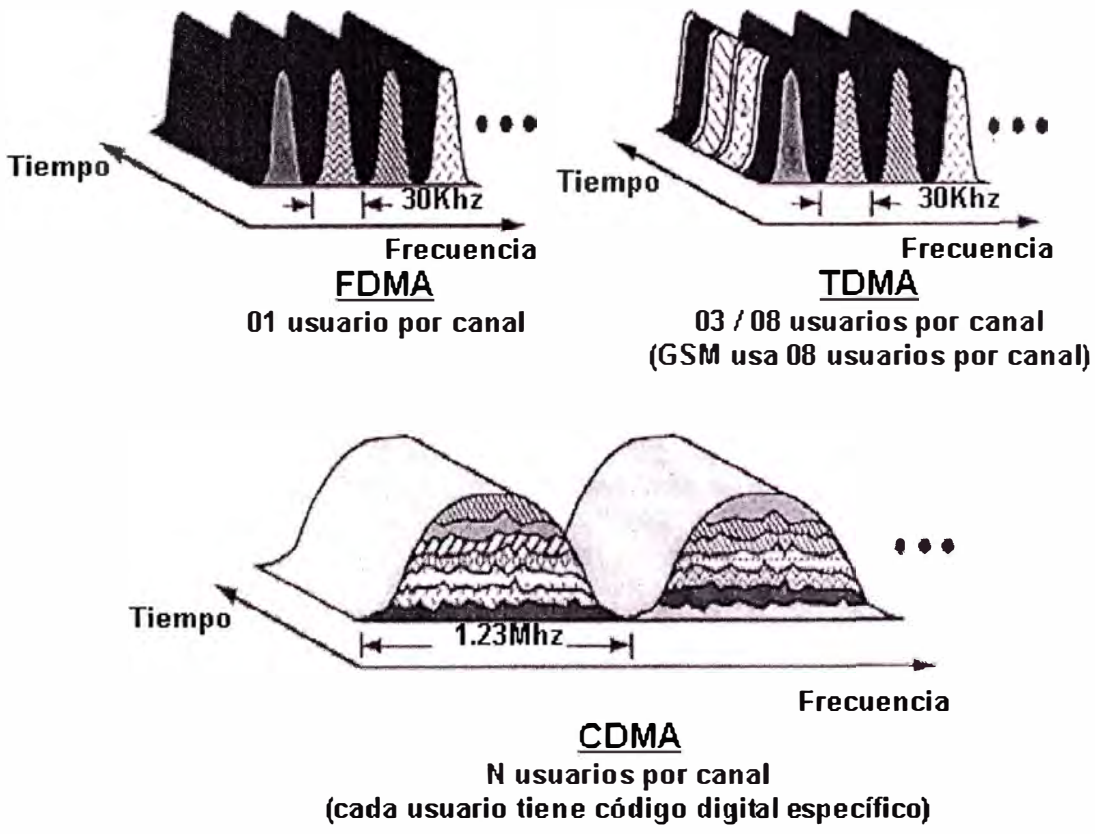


Figura 2.1 Sistemas de Modulación

2.1 Historia de las Comunicaciones Móviles Celulares

Las redes de telecomunicaciones móviles pueden ser considerados como un sistema y un servicio. Puesto que los equipamientos de red, incluidas las estaciones base, las centrales de conmutación, las centrales de bases de datos, etc., representan en sí al sistema de telecomunicación móvil, los cuales proveen los servicios a los abonados suscritos en la red. Se podría decir que los sistemas móviles se han desarrollado en tres generaciones, aunque actualmente, ya se habla también de los sistemas de cuarta generación de

comunicaciones móviles. En las siguientes líneas explicaremos cada una de estas generaciones.

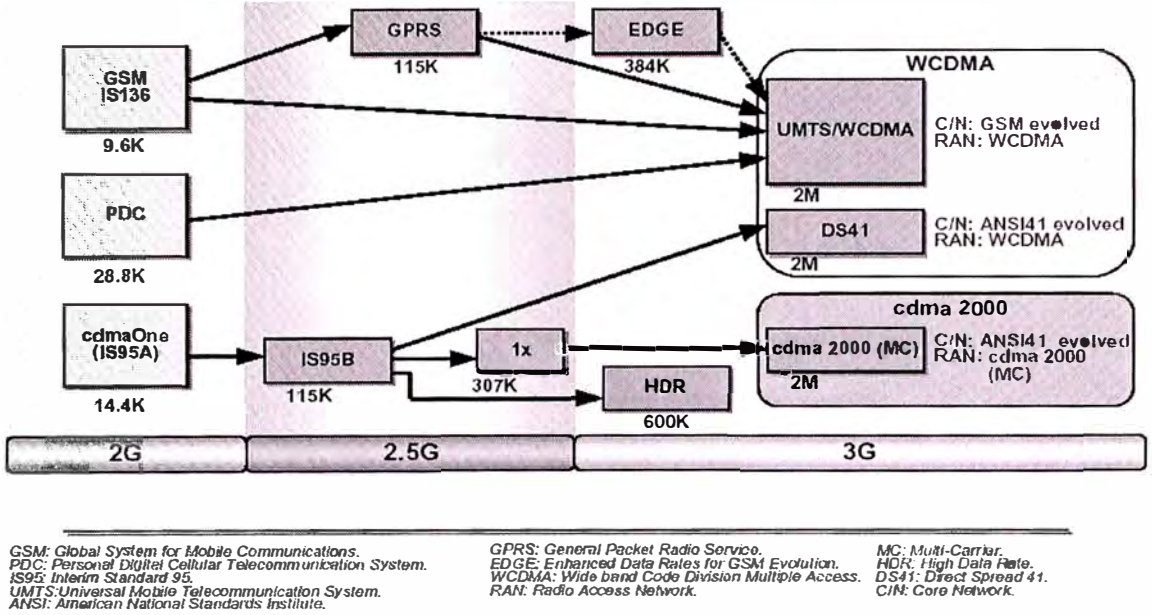


Figura 2.2 Evolución 3G

Sistemas de Primera Generación – 1G

Estos sistemas utilizan el FDMA (Frequency Division Multiple Access) - Acceso múltiple por división de frecuencias, el cual utiliza un circuito de voz por canal de frecuencia. Comúnmente los sistemas de Primera Generación son llamados Sistemas Analógicos, puesto que la información es transportada en ese formato.

El primer sistema celular fue conocido como AMPS (Advanced Mobile Phone Service) – Servicio Telefónico Móvil Avanzado, la cual fue desarrollada por Bell Laboratories en 1947(8). El término celular se refiere a que la red utiliza pequeñas celdas ó estaciones de radio, que proveen una cobertura muy limitada, estas estaciones de radio se conectan a una central de conmutación, que administra la movilidad de los abonados y además realiza la interconexión con la red de telefonía pública fija.

El sistema AMPS opera en el rango de frecuencia de 800 – 900 MHz, este se divide en 832 canales de frecuencias. Para la transmisión de la señal desde el teléfono MS (Mobile Station), a la estación base BTS Base Transceiver Station, se requiere una frecuencia y en la dirección inversa, desde la BTS al MS, se requiere otra. Esto permite un canal full

dúplex entre la MS y la BS. Cada canal opera en un ancho de banda de 30Khz, tal como se muestra en la siguiente figura. Los operadores que soportan esta tecnología en el Perú son Telefónica Móviles y BellSouth.

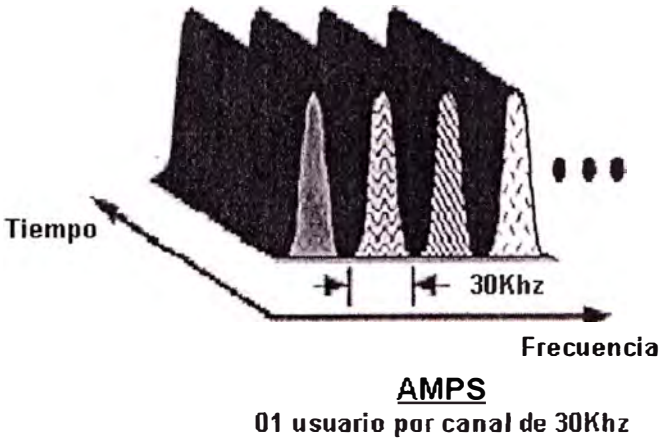


Figura 2.3 Sistemas AMPS

Así como en la región Americana apareció la norma AMPS, en Europa utilizaron la norma TACS (Total Access Communication System), Sistema de Comunicación de Acceso Total, estos funcionaban en la banda de 900MHZ, los cuales fueron junto al AMPS los sistemas que más abonados tenían en el mundo. En este caso, cada usuario utiliza un ancho de banda de 25KHZ, tal como se muestra en la siguiente figura:

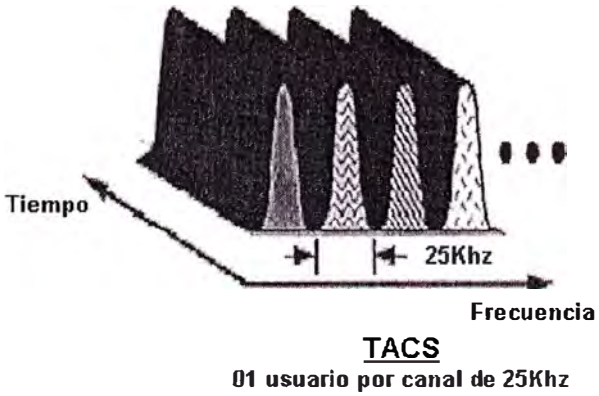
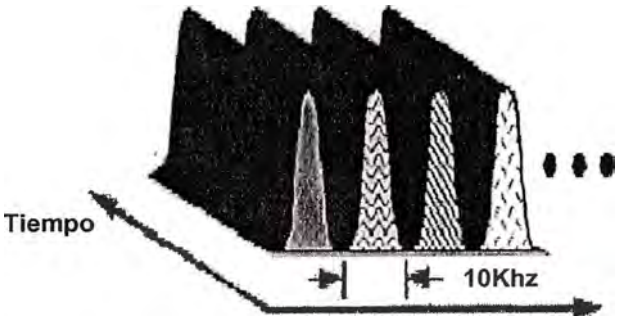


Figura 2.4 Sistemas TACS

Para expandir la capacidad de la red sin frecuencias adicionales, algunos fabricantes de equipos celulares prefirieron asignar más canales analógicos reduciendo el ancho de

banda de una llamada de voz a 10Khz (ver Figura 2.5). Esto permitió tener la misma capacidad que algunos sistemas de segunda generación, sin que se requiriera una nueva tecnología. Este nuevo sistema analógico se conoció como NAMPS (Narrowband AMPS), Sistema AMPS de Banda Estrecha, pero los teléfonos también deberían soportar esta funcionalidad. En Perú, solo Telefónica Móviles utiliza esta tecnología.



NAMPS
01 usuario por canal de 10Khz

Figura 2.5 Sistemas NAMPS

Sistemas de Segunda Generación – 2G

El sistema celular analógico creció aceleradamente y rápidamente se congestionó de abonados. Como respuesta, la industria celular aceptó una norma digital en 1989. Esta norma se conoció como la DAMPS (Digital AMPS)(4), las cuales utilizan dos tipos de sistemas de modulación: TDMA y CDMA.

En sistemas TDMA, cada usuario alterna el uso de la portadora en un time slot y solamente puede enviar ó recibir información en un tiempo dado. Es por ello, que el flujo de la información no es continua para un usuario, pero es enviada y recibida en ráfagas en un tiempo dado. Luego, las ráfagas son reensambladas por el receptor, el cual piensa que la información que recibe es continua debido a la rapidez de la información.

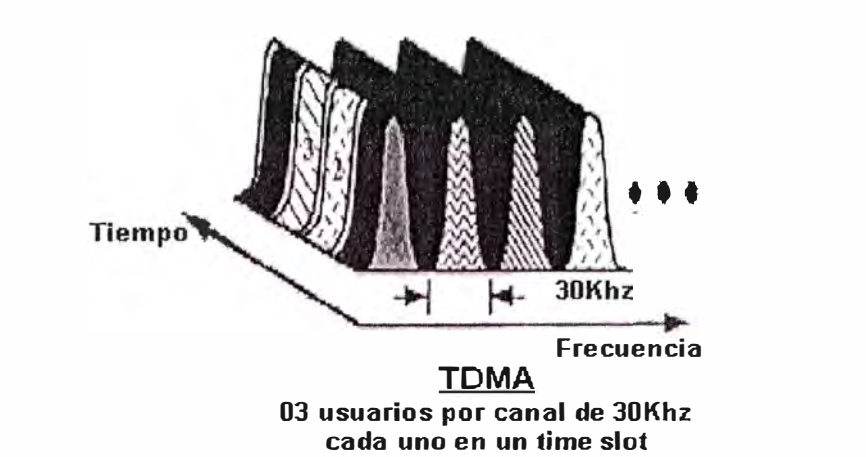


Figura 2.6 Sistemas TDMA

Es decir, utilizando la tecnología TDMA, la industria celular pudo triplicar el número de abonados que la red podía manejar sin agregar frecuencias adicionales. En el mismo ancho de banda de señal que se requería para una llamada analógica podían ahora realizarse tres llamadas digitales. DAMPS está diseñado para coexistir con el sistema AMPS. Los proveedores de servicio pueden respaldar tanto sistemas analógicos como digitales de la misma estación. La operadora que soporta esta tecnología en el Perú es BellSouth.

En los sistemas celulares digitales, las señales de los sistemas analógicos coexistentes se convierten a un formato digital y luego se "codifican" para reducir la cantidad de bits necesarios. La señal digital codificada se envía al MS donde es convertida nuevamente a una señal analógica. Es importante resaltar, que ningún usuario puede acceder en un time slot hasta que la llamada original haya finalizado ó hasta que la llamada haya pasado a una diferente frecuencia, a esto último se le conoce como el proceso de handoff. En algunos países de Europa surgió también el Sistema PDC, que es en sí un tipo de sistema TDMA, pero la portadora es dividida en tres canales de 25KHZ, tal como se muestra en la siguiente gráfica:

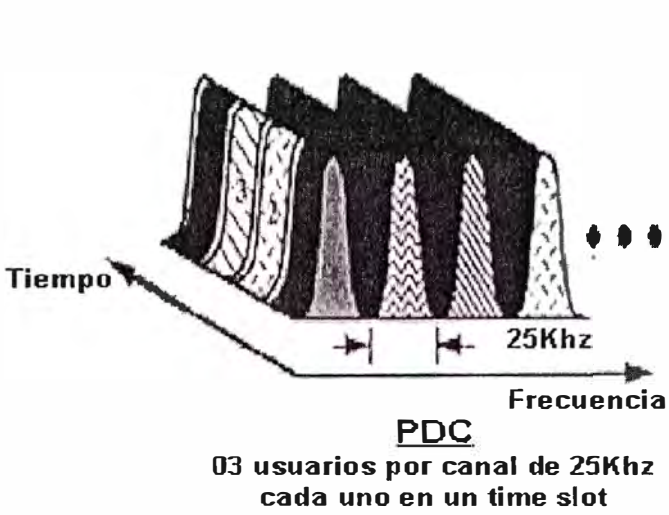


Figura 2.7 Sistemas PDC

Pero el sistema digital que más se desarrollo en Europa y que predomina actualmente en todo el mundo es el Sistema GSM - Global System for Mobile Communications (Sistema Global para Comunicaciones Móviles)(12). GSM fue uno de los primeros sistemas digitales seguido a la era analógica. Surgió principalmente para resolver los problemas de los sistemas analógicos, entre ellos están los referidios a la capacidad, disponibilidad de frecuencias y sistemas no seguros entre otros. Debido a ello, se creó en 1982 en la CEPT (Conference Européenne des Postes et Telecommunications) un grupo de trabajo denominado GSM (Groupe Spéciale Mobile), con el fin de preparar un estándar europeo de red móvil ó PLMN (Public Land Mobile Network) para todos los países pertenecientes a la CEPT. Una de las primeras decisiones adoptadas fue la de reservar una banda de frecuencia común que permitiera el roaming (itinerancia) internacional. La banda elegida consta de dos sub-bandas de 25MHz de ancho de banda, cada una: 890-915 MHz y 935-960 MHz.

El nombre del grupo acabo designando la norma, la cual hoy día se conoce como red PLMN-GSM, ó abreviadamente GSM. En el año 1989 la responsabilidad de normalización recae en el ETSI (European Telecommunications Standards Institute), reestructurándose los grupos de trabajo que adquieren otra denominación. Entonces se reinterpreta el significado del acrónimo GSM pasando a designar el término Global System for Mobile Communications. Este sistema opera sobre la norma TDMA. Los canales GSM son de

200 kHz de ancho y soportan hasta ocho usuarios por canal. Este sistema fue diseñado para operar en el espectro de 900 MHz.

En la región americana (América del Norte, Centro y Sur) existe una variación de GSM que opera en el espectro PCS cuyo rango de frecuencias esta entre los 1800 – 1900 MHz (excepto Brasil que opera a la misma frecuencia de Europa 900MHZ). Actualmente, el único operador que ofrece esta tecnología en Perú es TIM.

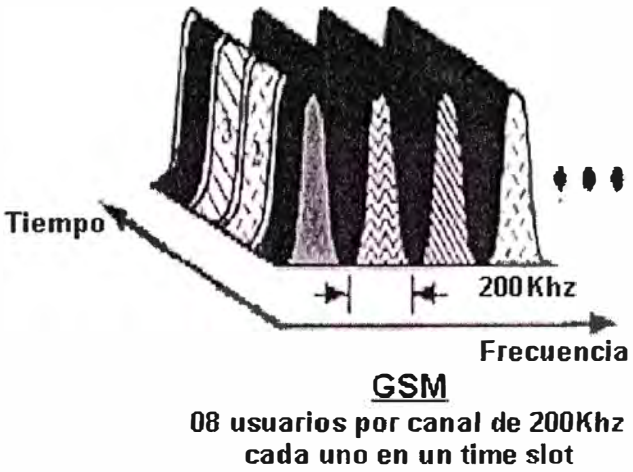


Figura 2.8 Sistemas GSM

Así como en Europa surgió la tecnología GSM, en Estados Unidos el gobierno americano desarrollo la tecnología CDMA para tener un medio de comunicaciones seguro que fuese también resistente a los efectos de interferencias de señales enemigas. La tecnología CDMA expande la data digital de la señal a ser entregada a un espectro de frecuencia ancho, reduciendo el efecto negativo de una señal de interferencia en un ancho de banda angosto de una frecuencia particular. La tecnología CDMA fue primero propuesta para uso en un ambiente celular por la compañía QualComm, con sede en San Diego Califomia(13). La tecnología CDMA es definido por un Interim Standard de la CTIA: IS-95A. El estándar actual es el IS95B que contiene algunas mejoras de la versión anterior. El primer canal CDMA físico requerirá 1.77 Mhz (1.23 Mhz de banda, 270 Khz de banda de guarda en cada extremo). Actualmente, el único operador que ofrece esta tecnología es Telefónica Móviles.

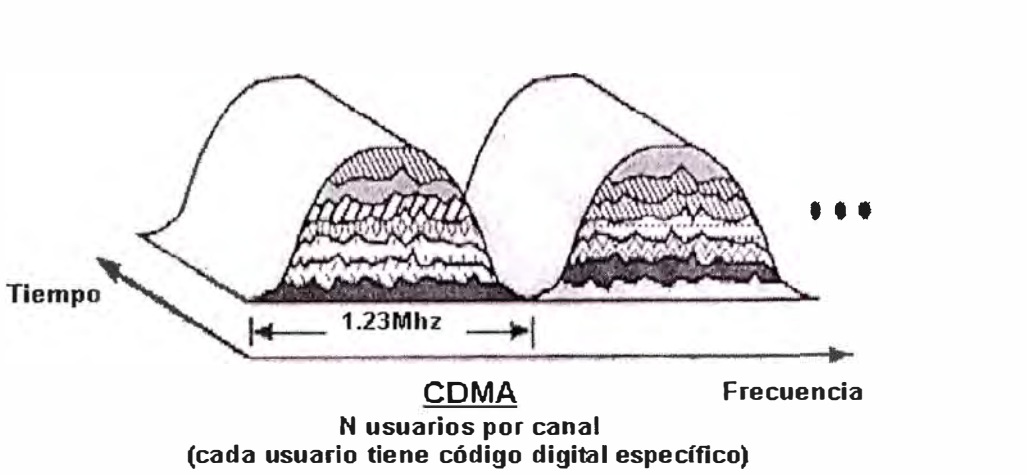


Figura 2.9 Sistemas CDMA

Sistemas de 2.5G

Una forma de mejorar la capacidad de GSM y al mismo tiempo, aumentar los servicios es introducir la tecnología de conmutación de paquetes. El GPRS utiliza esencialmente, la misma interfase aire que el GSM convencional, pero incluye una nueva capa de acceso al medio MAC (Médium Access Control) y una nueva capa de control de radio RLC (Radio Link Control) permitiendo que la transmisión de la información se pueda realizar a distintas velocidades dependiendo del tipo de codificación.

Bajo el estándar americano, la tecnología que se encuentra dentro de esta fase es la denominada CDMA IS95B.

Sistemas de Tercera Generación – 3G

La Tercera Generación es un concepto que actualmente se identifican con las siglas IMT-2000 (International Mobile Telecommunications 2000). Desde el punto de vista del Núcleo de Red, las tecnologías de 3G se agrupan en dos grandes bloques. Uno de ellos es el constituido por aquellas soluciones basadas en la evolución desde el núcleo de red GSM/MAP utilizado por las redes GSM. El otro por las que evolucionan desde la solución ANSI41, adoptada por los sistemas TIA/EIA-136 e IS95 de Segunda Generación (2G). Alguna de las principales diferencias entre ambas son:

- La separación entre terminal e identidad del cliente GSM, lo que no ocurre en ANSI41.

- Los algoritmos de autenticación. ANSI41 utiliza el denominado CAVE (Cellular Authentication and Voice Encryption), frente a los A3/A8 del GSM, que residen en la SIMCARD.
- El uso en GSM del sistema de señalización No. 7 por canal común para la comunicación entre las bases de datos. ANSI41, en cambio, permite tanto esta solución como el protocolo X.25.

En la evolución de las actuales redes móviles, como es GSM, se irán introduciendo mejoras tales como WAP (acceso a contenidos de Internet adaptados para el móvil), GPRS (mayor velocidad de acceso y conmutación de paquetes), EDGE, etc., que harán necesaria la adaptación de las redes con la introducción de nuevos elementos de red.

Básicamente, cuando se habla de 3G se refiere a los sistemas de EDGE, UMTS (por el lado GSM) y los sistemas CDMA 1XRTT, 3XRTT EVDO y EVDV (por el lado CDMA).

Sistemas de Cuarta Generación – 4G

Los sistemas 4G proporcionan roaming a través de diferentes tipos de redes, como puede ser una red de satélite, una WLAN (Wireless LAN) ó una red celular, algo que no esta al alcance de 3G, y esta capacidad permite que se pueda acceder a diferentes servicios con un único equipo y una única factura, al mismo tiempo que se mejora la cobertura y la fiabilidad del acceso a la red y se consiguen velocidades de hasta 100Mbps.

La Cuarta Generación que tiene características claramente superiores a 3G podrían desplegarse aproximadamente en los próximos 05 años.

2.2 Arquitectura de la Red GSM

A partir de este capitulo hacia delante, nos concentraremos específicamente a desarrollar la arquitectura de los núcleos de red GSM/MAP utilizado en las redes GSM/GPRS/EDGE.

Subsistemas

Puede definirse un subsistema como una entidad constituida por uno ó más equipos físicos encargados de ejecutar una tarea específica. La unión de todas estas tareas

asegura el funcionamiento de la red. En la red GSM se distinguen los siguientes subsistemas(12):

- Subsistema de Estaciones Base, BSS (Base Station System)
- Subsistema de Conmutación y Gestión, SMSS (Switching and Maintenance Subsystem)
- Subsistema de Operación y Mantenimiento, OMSS (Operation and Maintenance Subsystem)

Cada subsistema está formado por una ó varias entidades funcionales que se intercomunican a través de diferentes interfases mediante protocolos de señalización específicos. Las interfaces se designan por letras. Fuera de lo que es estrictamente la red, está el conjunto de unidades móviles MS que al no tener relación mutua no forman un subsistema, pero sí tienen una entidad común. La relación entre este conjunto y la red se realiza a través de la "interfase aire" (air interface) llamado también interfase radio, que se designa abreviadamente por la "interfase Um".

El BSS se relaciona con el SMSS a través de la denominada "interfase A". En la siguiente figura se muestra una estructura general de los subsistemas de la red GSM (se representan los subsistemas en cajas rectangulares):

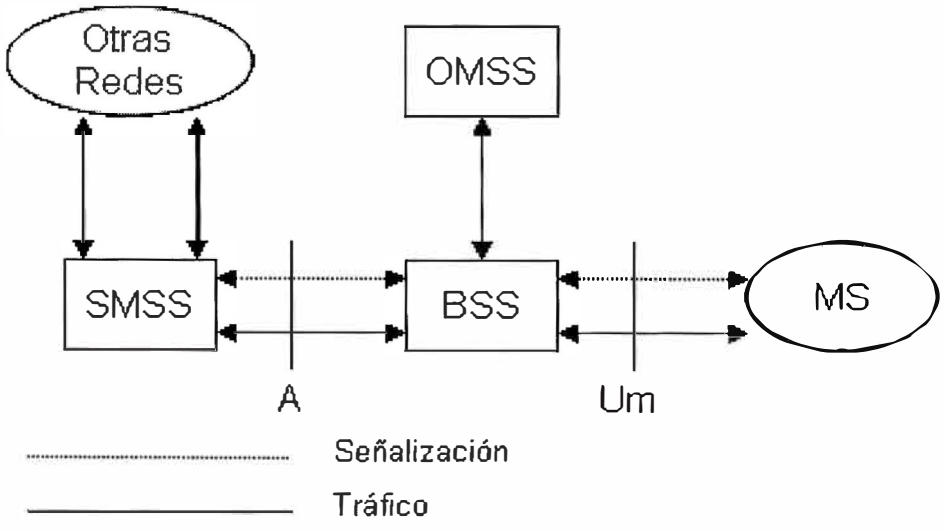


Figura 2.10 Subsistemas en GSM

Subsistema de Estación Base

El subsistema de estación base comprende las funciones de capa física, según el modelo OSI, para interconexión con las MS a través de la interfase Um. Para ello hace uso de un conjunto de canales lógicos. Los canales lógicos son estructuras de datos y protocolos que realizan funciones de intercambio de información para:

- Seguimiento/Localización de las MS y aviso a las mismas
- Establecimiento de las llamadas
- Mantenimiento de las comunicaciones establecidas
- Supervisión y control de la calidad
- Facilidades operativas

En el BSS se identifican dos unidades funcionales:

- Controlador de estación base, BSC (Base Station Controller)
- Estación Transreceptor Base, BTS (Base Transceiver Station)

Donde la interfase entre el BSC y la BTS se denomina "A-bis".

Subsistema de Conmutación y Gestión

El subsistema de conmutación y gestión tiene a su cargo todas las funciones requeridas para manejar los protocolos de señalización necesarios para el establecimiento, mantenimiento y liberación de las llamadas, con la componente específica de la movilidad. Las funciones básicas del SMSS son:

- Localización y registro con autenticación de los abonados
- Enrutamiento de las llamadas
- Administración de los recursos de radio durante la llamada
- Administración de la movilidad
- Intercambio de señalización entre entidades funcionales de la red GSM con redes externas.

El subsistema de conmutación y gestión está constituido por las siguientes unidades funcionales:

- Centro de Conmutación Móvil, MSC (Mobile Switching Center)
- Registro de Ubicación Local, HLR (Home Location Register)
- Registro de Ubicación Visitante, VLR (Visitor Location Register)

Subsistema de Operación y Mantenimiento

El subsistema de operación y mantenimiento tiene a su cargo las funciones de gestión de red, características de las redes de telecomunicaciones y los aspectos relativos a la seguridad del acceso a la red y de las comunicaciones para los usuarios y los equipos.

La primera aplicación se realiza mediante el centro de operaciones y mantenimiento (Operations and Maintenance Center). Para la segunda hay dos unidades funcionales:

- Centro de Autenticación, AuC (Authentication Center)
- Registro de Identidad de Abonados, EIR (Equipment Identity Register)

2.2.1 Arquitectura Funcional de la Red GSM

La arquitectura funcional de una red GSM esta compuesto por diferentes entidades funcionales, pertenecientes a los subsistemas descritos anteriormente, con las interfaces e interconexiones lógicas que las separan. En la siguiente figura se representa la arquitectura denominada también modelo de referencia de GSM.

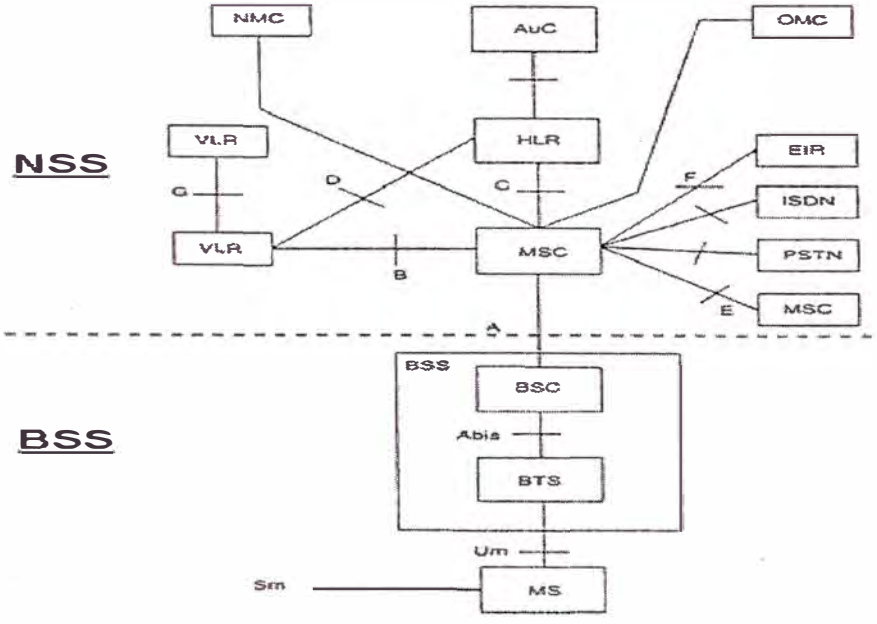


Figura 2.11 Arquitectura Funcional de una Red GSM

Una unidad funcional puede corresponder a un equipo físico concreto ó alternativamente, un mismo equipo físico puede comprender dos unidades funcionales, en cuyo caso la interfase entre ellas es interna al equipo.

A continuación se describen las diferentes unidades funcionales.

Estación Móvil

La estación móvil, MS (Mobile Station), es el equipo físico utilizado por el usuario GSM para acceder a los servicios proporcionados por la red a través de la interfase Um. Se ha especificado esta interfase de forma que las tecnologías de MS y de red GSM puedan evolucionar por separado, sin tener alguna restricción entre ellos.

Como equipo, la MS proporciona la plataforma física para el acceso, pero es "anónima" y no puede funcionar con la red hasta que sea "personalizada" mediante la inserción de una "tarjeta inteligente" (smart card) denominada módulo de identidad de abonado, SIM (Subscriber Identity Module) donde figura, entre numerosas informaciones, la identidad del abonado, IMSI (International Mobile Subscriber Identity) que equivale a la "línea virtual" que conecta al usuario con la red.

En GSM se considera por separado al usuario y a los terminales, lo que acrecienta la movilidad personal. Por ejemplo, un usuario que viaja fuera de su lugar de residencia no necesita llevarse el terminal. Puede alquilar uno en el lugar de destino y personalizarlo con su tarjeta SIM. En cuanto se inserta la tarjeta en cualquier MS homologada, ésta queda preparada para efectuar / recibir llamadas y acceder a los servicios inscritos.

La MS desempeña las siguientes funciones básicas:

- Proporcionar una interfase de comunicaciones entre los usuarios y la red vía radio.
- Realizar la transmisión / recepción de las informaciones de usuario y de señalización a través de la interfase radio.
- Efectuar la inicialización de la conexión con la red.
- Realizar la sintonización de frecuencias y seguimiento automático de las estaciones base en cuya zona de cobertura se encuentre.

- Efectuar funciones de procesamiento de la voz: conversión analógico / digital y viceversa.
- Realizar la adaptación de interfases y velocidades para las señales de datos.

Subsistema de Estaciones Base

El BSS comprende el conjunto de equipos utilizados para proporcionar cobertura radioeléctrica en el área celular. Se divide en dos partes: las estaciones transceptoras de base BTS y los controladores de esas estaciones, BSC.

Las BTS están constituidas por los equipos transmisores – receptores de radio (transceptores), los elementos de conexión al sistema radiante (combinadores, multiacopladores, cables coaxiales), las antenas y las instalaciones accesorias (torres soporte, pararrayos, tomas de tierra, etc.).

Debido al elevado número de BTS de una red y debido a que éstas funcionan en lugares donde no hay mantenimiento "in situ", los equipos de BTS deben ser sencillos, fiables, duraderos y de costo moderado. Por ello, la mayoría de las funciones de control se realizan en el BSC. El BSC se encarga de la gestión de varias BTS en lo relativo a los recursos de radio: asignación, utilización y liberación de las frecuencias, traspasos, funcionamiento con saltos de frecuencia, etc. También puede realizar ciertas funciones de conmutación. Las interfaces del BSC con las BTS y con la red, son la A-bis y la A, respectivamente. El BSS desempeña las siguientes funciones:

- Transmisión / recepción radioeléctrica a través de la interfase Um.
- Localización de las MS para su registro inicial ó actualización.
- Establecimiento, supervisión y conclusión de las llamadas.
- Traspaso entre BTS controladas por el mismo BSS.
- Procesado de voz y adaptación de velocidad.
- Control de equipos y funciones de re-configuración.
- Control de mantenimiento rutinario.

En la siguiente figura se representa esquemáticamente un BSS formado por un BSC y dos BTS, cada una de las cuales tiene varios transceptores radio TRX con ciertas funciones de control. Se han indicado también las interfaces A-bis y A.

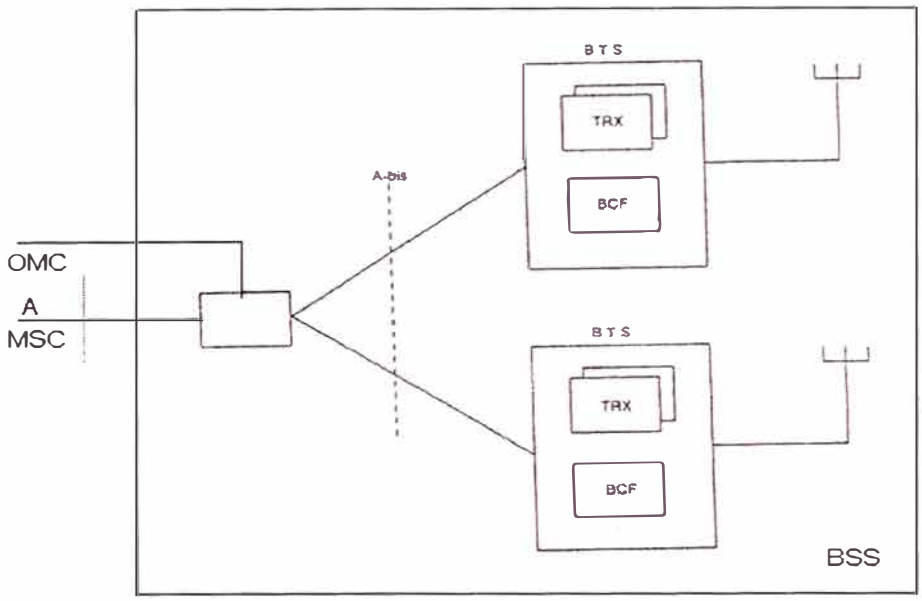


Figura 2.12 Subsistema de Estaciones Base

Componentes del Subsistema de Conmutación y Gestión

En la siguiente figura podemos ver los componentes principales del subsistema de conmutación. Esta muestra los flujos de información entre los diferentes elementos: con línea continua la transmisión de voz ó datos y con línea discontinua la señalización. En está gráfica no se ha representado ninguna conexión con redes externas.

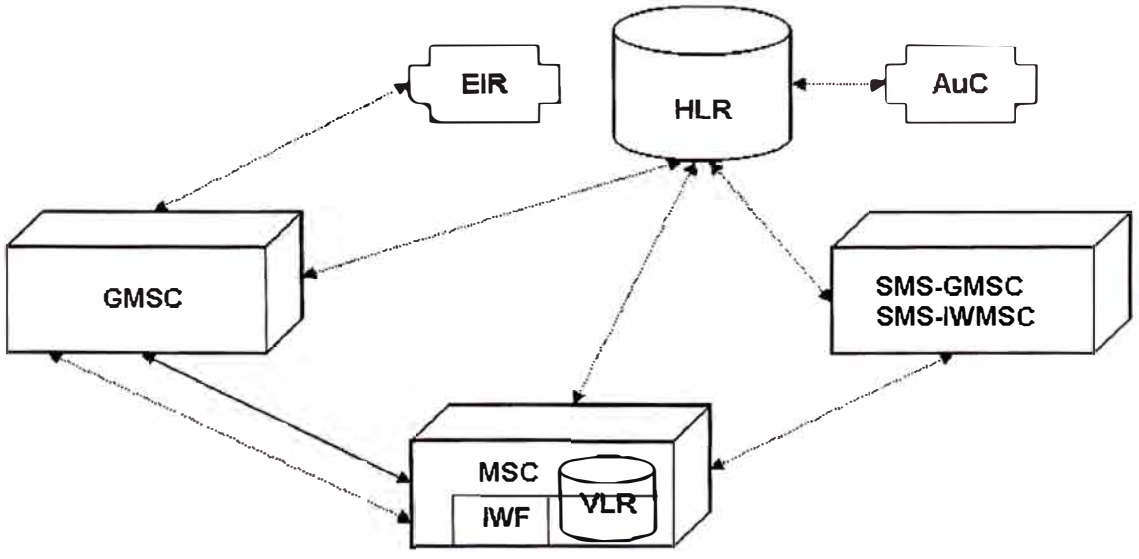


Figura 2.13 Subsistema de Conmutación

A. MSC/VLR

Ambos son imprescindibles para la existencia de la red GSM. Aunque funcionalmente son diferentes, se les suele tratar conjuntamente ya que están íntimamente relacionados. El MSC (Mobile Switching Center) es el nodo que contiene las funciones de conmutación y señalización básicas, es decir, su principal misión consiste en la gestión completa (establecimiento, encaminamiento, control y finalización) de las llamadas desde y hacia usuarios GSM.

El VLR (Visitor Location Register) es una base de datos en la que se guarda información temporal de cada cliente que se encuentra en el área de influencia de los MSC a los que está asociado (las especificaciones GSM permiten que un VLR esté asociado a un único MSC ó a varios). El VLR intercambia información frecuentemente con el HLR. Para el VLR, todos los clientes bajo su área de influencia son visitantes. El tipo de información que guarda de cada uno de ellos es variada: desde datos de identificación del usuario como el IMSI o el TMSI, datos que permiten el encaminamiento de llamadas como el MSRN, servicios provisionados, datos relativos a la seguridad como la autenticación, etc.

Suponiendo que el VLR y el MSC estuvieran físicamente localizados en nodos diferentes, el intercambio de señalización entre ambos para cada llamada sería muy elevado, debido a ello, normalmente se fabrica en un solo nodo MSC / VLR las dos entidades funcionales, los cuales interaccionan usando protocolos propietarios, que normalmente son una variante del protocolo MAP. Otra funcionalidad del MSC, es la realización de traspasos entre dos BSC que estén conectado a él ó a otro MSC. Para ello, el MSC tiene una parte exclusivamente dedicada a este propósito, que se denomina aplicación de control de traspasos, HOCA (HandOver Control Application). El MSC también proporciona el control de la autenticación y de la actualización de posición de los móviles, la prestación de servicios suplementarios y la tarifación de las llamadas.

El MSC constituye la interfase entre el sistema radio y la red fija. Por lo tanto, una de las fronteras del MSC es siempre el subsistema BSS, en forma de uno ó varios BSC,

dependiendo del número de los mismos, de la tecnología y estrategia elegidas por el operador. El resto de las fronteras pueden ser otros nodos internos ó externos a la red GSM. La cobertura de un MSC puede ser muy diversa y se denomina área del MSC. Un área de MSC puede estar formada por una o varias áreas de localización LA (Location Area).

B. HLR – Home Location Register

El HLR es una base de datos inteligente en la que se guarda información estática relativa al servicio de todos los clientes de la red GSM y también información dinámica relativa a los mismos, como el VLR en el que se encuentran. Para dar de alta a un nuevo usuario en la red, es necesario introducir un registro con sus datos en el HLR.

Conceptualmente, existe un único HLR por red GSM. Sin embargo, en la práctica, puede estar distribuido dependiendo de la cantidad de clientes de la red, de la capacidad de los nodos ó bien por razones de seguridad. Otra opción es disponer de HLR redundantes (Mated Pair) como medida de precaución. Entre los datos que guarda el HLR, se encuentran el MSC y VLR que están sirviendo al abonado, los servicios contratados por el usuario y datos adicionales como el número C en el caso de desvío de llamada y la autenticación.

Los nodos con los que el HLR se comunica directamente a través de los enlaces de señalización son los VLR (por ejemplo, para actualizar la posición del móvil), el AuC para hacer la autenticación, y el GMSC, por el cual se intercambian números de encaminamiento MSRN, necesarios para dirigir la llamada al MSC apropiado.

En la siguiente figura se muestran todas las interfaces del HLR y el tipo de información que intercambia con cada una de ellas.

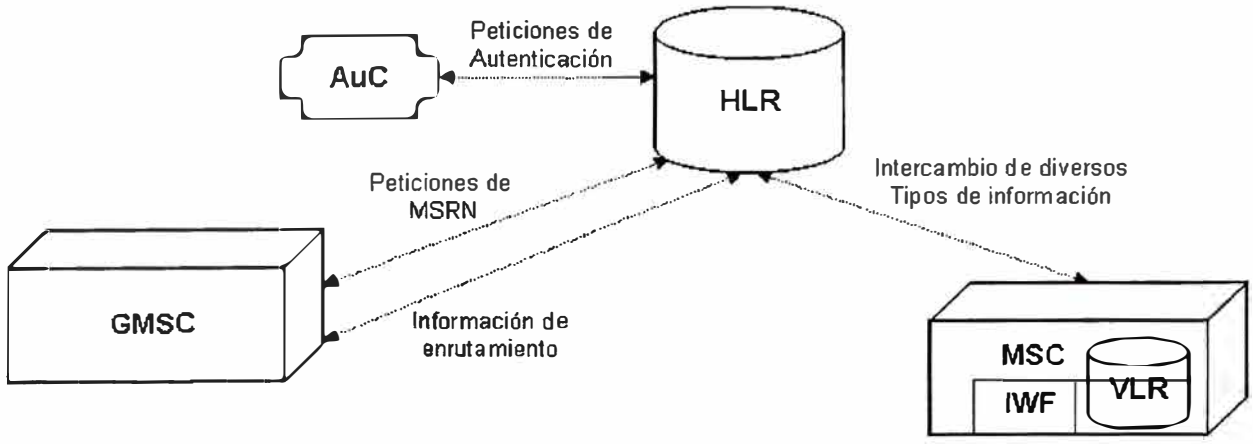


Figura 2.14 Flujo de Información al HLR

C. GMSC

El GMSC (Gateway Mobile Switching Center) es un nodo que permite interrogar al HLR para obtener información de encaminamiento para una llamada dirigida a un móvil. Por tanto, entre sus funciones está la de ser el nexo de unión de la red GSM con otras redes externas.

Quizás el nombre no es muy adecuado, ya que hace pensar en que debe tener VLR ó subsistema BSS asociado, cuando no es necesario, pues estas funciones pueden ser realizadas por un nodo dedicado exclusivamente a la conmutación. En consecuencia, es imprescindible que pueda interrogar al HLR.

Cuando a la red GSM llega una llamada (desde el exterior ó generada en la propia red) hacia un móvil cuya localización no se conoce, dicha llamada se encamina hacia un GMSC, que será el encargado de interrogar al HLR para obtener de él la información de encaminamiento necesaria y luego enviar la llamada hacia el MSC correcto.

El número de GMSC que puede haber en una red GSM puede ser variable, lo más común, es que todos los MSC sean GMSC. De esta manera podrán interrogar al HLR para saber cómo encaminar una llamada que les llega desde un móvil que se encuentra en su área de influencia, sin necesidad de dirigirla a otro nodo para que obtenga esta información. Por esta razón, muchas veces existe ambigüedad entre los términos MSC y GMSC.

En la siguiente figura se esquematiza el proceso de obtención de información de enrutamiento:

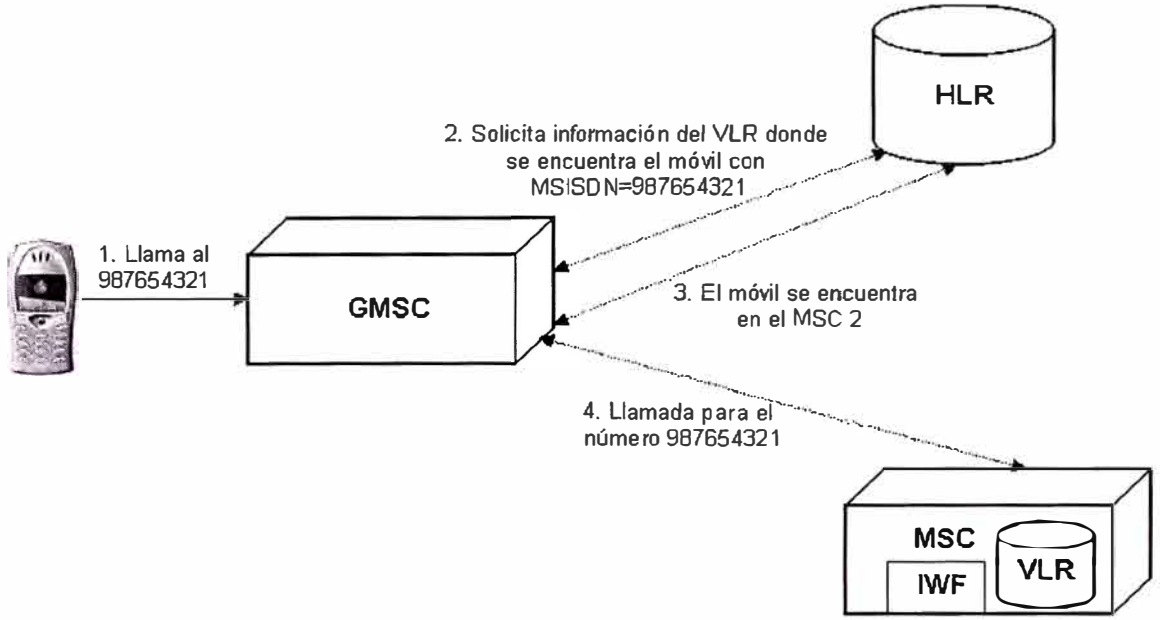


Figura 2.15 Flujo de Obtención de Información de enrutamiento

D. AuC

El centro de autenticación de la red GSM, AuC (Authentication Center), es una base de datos que se podría considerar conceptualmente como parte del HLR. Sin embargo, en la práctica, puede encontrarse tanto como un nodo aislado como integrado con el HLR. Las especificaciones GSM tratan de separar el concepto de AuC del de HLR, lo que va encaminado a dar más importancia a la seguridad, tema clave en redes móviles, en las que la interfase radio constituye un gran riesgo.

Cuando se da de alta a un nuevo cliente en la red, se le proporciona junto a su IMSI una clave de autenticación Ki. La pareja IMSI-Ki, quedará almacenada en la SIM por un lado y en el AuC por otro. El AuC producirá un número aleatorio RAND que junto con el Ki, se harán pasar por dos algoritmos diferentes, A3 y A8, para obtener la respuesta firmada SRES (Signed Response) y la clave de cifrado Kc. Así, el AuC obtiene las llamadas tripletas de autenticación (RAND, SRES, Kc) que enviará al HLR en el caso que este requiera.

Es importante señalar que la clave Ki nunca se transmite a través de la red. La siguiente figura muestra el contenido del AuC y el proceso de petición de las tripletas por parte del HLR.

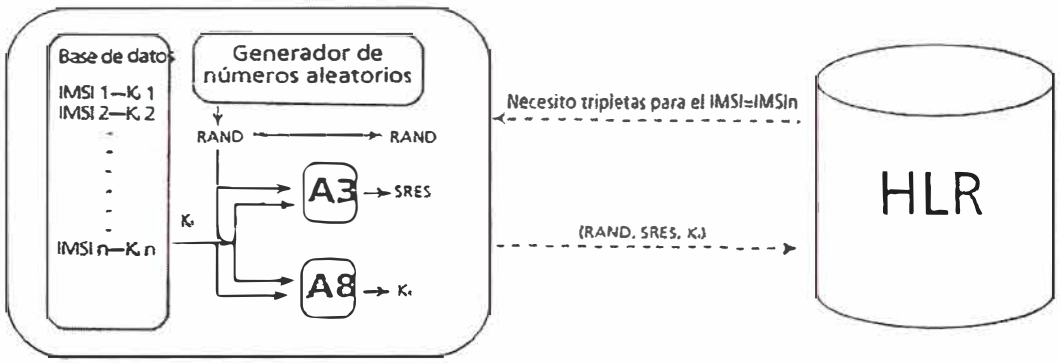


Figura 2.16 Flujo de Autenticación

E. EIR

El EIR (Equipment Identity Register) es el registro de identificación de equipos terminales. Su función consiste en evitar que se utilicen equipos móviles que no están autorizados en la red, por ejemplo, porque han sido robados ó porque pueden producir perturbaciones a la misma.

Para la comprobación se utiliza el IMEI ó identificación internacional del equipo móvil. El EIR es básicamente una base de datos que clasifica los IMEI en tres listas:

- Blanca: no tiene ninguna restricción.
- Negra: se les impide el acceso a la red.
- Gris: degradan la calidad de la red, pero no lo bastante como para impedir que sean utilizados.

El EIR va conectado directamente sólo a los MSC y GMSC. Su implementación física consiste en una base de datos con un software de comunicaciones para establecer el diálogo con el MSC y/o GMSC. Puede encontrarse como nodo aislado, pero también integrado con otros nodos GSM, como el HLR y el AuC.

F. IWF

El IWF (InterWorking Function) es una entidad funcional asociada al MSC. Proporciona los medios necesarios para interactuar la red GSM con las redes externas fijas (PSTN, ISDN y redes de paquetes PDN).

Sus funciones dependerán de los servicios y del tipo de red fija a la que se conecte. Puede que en algunas ocasiones, no aporte ninguna funcionalidad en el caso que ambas redes son compatibles.

G. VMS

Es el nodo que permite proporcionar el servicio de buzón de voz, VMS (Voice Mail System). El VMS lleva asociado en algunos casos un centro de mensajes cortos, el cuál es utilizado para avisar a los usuarios cuando tienen mensajes en sus casillas de voz. En otras ocasiones, el SMSC encargado de esta actividad es el mismo que el que proporciona los servicios MOSMS y MTSMS.

H. SMSC - Centro de Mensajes Cortos

El SMSC es un nodo interno ó externo a la red GSM, que debe ser capaz de enviar y recibir mensajes cortos (SM – short message) hacia y desde móviles. También debe ser capaz de intercambiar mensajes de confirmación de la recepción ó envío de los SM con la red GSM. No necesariamente, cuando el SMSC reciba un mensaje para un determinado móvil, éste será enviado inmediatamente, pues es posible que el móvil se encuentre apagado. En ese caso, deberá esperar a que esté encendido para enviárselo.

Si esto sucede, la red notificará al SMSC para que tenga constancia e intente volver a enviárselo más tarde. Para ello, el SMSC suele disponer de una tabla de reintentos, en la que se especifican los intervalos de tiempo entre los que el SMSC debe intentar de nuevo el envío. Un SMSC puede estar conectado a uno ó varios MSC.

I. SMS-GMSC

Es el nodo que realiza las funciones de gateway para el servicio MT-SMS, es decir, sólo interviene cuando hay un SM dirigido a un móvil. Físicamente, puede ser un MSC cualquiera.

Cuando el SMS-GMSC recibe un SM desde el SMSC, comprueba que todos los parámetros son correctos e interroga al HLR para que le envíe la información de encaminamiento que necesita para entregar el SM. Con esta información, el SMS-GMSC envía el SM al MSC correspondiente, quien finalmente intentará entregar el mensaje al móvil.

El SMS-GMSC informará al HLR del resultado de la entrega, tanto si ha sido satisfactoria ó no. En este último caso, deberá indicar la causa por la que no se ha podido entregar el mensaje al HLR, así éste informará al SMSC para que utilice la tabla de reintentos.

J. SMS-IWMSC

Es el nodo que realiza las tareas de enrutamiento en el escenario de MOSMS, es decir, sólo interviene cuando hay un SM originado por un móvil.

Cuando un móvil genera un SM, el MSC recibe dicho SM desde el móvil y pide a su VLR asociado información para poder continuar la operación de entrega del SM. Cuando recibe la confirmación por parte del VLR de que todo es correcto, entonces entrega el SM al SMS-IWMSC.

El SMS-IWMSC recibe el SM y establece una comunicación con el SMSC correspondiente para entregárselo. Una vez que el SMSC recibe el SM, responderá al SMS-IWMSC indicándole el estado final del mensaje, es decir, si es satisfactorio ó si se ha producido algún error. El SMS-IWMSC deberá remitir esta información al MSC donde está el móvil que ha originado el SM.

En el caso de que pase el intervalo de tiempo estipulado por el operador, sin que el SMS-IWMSC reciba respuesta del SMSC, éste informará al MSC de que ha habido algún error, ya que no ha recibido confirmación del SMSC.

El SMS-IWMSC tiene otra función, que consiste en avisar al SMSC de que un móvil para el que tiene guardado un SM, ya está disponible para recibir el mensaje. Cuando el móvil entra en actividad, el HLR es notificado y avisa al SMS-IWMSC para que le comunique al SMSC que ya puede enviar el SM al móvil. El HLR avisa al SMS-IWMSC sólo cuando sabe que dicho móvil tiene mensajes cortos por entregar. Esto lo sabe a través de unos indicadores de espera de mensajes, MWI (Message Waiting Indication), entre los que están las direcciones de los SMSC que tienen mensajes hacia ese móvil.

2.2.2 Interfases de la Red GSM

En la siguiente figura se representan todas las interfaces de una red GSM:

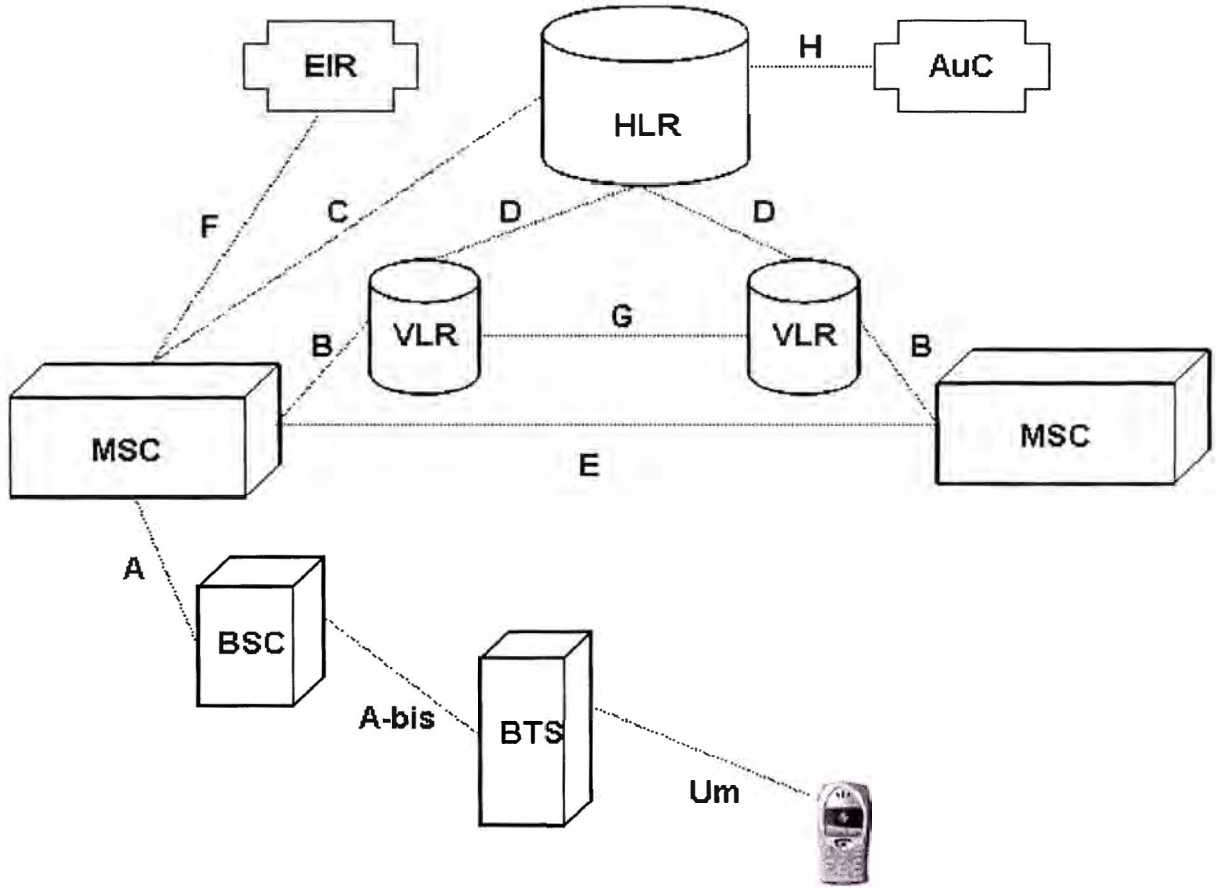


Figura 2.17 Interfases de la Red GSM

Interfase A (MSC-BSC)

Esta interfase se utiliza para intercambiar información sobre la gestión del subsistema BSS de las llamadas y de la movilidad de los móviles. Por ejemplo, a través de esta interfase se negocian los circuitos a utilizar entre el BSS y el MSC.

Interfase A-bis (BSC-BTS)

Es la interfase entre la estación base y el BSC. Permite el control del equipo de radio.

Interfase B (VLR y MSC asociados)

El VLR es la base de datos que contiene toda la información que permite dar el servicio a los clientes que se encuentran en el área de influencia de sus MSC asociados. Por tanto, cuando un MSC necesite cualquier información sobre un móvil acudirá a su VLR y de la misma manera, le informará debidamente cuando tenga que hacerlo, por ejemplo, al recibir por parte de un móvil una petición de actualización de posición.

En algunos casos, cuando el móvil requiera un servicio especial ó cambiar los datos suscritos con el operador, el MSC informará al HLR (siempre vía el VLR). Debido a que en esta interfase se intercambian muchos mensajes de señalización, se recomendó que esta interfase no sea externa. Ésta es la razón por la que prácticamente todos los fabricantes tienen nodos MSC / VLR integrados.

Interfase C (HLR-GMSC)

Es la interfase utilizada por los GMSC cuando necesitan interrogar al HLR para obtener el número de roaming - MSRN del móvil llamado y poder así enrutar la llamada hacia el MSC destino. No debe confundirse con la interfase D, ya que el GMSC no tiene porqué tener VLR, puede ser perfectamente un nodo que sólo haga un enrutamiento de las llamadas.

Interfase D (HLR-VLR)

Es la interfase existente entre el HLR y el VLR. Principalmente sirve para intercambiar información entre ambas bases de datos, relativas a la posición del móvil y a la gestión del servicio contratado por el cliente.

Por ejemplo, cuando un móvil entra en el área de influencia de un VLR, éste envía una notificación al HLR. El HLR también se encarga de avisar al VLR anterior de que cancele el registro de posición del móvil, pues éste ya se encuentra en otro VLR.

También se utiliza esta interfase para intercambiar información cuando el móvil requiere un servicio especial, cuando el cliente desea cambiar datos suscritos, cuando deben cambiarse datos de la misma por motivos administrativos, para el intercambio de tripletas de autenticación, etc.

Interfase E (MSC-MSC)

Esta interfase la utilizan los MSC para intercambiar la información necesaria para iniciar y realizar una transferencia a otro MSC, con objeto de que la comunicación continúe cuando el móvil cambia de área de influencia de un MSC a otro.

Interfase F (MSC-EIR)

Se utiliza cuando el MSC quiere comprobar el IMEI de un equipo.

Interfase G (VLR-VLR)

Se utiliza en el caso de que un móvil inicie la petición de actualización en un nuevo VLR.

Interfase H (HLR-AuC)

Es la interfase utilizada por el HLR para solicitar tripletas al AuC, cuando no dispone de ellas. El protocolo utilizado para la transferencia de estos datos, no es estándar. Muchas veces se encuentran nodos HLR / AuC integrados.

Interfase Um (BSS-Móvil)

Es la interfase radio, que se encuentra entre el móvil y el BSS.

2.2.3 Numeración en la Red GSM

A continuación se describen los diferentes números y direcciones que son utilizados en una red GSM.

Identificación de usuarios móviles: IMSI, TMSI, LMSI

El IMSI (International Mobile Subscriber Identity) es la identidad internacional del usuario móvil y por tanto es único para cada abonado en todo el mundo. Para asegurar la privacidad del IMSI y evitar que esté viajando continuamente en la interfase radio, el VLR asigna un número temporal TMSI (Temporary Mobile Subscriber Identity) a cada uno de sus visitantes.

De forma opcional y para acelerar la búsqueda de los datos de un cliente en el VLR se define el LMSI (Local Mobile Station Identity). El LMSI es asignado por el VLR en el procedimiento de actualización de posición y es enviado al HLR junto con el IMSI. Aunque el HLR no lo utiliza, en caso de que disponga de él, lo envía siempre junto al IMSI en todos los mensajes referentes a dicho móvil hacia el VLR para facilitarle la búsqueda dentro de su base de datos.

A. IMSI

La estructura del IMSI es la que se muestra en la siguiente figura. Todos los caracteres deben ser numéricos y en ningún caso se excede los 15 dígitos.

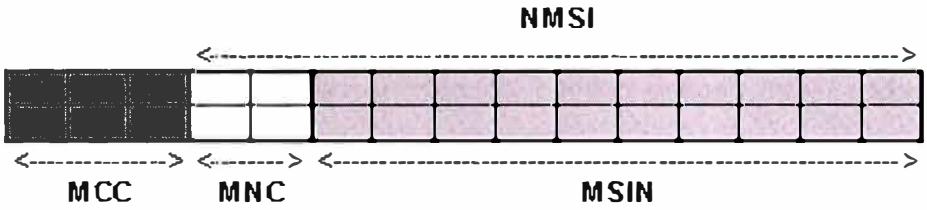


Figura 2.18 Estructura del IMSI

Tal como se observa esta formado por tres partes:

- MCC (Mobile Country Code), que consta de tres dígitos e identifica unívocamente el país donde está domiciliado el cliente móvil. Para Perú el MCC es el 716.
- MNC (Mobile Network Code), que tiene dos dígitos e identifica dentro de un país, la red GSM a la que pertenece el usuario. La asignación de los MNC dentro de un país la realiza la administración de ese país. Si en un mismo país hay más de una red GSM, a cada una se le asignará un MNC único. Para el caso de TIM Perú el MNC=10.
- MSIN (Mobile Subscriber Identification Number), identifica al abonado en cuestión dentro de su red GSM. Así como el MCC y el MNC están completamente prefijados por administraciones y organismos, el MSIN no lo está y lo asigna cada operador. Es recomendable en aquellas redes en las que exista más de un HLR físico, que los primeros dígitos del MSIN hagan referencia al HLR en el que está dado de alta el IMSI.

Adicionalmente se define el NMSI (National Mobile Subscriber Identity) como el conjunto del MNC y el MSIN. Con la estructura definida, bastará que un nodo determinado analice el conjunto MCC+MNC para saber a qué red GSM pertenece el móvil.

B. TMSI

Debido a que el TMSI sólo tiene significado dentro del VLR y en su zona de influencia, no hay regulación establecida sobre el mismo, sino que deberán ser el operador y el suministrador los que lleguen a un acuerdo sobre este mismo.

La longitud del TMSI es de 4 octetos (1 octeto = 8 bits), que se pueden expresar en forma hexadecimal. Para asegurarnos de que al producirse un reinicio en un VLR, no se duplican sus TMSI, una parte de los mismos debe incluir información que señale de alguna forma que se ha producido un reinicio. La red deberá evitar mandar TMSI que sean 31 bits a "1", puesto que esto significaría que no hay TMSI disponible en ese momento.

C. LMSI

Puesto que es número interno del VLR, lo único que hay regulado sobre él es que debe tener una longitud de 4 octetos. Este es un número que asigna el VLR al móvil en el proceso de actualización de posición, con objeto de acelerar el proceso de búsqueda en dicho VLR.

2.2.3.1 Plan de Numeración Móvil

Cada operador realizará el plan de numeración para las redes móviles de su país. En principio, cualquier usuario de PSTN ó de ISDN deberá poder comunicarse con un móvil, por lo que los números de teléfono de los móviles deberán cumplir el plan de numeración de ISDN de cada país. Es importante que pueda cambiarse el IMSI sin necesidad de cambiar el número ISDN y viceversa. A cada usuario móvil se le podrá asignar uno o varios números ISDN.

A. MSISDN

Es el número ISDN internacional de la estación móvil, MSISDN (Mobile Station International ISDN Number), identifica de forma única al abonado móvil dentro del plan de numeración de la red telefónica pública. Su estructura es la que se muestra en la siguiente figura:

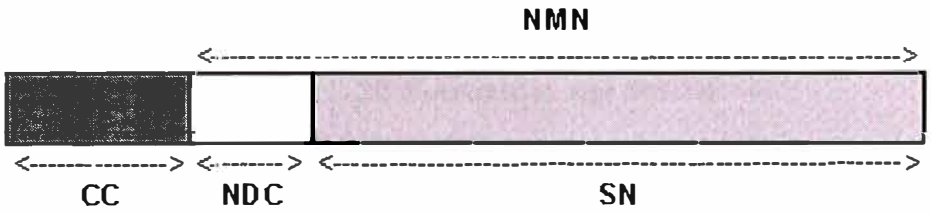


Figura 2.19 Estructura del MSISDN

Tiene tres partes principales:

- CC (Country Code), es el código del país en el que se ha registrado el móvil.
- NDC (National Destination Code), es el código que dentro de un país se asigna a cada red GSM. En determinados países cada red GSM puede tener asignados más de un NDC.
- SN (Subscriber Number), son los dígitos que identifican al usuario.

Adicionalmente se define, el NMN (National Mobile Number), como NDC+SN. La longitud global del MSISDN dependerá de cómo sea el plan de numeración de cada operador. El MSISDN debe ser un número tal que pueda ser utilizado como una dirección global de enrutamiento para dirigir mensajes al HLR de la estación móvil. Está información la proporcionan el CC y el NDC. Si se necesitase información adicional, por ejemplo, para saber a qué HLR pertenece dentro de una red GSM que lo tuviera distribuido, ésta deberá estar incluida en los primeros dígitos del SN.

B. MSRN

Es el número de roaming, el MSRN (Mobile Station Roaming Number) sirve para que el GMSC pueda encaminar una llamada terminada en móvil al MSC correcto. El proceso es el siguiente: cuando una llamada llega al GMSC, éste interroga al HLR para saber donde está el móvil llamado y le pasa como parámetro el MSISDN de dicho móvil. El HLR busca

en su base de datos el VLR en que se encuentra el móvil en cuestión y le pide que le envíe un MSRN para dicho móvil. Una vez que el VLR le ha enviado el MSRN al HLR, éste se lo remite al GMSC.

Figura 2.20 Estructura del MSRN

El MSRN tiene la misma estructura que el MSISDN, sólo que ahora el SN en vez de hacer referencia a un usuario, la hace a un MSC, es decir:

- El CC debe ser el del país en que se encuentre el VLR que proporciona el MSRN.
- El NDC de la red GSM a la que pertenece el VLR.
- Un SN con la estructura acorde a esa área de numeración.

Debe evitarse utilizar el MSRN como número de marcación, reservando cuidadosamente para ellos un rango de numeración. Debe hacerse notar que en determinados casos un MSISDN y un MSRN podrían ser idénticos. Para evitar errores, por ejemplo, que el GMSC encaminase basándose en un MSISDN erróneo que ha marcado un cliente y que es igual a un MSRN, deben utilizarse indicadores de encaminamiento en los nodos de conmutación.

2.2.4 Base de Datos Móviles

En una red GSM, es imprescindible la existencia de bases de datos que guarden los parámetros de cada móvil que hacen posible la gestión de la movilidad, de las llamadas, de la tarifación y de la seguridad, entre otras funciones.

Deben distinguirse dos tipos de bases de datos: por un lado tenemos la SIM, que reside en la parte del móvil y por otro, el resto de las bases de datos del sistema que se encuentran en la red. Dentro de estas últimas, las principales son el VLR y el HLR, que deben mantener la consistencia de los datos entre sí. Pero además existen otras, como el AuC y el EIR, que también guardan algunos parámetros del cliente y están enfocadas a

funciones más específicas, como son las relacionadas con la seguridad de los usuarios y de la red.

2.2.4.1 SIM – Subscriber Identity Module

La SIM (Modulo de Identidad de Usuario) es más que una base de datos, es una especie de computadora que se encuentra integrada en una tarjeta. La información se estructura en archivos y es posible establecer una comunicación con la SIM mediante comandos.

Dentro de toda la información que es capaz de guardar la SIM: administrativa, de operación, etc., debe tenerse en cuenta que la SIM guarda otros tipos de información, entre los cuales, los algoritmos de autenticación y de obtención de Kc.

La obtención de esta tarjeta puede ser personalizada por el usuario, es decir, cada persona puede tener archivos adicionales propios. Esto depende, por ejemplo de determinados servicios que se hayan contratado. En algunos casos, también existe la posibilidad de introducir pequeños programas que entienda la SIM. Esto se realiza mediante la herramienta SIM Toolkit, que abre un nuevo rango de posibilidades al ofrecer nuevos servicios desde la propia SIM.

2.2.4.2 VLR – HLR

Dentro de los datos que se guardan aquí, podemos distinguir aquellos que son permanentes como el número de teléfono (MSISDN) y que sólo los puede cambiar el operador de la red y otros que van variando como puede ser el parámetro del HLR que indica el VLR en que se encuentra un móvil.

El HLR contiene todos los datos permanentes de todos los clientes de su red GSM. También contiene datos temporales que se necesiten para el correcto funcionamiento de la red (por ejemplo el MSC y el VLR en que se encuentra el móvil en cada momento). Sin embargo, no contiene ningún tipo de información de usuarios que estén visitando su red GSM, pero que pertenezcan a otra.

El VLR contiene todos los datos de usuarios necesarios para la correcta gestión de las llamadas y otros procesos. Sólo contiene información de aquellos usuarios que se

encuentran bajo su área de influencia, aunque sean clientes de otras redes GSM, que se encuentran de visita en la suya.

2.2.5 Sistema de Señalización No. 7

En las redes de telecomunicación tanto en la red telefónica básica PSTN como la red digital de servicios integrados ISDN, se utiliza el llamado Sistema de Señalización No 7, SS7 (Signalling System # 7) desarrollado y normalizado por el antiguo Comité Consultivo Internacional Telefónico y Telegráfico (CCITT) que hoy en día es el Sector de Normalización de Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T).

Puede definirse el SS7 como un conjunto de protocolos que rigen la transferencia de información de control por una red de señalización de tipo conmutación de paquetes. El SS7 es una norma abierta, que permite la interoperabilidad de equipos. Los objetivos fundamentales del diseño del SS7 han sido:

- Aplicación a las redes digitales de telecomunicación que utilizan centrales de conmutación.
- Satisfacer las necesidades actuales y futuras de transmisión de información con / sin conmutación de circuitos, para transacciones entre nodos de las redes de comunicación, para el control de las llamadas, acceso a bases de datos de las redes y funciones de gestión y mantenimiento.
- Proporcionar un mecanismo seguro y fiable de intercomunicación en secuencia correcta, sin pérdida ni duplicación de la información entre centros de conmutación ó nodos de una red de telecomunicaciones.

Las características básicas del SS7 son:

- Transferencia de información mediante mensajes construidos con señales digitales.
- Modalidad por canal común, con señalización entre centrales tramo a tramo.
- Funcionamiento a la velocidad normalizada de 64 kbps.

- Modo no asociado, con conmutación de paquetes.

La estructuración en mensajes otorga al sistema una gran flexibilidad y un importante valor añadido. En virtud de la primera, el SS7 ha demostrado su idoneidad para la señalización en la red telefónica convencional, red digital de servicios integrados y, modernamente, en las redes móviles.

El SS7 se ha ido introduciendo en la PSTN a medida que esta red se ha modernizado con la digitalización de la transmisión y la conmutación. Además, para aprovechar las enormes posibilidades del sistema, se ha establecido una red específica, la red de señalización, superpuesta a la de telecomunicación. La red de señalización permite regular la transmisión de información entre usuarios de diferentes categorías de tráfico: telefonía, datos, así como comunicaciones de operación, mantenimiento y gestión de la red de telecomunicaciones. La red de señalización esta constituida por nodos ó puntos de señalización SP, donde están ubicados los servicios – usuarios del sistema y a los que deben acceder los centros de conmutación con sus mensajes de señalización. Los "usuarios" de la red de señalización, son aplicaciones residentes en los nodos que ejecutan funciones de control de las llamadas y de búsqueda en bases de datos de informaciones relativas a las llamadas.

Los SP proporcionan funciones de red de señalización mediante la transmisión / recepción de mensajes hacia / desde los usuarios del nodo a través de los enlaces de señalización SL. Pueden ser unidades terminales ubicadas en las centrales de conmutación ó nodos especiales que efectúan el tratamiento y la retransmisión de la señalización, denominándose en ese caso puntos de transferencia de señalización, STP.

Un STP, típicamente, transmite mensajes de un SP a otro. En el STP se analizan los mensajes de señalización recibidos, a fin de presentarlos al canal de salida adecuado, teniendo en cuenta, si procede su prioridad. Existen además SP especiales que proporcionan servicios de bases de datos a varios nodos de conmutación (por ejemplo,

para el tratamiento de llamadas de líneas "0800"), que se denominan punto de control de servicios, SCP (Service Control Point).

2.2.5.1 Arquitectura del SS7

La arquitectura del SS7 se basa en el modelo estratificado de interconexión de sistemas abiertos OSI de 7 capas, con algunas diferencias(10). La estructura de protocolos se ha dividido en dos partes independientes:

A. Parte de Transferencia de Mensajes, MTP (Message Transfer Part)

B. Parte de Usuario, UP (User Part)

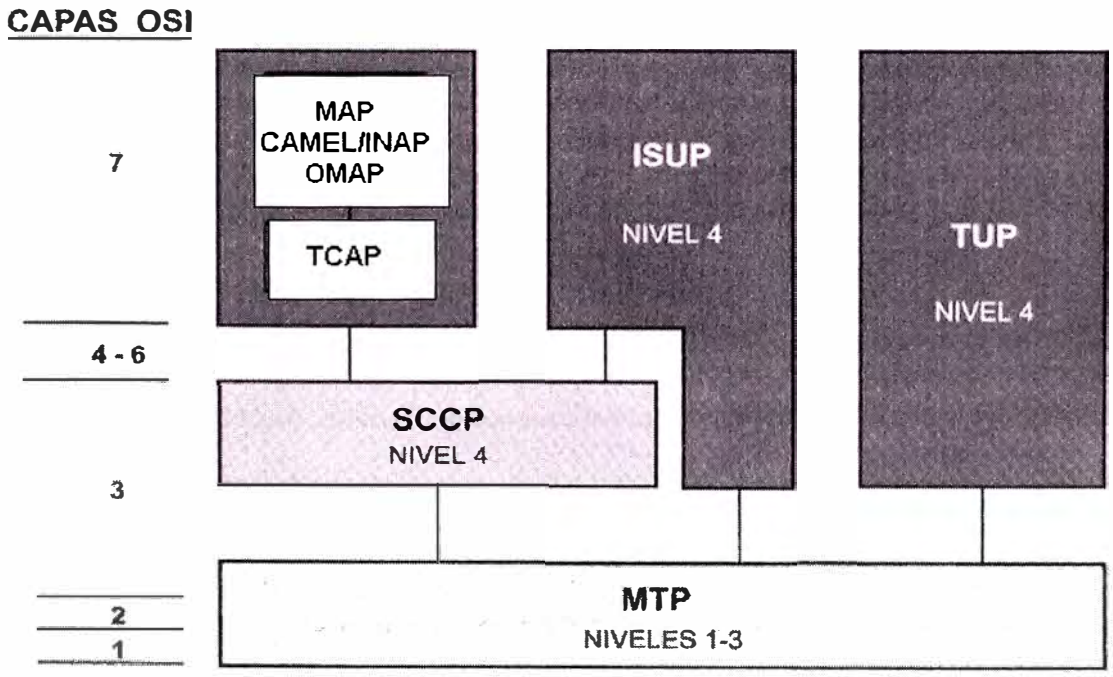


Figura 2.21 Arquitectura del SS7

Parte de Transferencia de Mensajes – MTP (Message Transfer Protocol)

La MTP proporciona un servicio de transferencia de mensajes sin conexión que asegura el transporte y la entrega fiables y sin errores de los mensajes de señalización a través de la red. Incluye, en consecuencia, métodos para contrarrestar posibles fallos. Se divide, a su vez, en tres niveles funcionales:

- **MTP de Capa 1**

Que corresponde con el nivel 1 (capa física) del modelo OSI y proporciona el soporte físico para la transmisión dúplex de información entre puntos de señalización, mediante el

llamado enlace de señalización, SL (Signalling Link). Un SL es un circuito de transmisión bidireccional a 64 kbps entre dos SP, formado por canales de transmisión digital y sus equipos terminales.

- **MTP de Capa 2**

Que corresponde con el nivel de enlace del modelo OSI y define funciones y procedimientos relativos a la transferencia, por un SL, de mensajes denominados "unidades de señalización" entre dos SP. Se utilizan métodos de verificación de mensajes y corrección de errores para asegurar la fiabilidad de los enlaces y una baja tasa de errores en los mensajes. La corrección de errores se basa en la retransmisión de los mensajes detectados como erróneos. Por ello los mensajes se almacenan en un registro hasta que se recibe la confirmación, por parte del receptor, de que el mensaje se ha recibido correctamente.

- **MTP de Capa 3**

Que corresponde parcialmente con la capa 3 (Red) del modelo OSI y se ocupa del mantenimiento del enlace, encaminamiento, discriminación y distribución de los mensajes de señalización, así como de su tratamiento y la gestión de la red de señalización. La función de gestión de red es muy importante y consiste en monitorear constantemente los enlaces de señalización e ir contando los errores que se producen. Cuando el número de errores alcanza un determinado número, este nivel se encarga de poner al enlace en cuestión fuera de servicio y volverlo a sincronizar. De esta forma se resuelven la mayoría de los problemas que por lo general se deben a que el reloj se va degenerando con el tiempo.

Para la gestión de la red, la capa 3 de MTP dispone de las funciones de gestión de enlace, tráfico y ruta. La función de gestión de enlace se centra en cada enlace y utiliza el nivel dos para detectar si hay problemas en el enlace, teniendo capacidad para bloquear un enlace determinado y ordenar al nodo adyacente que haga lo mismo. Esto puede tener un gran impacto en la red, ya que provoca que el tráfico se encamine por otros enlaces

que se pueden congestionar. Cuando el enlace se ha recuperado, también tiene la posibilidad de volver a ponerlo en servicio.

La función de gestión de tráfico es la que dispone que el tráfico se encamine por los señalizadores que están en buen estado dentro de un "linkset". Un linkset es el conjunto de señalizadores de una misma ruta.

Por último, la función de gestión de encaminamiento es la que se encarga de avisar a otros SP de que uno no puede alcanzar un destino determinado, con el objeto de que los demás no le envíen mensajes para él. Uno de los mensajes más comunes que utiliza es "Transfer Prohibited".

La MTP se desarrolló para aplicaciones de telefonía básica en tiempo real. Posteriormente, cuando aparecen otras necesidades (por ejemplo la transmisión de datos) y extensiones del servicio telefónico se ha desarrollado una nueva aplicación llamada parte de control de la conexión de señalización, SCCP (Signalling Connection Control Point) que está ubicada sobre la MTP y corresponde con el nivel superior de la capa de red del modelo OSI.

Parte de Control de Conexión de Señalización – SCCP (Signalling Connection Control Point)

Como se acaba de ver, cuando se requiere un acceso a una base de datos, la MTP va acompañada de un protocolo superior tal y como se ve en la siguiente figura, que se denomina SCCP (Signalling Connection Control Part) y que proporciona el direccionamiento necesario para encaminar la llamada hacia la base de datos de que se trate. Las direcciones de las bases de datos se denominan números de subsistema (SSN).

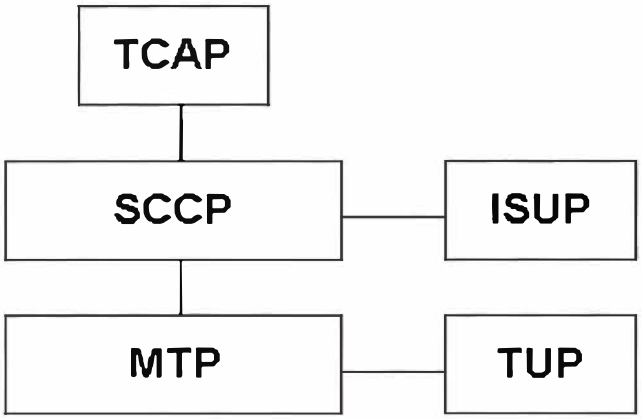


Figura 2.22 Parte de Control de Conexión de Señalización

La combinación de MTP y SCCP se denomina parte de servicio de red, NSP (Network Service Part). El SCCP puede soportar servicios orientados a conexión y servicios no orientados a conexión. Los primeros se utilizan cuando la cantidad de mensajes a transmitir es muy alta y es necesario establecer previamente un camino de señalización. Los segundos no utilizan ningún camino de señalización previamente establecido: la información de encaminamiento va incluida en cada paquete. El propósito de SCCP es proporcionar los medios necesarios para establecer una comunicación de señalización extremo a extremo y no sólo punto a punto como hacia el MTP. El SCCP proporciona el direccionamiento para que un mensaje pueda ser encaminado a través de toda la red.

La diferencia principal con el MTP está en la forma de direccionar. MTP proporciona solamente el OPC y DPC de los SP de ambos extremos de un enlace. SCCP basa su direccionamiento en tres parámetros que son las partes llamada y llamante, el punto de señalización y el SSN (número de subsistema). El encaminamiento se puede basar en cualquiera de los tres anteriores. SCCP es necesario para que la red pueda encaminar mensajes TCAP a la base de datos requerida. De hecho, actualmente, SCCP se utiliza sólo con TCAP y no con ISUP. En los estándares se indica el uso de SCCP con ISUP, pero todavía no está implementado en ninguna red SS7.

Parte de Usuario – UP (User Part)

La parte usuario desempeña funciones que corresponden con el nivel 7 del modelo OSI y tienen por objeto la creación y el tratamiento de la información de señalización antes de

que ésta se transmita por la red de señalización. En el contexto del SS7, el término "usuario" designa cualquier entidad funcional que utiliza la capacidad de transferencia proporcionada por la MTP.

Como en el sistema de señalización se intercambia información entre diferentes clases de usuarios, las funciones de la UP se particularizan para esas clases. En la PSTN, el usuario principal es la señalización correspondiente a las llamadas telefónicas, que configura la parte usuario de telefonía, TUP (Telephony User Part). En consecuencia, la TUP utiliza la capacidad de transporte de la MTP para proporcionar señalización en aplicaciones con conexión (conmutación de circuitos), para el control de las llamadas en telefonía analógica y digital.

En el caso de la red digital de servicios integrados, ISDN, la parte usuario se denomina ISUP (ISDN User Part). La ISUP es la parte del SS7 que utiliza la capacidad de transporte de la MTP y la SCCP para proporcionar servicios relativos a las llamadas por la ISDN tales como el control de las conexiones de red, con / sin conmutación de circuitos, entre centrales para las comunicaciones de voz y datos así como servicios de red inteligente.

La ISUP corresponde a los niveles altos del modelo OSI. ISUP está relacionado con voz y datos, pero no puede soportar tecnologías de banda ancha como ATM o Frame Relay. Es por esta razón que se ha desarrollado una nueva versión de ISUP denominada BISUP o Broadband ISUP (ISUP de banda ancha). ISUP fue desarrollado a partir de TUP y para sustituirlo, ya que TUP no es capaz de soportar circuitos digitales ni transmisión de datos, en cambio ISUP sí.

Otras Funciones

Existen, además, otras funciones de red no relacionadas estrictamente con los circuitos de comunicación, como, por ejemplo, el acceso a bases de datos ó funcionalidades de control remoto. En una arquitectura de protocolos, se definen las capacidades de transacción, TC (Transaction Capabilities) como el conjunto de protocolos y

funcionalidades utilizados por un grupo de aplicaciones distribuidas en una red para su intercomunicación.

En el contexto del SS7, las TC se refieren a los protocolos de la capa de aplicación, por lo que se denomina parte de aplicación de las capacidades de transacción, TCAP (Transaction Capabilities Application Part). La TCAP utiliza los servicios de SCCP y MTP y proporciona un conjunto de métodos, en un entorno sin conexión, disponibles por una aplicación en un nodo para invocar la ejecución de un procedimiento en otro nodo e intercambiar los resultados de esa invocación.

Por consiguiente, TCAP comprende protocolos y servicios para ejecutar operaciones remotas. En las redes de telecomunicaciones, las aplicaciones distribuidas que utilizan TCAP pueden residir en centrales y bases de datos de la red. El elemento del servicio de aplicación, ASE (Application Service Element) de la TCAP proporciona la información específica que requiere una aplicación determinada.

Existen diversos protocolos de aplicación que corren sobre TCAP, podemos mencionar los siguientes:

- MAP (Mobile Application Part), que contiene los protocolos necesarios para las comunicaciones entre las unidades funcionales específicas de las redes móviles, como son los centros de conmutación del servicio móvil MSC y los registros de abonados y equipos. La MAP proporciona las funciones básicas asociadas a la movilidad: roaming, registro, actualización, traspaso y la seguridad: autenticación de usuarios y equipos que son utilizados para la señalización de las redes de telefonía móvil
- CAMEL (Customized Application for Mobile network Enhanced Logic), que es utilizado para aplicaciones de redes inteligentes; y por último
- OMAP (Operation, Maintenance and Administration Part), el cual proporciona los protocolos y procedimientos de aplicación para la supervisión, coordinación y control de los recursos de red que hacen posible las comunicaciones del SS7.

2.3 GPRS (General Packet Radio Service)

El servicio GPRS es una evolución de GSM y su característica principal es que permite a los usuarios móviles enviar y recibir datos por paquetes. En modo de conmutación de paquetes no se reserva un canal de comunicaciones físicamente durante el tiempo que dura la transferencia de datos sino que los paquetes se envían a través de unos recursos compartidos por todos los usuarios (mayor eficiencia con respecto a una comunicación por circuitos). Además permite asignar calidades de servicio (QoS) diferenciadas a los distintos usuarios móviles.

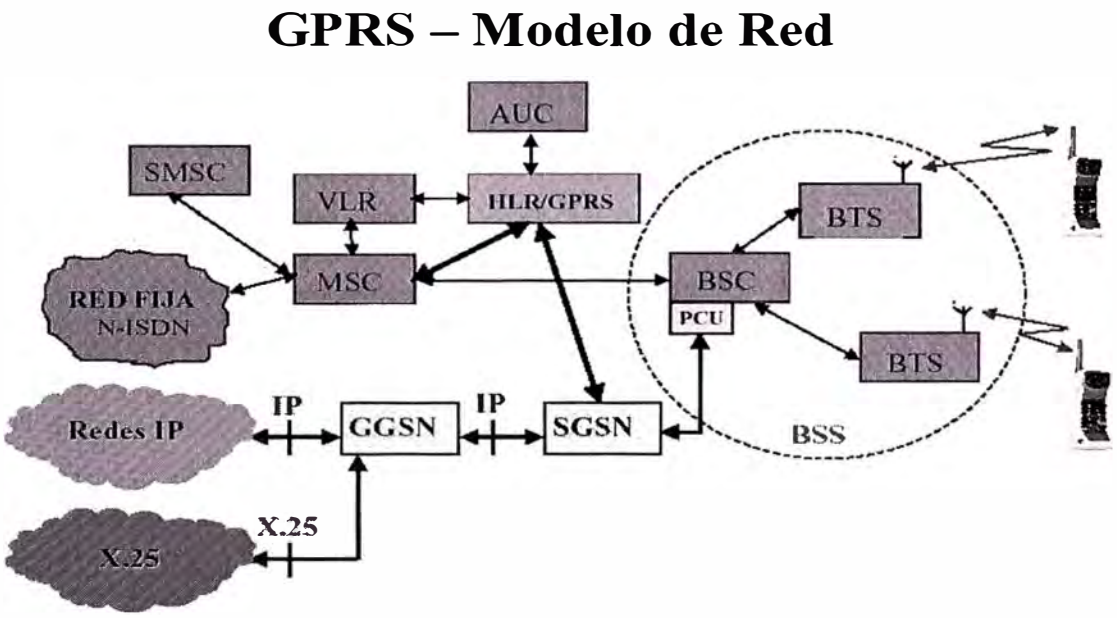


Figura 2.23 Modelo de una Red GPRS

El servicio GPRS es el estándar, definido en el ámbito ETSI, que permite la introducción de la transmisión de datos a paquetes en el sistema GSM. El GPRS también ha sido aceptado por la asociación americana TIA (Telecommunications Industry Association) como estándar de datos para el sistema TDMA/136.

El GPRS permite transmitir y recibir datos con una modalidad de transmisión a paquetes tanto sobre la interfaz radio, como en la infraestructura de red, sin utilizar recursos de conmutación de circuitos. La conmutación de paquetes es una tecnología idónea para las aplicaciones de datos y permite por ejemplo que varios usuarios puedan compartir un

mismo canal de GPRS. De hecho la arquitectura de red está basada en el protocolo TCP/IP que es el que se usa en las redes de datos (LAN).

Las tasas de transmisión de datos (throughput) están divididas en categorías dependiendo del número de slots que utilicen (multislots). De esta manera podemos distinguir 4 tipos (CS – Coding Schemes)(1):

- CS-1 – Ofrece una tasa variable entre 8 kbps a 64 kbps.
- CS-2 – Ofrece una tasa variable entre 12 kbps a 96 kbps.
- CS-3 – Ofrece una tasa variable entre 14.4 kbps a 96+ kbps.
- CS-4 – Ofrece una tasa variable entre 20 kbps a 115+ kbps.

Todos estos dependen de las capacidades de la estación móvil (MS) y el número de timeslots aceptados (multislots). Las tasas de transmisión altas son más sensibles para la calidad del enlace de radio:

- CS-1 es mandatario para el BSS y es también usado para la señalización.
- CS-1, CS-2, CS-3 y CS-4 son mandatarios para la estación móvil.
- CS-4 no tiene corrección de error hacia delante.

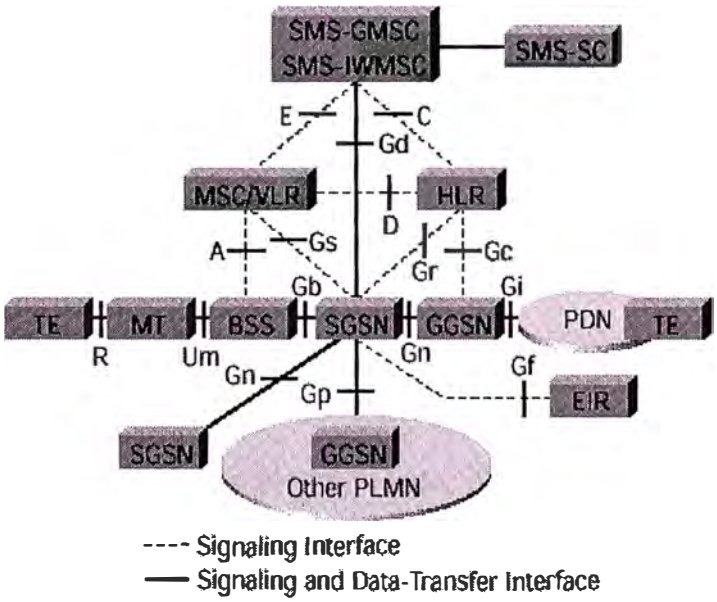
Tradicionalmente, la transmisión de datos inalámbrica se ha venido realizando utilizando un canal dedicado GSM a una velocidad máxima de 9.6 kbps. Aunque también muchos operadores han implementado el HSCSD (High Speed Circuit Switched Data) que alcanzan velocidades hasta los 28 kbps. Pero con GPRS, la velocidad de transmisión de datos puede llegar a un máximo de 115 kbps por comunicación y en promedio a unos 40 kbps. GPRS es una red superpuesta a GSM que comparte con ella la red de acceso. Sin embargo, GPRS introduce dos nuevos nodos: Gateway GPRS Support Node (GGSN) y el Serving GPRS Support Node (SGSN). El GGSN actúa como una interfase hacia las redes de paquetes de datos externas mientras que el SGSN es responsable de la entrega de paquetes al usuario móvil en su área de servicio.

En cuanto a los tipos de servicios soportados mediante GPRS se encuentran los siguientes:

- Servicios basados en el envío de mensajes cortos
- Servicios generales de Internet y conexiones a Intranets.
- Aplicaciones WAP
- Servicios específicos de GPRS
- Servicios basados en la localización
- Servicios de VideoStreaming (TV Móvil)

2.3.1 Arquitectura de la Red GPRS

La red GSM clásica no ofrece funcionalidades adecuadas para el encaminamiento de datos de conmutación de paquetes. Por esta razón, la estructura convencional GSM ha sido extendida con la introducción de una nueva clase de entidades lógicas de red denominadas GSN (GPRS Support Node).



Source: ETSI

Figura 2.24 Arquitectura de la Red GPRS

Los nodos GSN gestionan la interconexión con otras redes y desarrollan múltiples funciones: gestión de la movilidad, roaming y reencaminamiento geográfico, control de la conexión virtual, transmisión de los paquetes. El Serving GPRS Support Node (SGSN), que está conectado a la red de acceso y se encuentra al mismo nivel jerárquico que las centrales de conmutación (MSC/VLR), es el nodo que da servicio al terminal móvil GPRS,

conservando la información de posición y ejecutando funciones relativas a la seguridad de la comunicación y al control del acceso. El Gateway GPRS Support Nade (GGSN) es visto, desde el exterior, como la puerta de acceso a la red GPRS y funciona como una unidad de interworking hacia las redes externas de conmutación de paquetes. Dentro de la red, el GGSN está conectado a los nodos SGSN a través de una red de transporte basada en IP.

La base de datos HLR debe ser actualizada con las nuevas funciones para almacenar los datos relativos a los perfiles de los usuarios GPRS y a la información de encaminamiento. Finalmente, los centros de mensajes cortos (SMSC) están conectados al SGSN para permitir la transmisión de mensajes cortos también a través de los canales de radio GPRS. El área de cobertura, es decir, la parte del territorio sobre la que se garantiza el servicio, está organizada en zonas de localización que permiten a la red conocer la posición del terminal móvil durante sus movimientos. Dichas zonas, definidas análogamente a las Áreas de Localización (LA) utilizadas por la red de conmutación de circuitos, se denominan Routing Área (RA) y determinan áreas de superficie inferior respecto a las de las LA.

Con el objetivo de satisfacer las necesidades de los diversos segmentos de mercado se definieron tres tipos de terminales distintos(15):

- **Terminal de clase A**: el terminal puede estar simultáneamente conectado tanto a la red GSM, para poder utilizar los servicios basados en conmutación de circuitos, como a la red GPRS, para poder transmitir y recibir datos de paquetes. En otras palabras, este tipo de terminales permite un uso simultáneo de tráfico de paquetes y de circuitos.
- **Terminal de clase B**: el terminal puede estar simultáneamente registrado sobre las dos redes, de circuito y de paquetes, pero no puede enviar y recibir tráfico a la vez en ambos modos.
- **Terminal de clase C**: el terminal sólo puede estar registrado en la red a modalidad de paquetes ó en la de circuitos, por lo que sólo puede soportar tráfico relativo al tipo de

servicio para el que está registrado.

Problemáticas de Encaminamiento y Señalización

La infraestructura de red para la realización del servicio GPRS se basa en la tecnología IP. La utilización de esta tecnología para transmisiones desde/hacia usuarios móviles, exige soluciones particulares de encaminamiento, para permitir la entrega de los paquetes IP enviados. De hecho, la versión de IP utilizada en el estándar GPRS no prevé ningún mecanismo para la gestión de la movilidad. Por ello, en el estándar GPRS ha sido introducido un método de encaminamiento específico que a continuación es ilustrado brevemente.

En la transmisión de los paquetes de información dentro de la red GPRS, el terminal móvil está caracterizado por una dirección IP que se le asigna permanente o dinámicamente, en el momento del establecimiento de la sesión. Los paquetes, provenientes de las redes externas son enviados al GGSN a la que el terminal pertenece. El GGSN posee las informaciones de encaminamiento necesarias para enviar el paquete (utilizando el método de tunnelling) al nodo SGSN, que da servicio al área geográfica donde se encuentra actualmente localizado el móvil. El SGSN, a su vez, realiza una conexión lógica con el terminal, a través de la cual tiene lugar la entrega del paquete.

En el caso de una transmisión originada por un terminal móvil, el SGSN encapsula los paquetes entrantes y los transfiere a su GGSN, donde son transmitidos a las redes de datos de destino. Todos los datos relativos a los usuarios GPRS, necesarios en el nodo SGSN para realizar el encaminamiento y la transferencia de los datos, se encuentran almacenados en el registro GPRS, que conceptualmente forma parte del nodo HLR del sistema GSM. El registro GPRS contiene las informaciones de encaminamiento y la correspondencia entre la identificación del usuario (IMSI - International Mobile Subscriber Identity) y la dirección IP asignada, y entre esta última y el GGSN correspondiente.

2.3.2 Principales Procedimientos de Control

Los principales procedimientos de control utilizados en la red GPRS son:

Procedimiento de Registro (Procedimiento de GPRS Attach)

Antes de que un terminal móvil pueda acceder a los servicios GPRS, debe informar a la red de su presencia, llevando a cabo un procedimiento de GPRS Attach contra el nodo SGSN. El procedimiento de Attach incluye: la actualización de las informaciones de localización en el HLR, la transferencia de la información entre el antiguo SGSN, en el que el móvil estaba registrado anteriormente, y el nuevo SGSN; la cancelación de los datos del antiguo SGSN (y del antiguo VLR, si el móvil estaba también registrado en la red GSM para los servicios de conmutación de circuitos).

Los procedimientos de registro (GPRS Attach) y de activación de contexto PDP (Packet Data Protocol Context Activation) deben ejecutarse para permitir al usuario GPRS la conexión con las redes de datos externas. A todos los efectos, el procedimiento de GPRS Attach, análogamente al procedimiento correspondiente en el mundo de conmutación de circuitos (IMSI Attach), sirve para permitir que la red sea informada de la presencia del terminal móvil. Una vez que el terminal está registrado, la red conoce su posición en el ámbito de Routing Área, así como sus características de servicio. El procedimiento de GPRS Attach consiste en la ejecución de las siguientes acciones:

1. El terminal pide a la red la activación del procedimiento. En la petición que el terminal envía al SGSN se indica: la capacidad, por parte del terminal, de soportar altas velocidades de transmisión (utilización simultánea de más de un slot en la interfase radio), el algoritmo de cifrado utilizado y la modalidad para la que se pide el acceso (circuito, paquete o ambas).
2. Se ejecuta el procedimiento de autenticación.
3. Los datos de usuario se transfieren del registro del HLR a los nodos SGSN y MSC/VLR.
4. El nodo SGSN informa al móvil que el procedimiento requerido ha sido completado

con éxito.

Pero para transmitir ó recibir datos, un MS debe activar un contexto PDP. La activación del contexto PDP hace notar al GGSN correspondiente la presencia del móvil y permite la transferencia de paquetes a y desde el usuario. Para las comunicaciones destinadas a un terminal móvil, si los paquetes llegan al GGSN antes de que el móvil haya activado un contexto PDP, el GGSN podrá iniciar un procedimiento de activación del contexto PDP originado por la red (este procedimiento sólo es posible si la dirección ha sido asignada estáticamente). Con la ejecución del procedimiento de detach (originado por la red ó por el terminal), todos los contextos PDP de un determinado móvil se desactivan. El procedimiento de detach puede originarse implícitamente al expirar un tiempo preestablecido ó durante un período de inactividad del móvil. En el caso de abonados en roaming que tienen una dirección PDP asignada por la red HPLMN, se crea un camino de transferencia entre la HPLMN y la VPLMN para la comunicación con el móvil en ambos sentidos. Se pueden utilizar protocolos, como BGP (Border Gateway Protocol) (IETF RFC 1771), entre los routers de frontera, BG (Border Gateway), basándose en acuerdos bilaterales entre los operadores.

Procedimiento de Activación del Contexto (PDP Context Activation)

Para que el terminal móvil pueda comunicarse con las redes de datos externas, debe estar activado el contexto para el protocolo de transferencia de paquetes de datos (PDP Context Activation). El contexto PDP describe las características de la conexión con la red de datos externa como: el tipo de red, la dirección de destino, la dirección del GGSN a utilizar y las características de calidad de servicio. El procedimiento de PDP Context Activation consiste en la ejecución de las siguientes acciones:

1. El terminal móvil requiere la activación del contexto PDP, especificando algunos parámetros, entre ellos la asignación de una dirección estática ó dinámica y la calidad del servicio demandada.
2. El nodo SGSN convalida la petición, basándose en los datos aprovisionados recibidos

del registro del HLR (en el momento del procedimiento de registro).

3. El nodo SGSN determina la dirección del nodo GGSN según las informaciones recibidas del terminal y los datos de aprovisionamiento.
4. Se crea una conexión lógica entre SGSN y GGSN llamada túnel GTP.
5. El nodo SGSN pide al nodo GGSN la asignación de una dirección IP y entonces la transfiere al terminal móvil.
6. En este momento, puede empezar la comunicación entre el terminal móvil y la red de datos externa.

Gestión de la Movilidad en GPRS

El terminal móvil conoce su propia posición ya sea en términos de celda como de RA (Routing Area) visitada, mientras que en la red la posición del móvil se sigue a dos niveles, según el estado del procedimiento de gestión de la movilidad. Cuando el móvil ha ejecutado un procedimiento de attach en la red GPRS, pero no está involucrado en ninguna conexión activa, la red sigue sus movimientos a nivel de RA. Cuando el terminal está involucrado en una conexión activa, la posición se sigue a nivel de celda. La movilidad entre SGSN y GGSN se gestiona gracias a la utilización del protocolo de Tunnelling GPRS (GTP). El protocolo GTP también permite la transferencia de las informaciones entre distintos SGSN en el momento en el que el móvil cambia de SGSN. Para mantener actualizada su posición en la red, el móvil ejecuta un procedimiento de gestión de la movilidad cuando entra en una nueva celda ó en una nueva RA. La actualización de la RA podría también tener un cambio de SGSN (movilidad inter-SGSN), en cuyo caso se activa un procedimiento que involucra a las siguientes entidades:

- Al antiguo SGSN, para transferir las informaciones de contexto PDP relativas a los contextos activos y para preparar un camino de transferencia para los datos aun no transmitidos del GGSN al antiguo SGSN.
- Al GGSN en correspondencia a cada contexto PDP activo, para actualizar los túneles GTP.

- Al HLR, para almacenar las nuevas informaciones sobre el SGSN y eliminar las relativas al antiguo SGSN.

Para el transporte de los servicios en tiempo real (por ejemplo: videostreaming) sobre GPRS, un elemento crítico es la actualización de la RA. Es necesario verificar que este procedimiento sea lo suficientemente rápido para permitir la movilidad del terminal sin interrupciones en el servicio. De hecho, en GPRS el concepto de handover se introduce en términos de reselección de celda y actualización de la RA.

Procedimiento de Actualización de la Posición (Routing Area Update)

El procedimiento de Routing Area Update (RAU) se lleva a cabo cuando el móvil GPRS cambia el área geográfica (Routing Area) en la que se encuentra. Dicha área, definida independientemente de la organización de las Áreas de Localización de GSM, permite la distribución de los mensajes basándose en los criterios específicos del servicio.

El terminal móvil reconoce un cambio de Routing Area leyendo el contenido del canal de señalización broadcast, transmitido por la estación base que garantiza la cobertura radio de la celda utilizada. Este canal, transmite la identificación del Routing Area al que pertenece la celda. Cuando se produce un cambio en la selección de la celda utilizada, el terminal controla la identificación transmitida y, si éste es distinto al de la celda precedente, ejecuta el procedimiento de Routing Área Update que actualiza la información de localización relativa al usuario en los registros de red.

Nota referente a EDGE

EDGE es una tecnología 3G que ofrece velocidades de datos similares a una banda ancha, éste utiliza la misma estructura de trama del GSM actual, es decir con canales de 200Khz, por lo que su implementación es sencilla y se realiza sobre la red GPRS (sólo es necesario hacer unos cambios de Hw y Sw en el subsistema BSS).

La cobertura EDGE se activa por TRX, permitiendo al Operador activarlo en Hot Spots. Se pueden apreciar las bondades del EDGE cuando se utiliza para transmisión de grandes volúmenes de información

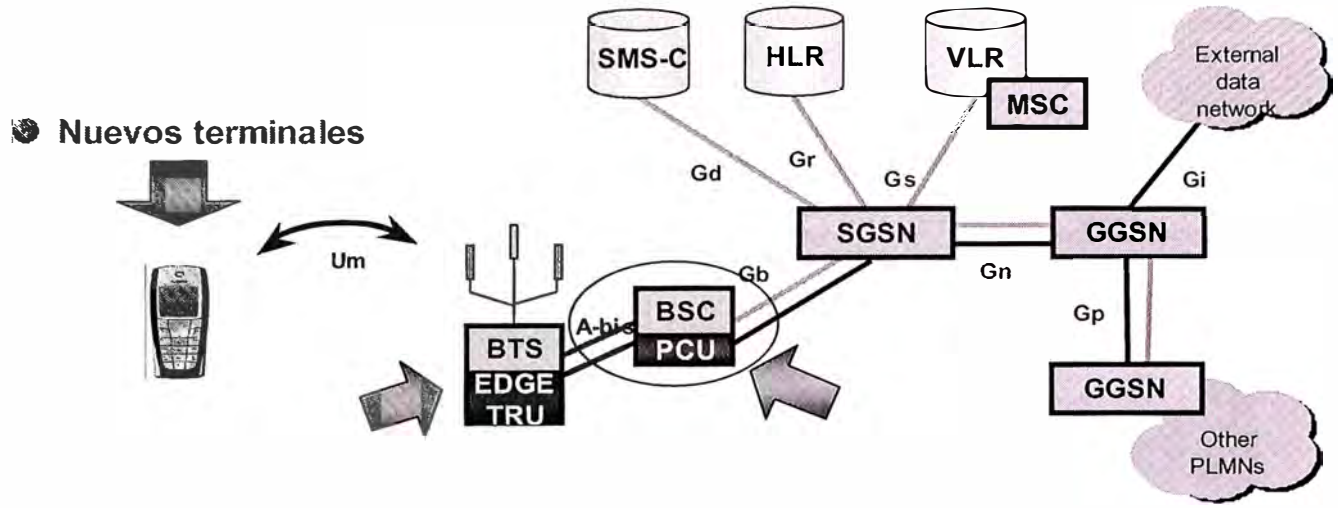


Figura 2.25 Qué se requiere para EDGE?

2.4 WAP (Wireless Application Protocol)

Uno de los desarrollos que despierta gran interés entre los operadores de redes móviles es el denominado WAP (Protocolo de Aplicaciones Inalámbricas) que permite la convergencia entre Internet y la Red Móvil.

El Forum WAP (http://www.wapforum.org), fundado en 1997 por Ericsson, Motorola, Nokia y Phone.com (antes denominado Unwired Planet), lanzó en sólo dos años la primera especificación WAP 1.1, que se ha convertido en el estándar universalmente aceptado para el acceso a Internet desde terminales móviles. Éste, no es un estándar de hecho, sino de facto, puesto que la asociación de industrias que lo apoya no es un organismo internacional de estandarización, aunque colabora estrechamente con varios de ellos.

WAP es un protocolo abierto, independiente de la plataforma en la que se instale el servidor de contenidos y del sistema de radio de transporte, de libre distribución, para ser utilizado desde cualquier tipo de terminal inalámbrico. Para ello, se parte del modelo basado en la arquitectura definida para el World Wide Web (WWW), pero adaptada a los nuevos requisitos del sistema. En la siguiente figura se muestra el esquema de la arquitectura WAP.

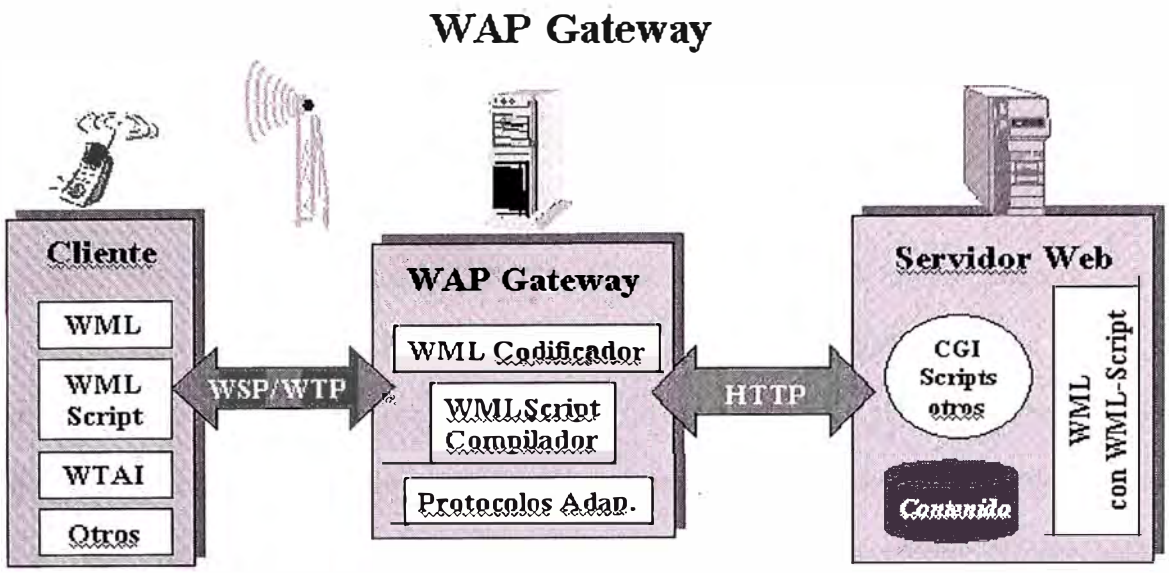


Figura 2.26 Esquema de WAP

En el terminal móvil hay un navegador específico simple, comparable a los que ofrecen Netscape Navigator ó Internet Explorer, encargado de la coordinación con el Gateway a la que realiza peticiones de información, que son tratadas y encaminadas hacia los servidores de información. Una vez procesado en el servidor la petición, la información resultante se envía al Gateway, que la procesa y la envía al teléfono móvil. Generalmente la inteligencia esta en los servidores WAP, mientras que en los terminales se añade un simple navegador con el objeto de que no se encarezcan demasiado.

Los lenguajes utilizados son el WML (Wireless Markup Language), una versión de HTML que tiene en cuenta el pequeño ancho de banda de los sistemas móviles, las limitaciones de las pantallas y la memoria de los teléfonos móviles (líneas que pueden visualizar, formas de navegación y entrada de datos, capacidad de almacenamiento, etc.), y el WMLScript, un lenguaje basado en JavaScript, que ofrece una lógica de tratamiento de datos y acceso a dispositivos WAP y a sus periféricos.

En vez de HTML, WAP usa el Wireless Markup Language (WML) que es diseñado para dispositivos con pantalla pequeña.

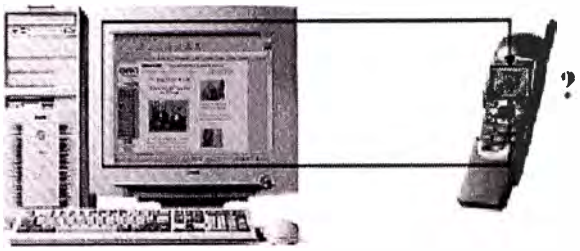


Figura 2.27 Comparación entre HTML y WML

Para conseguir consistencia en la comunicación entre el terminal móvil y los servidores de red que proporcionan la información, WAP define un conjunto de componentes estándar:

- Un modelo de nombres estándar. Se utilizan las URLs (*Universal/Uniform Resource Identifier* ó Identificador Uniforme/Universal de Recurso) definidas en WWW para identificar los recursos locales del dispositivo y el contenido WAP en los servidores de información.
- Un formato de contenido estándar, basado en la tecnología WWW.
- Unos protocolos de comunicación estándares, que permitan la comunicación del navegador del terminal móvil con el servidor Web.
- La sintaxis XML (eXtensible Markup Language) llamada WML.

Un papel muy importante en todo el proceso lo juega el lenguaje WML, diseñado para crear páginas Web que sean menos exigentes en cuanto al ancho de banda que las creadas con HTML, al incorporar menos recursos multimedia. Si el servidor Web no dispone de páginas creadas en este lenguaje, un filtro intermedio se encarga de adaptarlas para presentarlas en la pequeña pantalla del teléfono móvil, aunque el resultado de esa adaptación automática no suele ser muy bueno y siempre requiere un ajuste por el desarrollador. La mejor alternativa es crear las páginas específicamente para ser utilizadas con WAP y probar que se representan correctamente en distintos terminales.

2.4.1 La Arquitectura WAP

La arquitectura WAP está pensada para proporcionar un entorno escalable y extensible para el desarrollo de aplicaciones para dispositivos de comunicación móvil. Para ello, se define una estructura en capas, en la cual cada capa es accesible por la capa superior así como por otros servicios y aplicaciones a través de un conjunto de interfases muy bien definidos y especificados. Este esquema de capas de la arquitectura WAP la podemos ver en la siguiente figura:

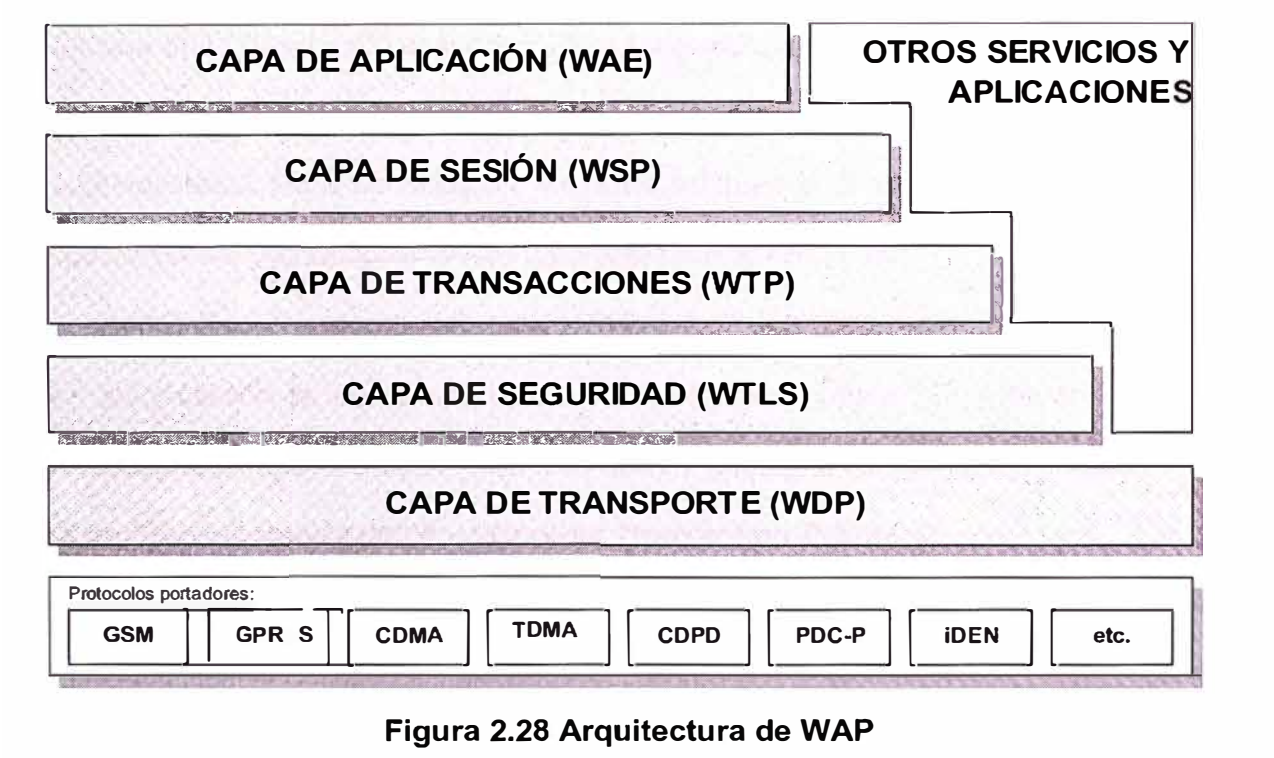


Figura 2.28 Arquitectura de WAP

Capa de Aplicación (WAE – Wireless Application Environment)

El Entorno Inalámbrico de Aplicación (WAE) es un entorno de aplicación de propósito general basado en la combinación del World Wide Web y de las tecnologías de Comunicaciones Móviles.

Este entorno incluye un micro navegador, que posee las siguientes funcionalidades:

- Un lenguaje denominado WML similar al HTML, pero optimizado para su uso en terminales móviles.
- Un lenguaje denominado WMLScript, similar al JavaScript (esto es, un lenguaje para su uso en forma de Script)

- Un conjunto de formatos de contenido, que son un conjunto de formatos de datos bien definidos entre los que se encuentran imágenes, entradas en la agenda de teléfonos e información de calendario.

Capa de Sesión (WSP – Wireless Session Protocol)

El Protocolo Inalámbrico de Sesión (WSP) proporciona a la Capa de Aplicación de WAP interfaz con dos servicios de sesión: Un servicio orientado a conexión que funciona por encima de la Capa de Transacciones y un servicio no orientado a conexión que funciona por encima de la Capa de Transporte (y que proporciona servicio de datagramas seguro ó servicio de datagramas no seguro).

Actualmente, esta capa consiste en servicios adaptados a aplicaciones basadas en la navegación Web, proporcionando las siguientes funcionalidades:

- Semántica y funcionalidades del HTTP/1.1 en una codificación compacta.
- Negociación de las características del Protocolo.
- Suspensión de la Sesión y reanudación de la misma con cambio de sesión.

Capa de Transacciones (WTP – Wireless Transaction Protocol)

El Protocolo Inalámbrico de Transacción (WTP) funciona por encima de un servicio de datagramas, tanto seguros como no seguros, proporcionando las siguientes funcionalidades:

- Tres clases de servicio de transacciones: Peticiones inseguras de un solo camino, Peticiones seguras de un solo camino, y Transacciones seguras de dos caminos (petición-respuesta)
- Seguridad usuario-a-usuario opcional.
- Transacciones asíncronas.

Capa de Seguridad (WTLS – Wireless Transport Layer Security)

La Capa Inalámbrica de Seguridad de Transporte (WTLS) es un protocolo basado en el estándar SSL, utilizado en el entorno Web para propósitos de seguridad en la realización de transferencias de datos. Este protocolo ha sido especialmente diseñado para los

protocolos de transporte de WAP y optimizado para ser utilizado en canales de comunicación de banda estrecha. Para este protocolo se han definido las siguientes características:

- Integridad de los datos. Este protocolo asegura que los datos intercambiados entre el terminal y un servidor de aplicaciones no ha sido modificada y no es información corrupta.
- Privacidad de los datos. Este protocolo asegura que la información intercambiada entre el terminal y un servidor de aplicaciones no puede ser entendida por terceras partes que puedan interceptar el flujo de datos.
- Autenticación. Este protocolo contiene servicios para establecer la autenticidad del terminal y del servidor de aplicaciones.

Capa de Transporte (WDP – Wireless Datagram Protocol)

El Protocolo Inalámbrico de Datagramas (WDP) proporciona un servicio fiable a los protocolos de las capas superiores de WAP y permite la comunicación de forma transparente sobre los protocolos portadores válidos.

Debido a que este protocolo proporciona un interfaz común a los protocolos de las capas superiores, las capas de Seguridad, Sesión y Aplicación pueden trabajar independientemente de la red inalámbrica que dé soporte al sistema.

2.5 Streaming

Las aplicaciones multimedia son aquellas que integran diferentes medios como el audio, video, imágenes, textos, entre otros. Estas aplicaciones imponen restricciones a los sistemas computacionales y redes de telecomunicaciones relacionados con los recursos necesarios (canales de radiofrecuencia disponibles, anchos de banda, etc.) para que se ejecuten correctamente y por la naturaleza de los medios relacionados con el video y el audio, normalmente caen en la categoría de sistemas en tiempo real.

Una aplicación de streaming es aquella en la cual el receptor reproduce el contenido recibido (audio, video, etc) conforme va llegando sin necesidad de descargarlo

completamente antes. El emisor envía paquetes pequeños de información de forma que el receptor puede acceder a la información a medida que los recibe.

La plataforma tecnológica requerida para los sistemas de streaming actualmente son propietarios y apenas se están dando pasos iniciales por lograr acuerdos entre proveedores de tecnologías de streaming. En la actualidad los dos principales proveedores de tecnologías para streaming representados por RealNetworks y Windows Media de Microsoft manejan distintos tipos de streaming no compatibles entre ellos.

2.5.1 Introducción

Una aplicación Streaming funciona de la siguiente manera: primero el computador cliente se conecta con el servidor y éste le empieza a mandar paquetes de información pertenecientes a un archivo previamente almacenado ó datos generados en tiempo real. El cliente comienza a recibir dichos paquetes los cuales almacena en un buffer donde empieza a guardar la información. Cuando se ha llenado el buffer con una pequeña parte de la información, el cliente empieza a reproducir el contenido multimedia y a la vez continúa con la descarga.

El sistema está sincronizado para que se pueda reproducir mientras se continua recibiendo paquetes, diferencia fundamental entre bajar primero todo el contenido de la sesión y al final reproducir (transferencia de archivos). Si en algún momento la conexión sufre reducción de velocidad, se utiliza la información que hay en el buffer, de modo que se puede aguantar un poco ese descenso. Si la comunicación se corta demasiado tiempo, el buffer se vacía y la reproducción se interrumpe hasta que se restaurase la señal.

Para explicar mejor el último comentario, se ha agregado la siguiente descripción de RealPlayer acerca de cómo funciona la tecnología de flujo en servicios multimedia.

En sí, el flujo toma los archivos, ya sean de sonido, vídeo, animación ó cualquier otro soporte multimedia, los divide en fragmentos más pequeños y los envía a su destino. Es muy parecido al método de envío de información por la red que se utiliza en los sistemas ó en Internet en general.

"RealPlayer es capaz de leer el flujo de archivos a medida que se recibe y empezar a reproducir antes de que llegue el resto de archivos. Imagine que está leyendo una novela mientras alguien le va pasando las páginas una a una. Contrástelo con el hecho de esperar a que se termine el libro entero para que le pasen la novela entera de una sola vez. Naturalmente, si sólo se leyera el archivo y se reprodujera a medida que fuera llegando, se producirían numerosas interrupciones. Sólo tiene que pensar en el tiempo que tiene que esperar para ver una página Web en el monitor, teniendo en cuenta que las páginas Web son mucho más pequeñas que la mayoría de los archivos multimedia (sonido, vídeo, animación, etc.). RealPlayer combina la tecnología de flujo con otra tecnología para hacer que la reproducción sea más fluida: el almacenamiento en buffer. Este método consiste en recopilar varios paquetes antes de empezar a reproducirlos.

Figura 2.29 Analogía en la Tecnología de Flujo en Servicios Multimedia

Imagine una taza que se vaya llenando escalonadamente. Un pequeño agujero en la base permite que haya un flujo constante de agua saliente. Mientras haya suficiente agua en la taza, el flujo continuará saliendo a una velocidad constante. Del mismo modo, cuando RealPlayer empieza a reproducir un archivo, continúa recabando los paquetes que están en reserva. Esto significa que incluso si se produce algún retraso al obtener los paquetes de información en el sistema, la música se escuchará de manera fluida, sin interrupciones."(23)

Los flujos pueden optimizarse para distintos anchos de banda. El ancho de banda es, básicamente, la cantidad de información que puede pasar a través de un punto determinado del cable durante un determinado período de tiempo. Cuanto mayor sea el ancho de banda, mayor será la información que se pueda transmitir. La velocidad del módem, si es éste el dispositivo que se utiliza para conectarse por ejemplo a Internet, determina el ancho de banda del flujo que se puede recibir.

Un módem a 28,8 Kbps puede recibir, aproximadamente, 28.800 bits por segundo. Un módem a 56 Kbps, puede recibir unos 56.000 bits por segundo, casi el doble que un módem a 28,8. Estos datos se proporcionan asumiendo que las conexiones telefónicas son perfectas, lo que no siempre ocurre. En otras palabras, el rendimiento real puede variar. Es habitual referirse equivocadamente a estas velocidades como velocidad en baudios. No obstante, el término baudio hace referencia a los cambios de sonido base que se producen por segundo (lo que suele denominarse onda portadora). La información se interpreta en función de los cambios de sonido. Al principio, un solo cambio, de un tono agudo a uno grave, por ejemplo, constituía un único bit de información. Gracias a las mejoras realizadas en las técnicas de compresión, ahora es posible transmitir mucha más información que un solo bit por cada cambio efectuado en la frecuencia portadora. Lo importante es que cuanto mayor sea el ancho de banda que se puede recibir, mejor será la calidad del sonido ó de la imagen de vídeo.

2.5.2 La Cadena de Valor del Servicio Streaming.

Los elementos de la cadena de valor del servicio streaming abarcan los siguientes aspectos:

- Personas, como los autores del contenido, los operadores de los equipos, y la audiencia;
- Tecnología, en los equipos y el software requerido para publicar y consultar el contenido; y

- Procesos, para actualizar constantemente el contenido publicado y analizar los beneficios obtenidos hasta el momento.

Estos elementos interactúan en 4 etapas de la cadena de valor, mostrada a continuación:

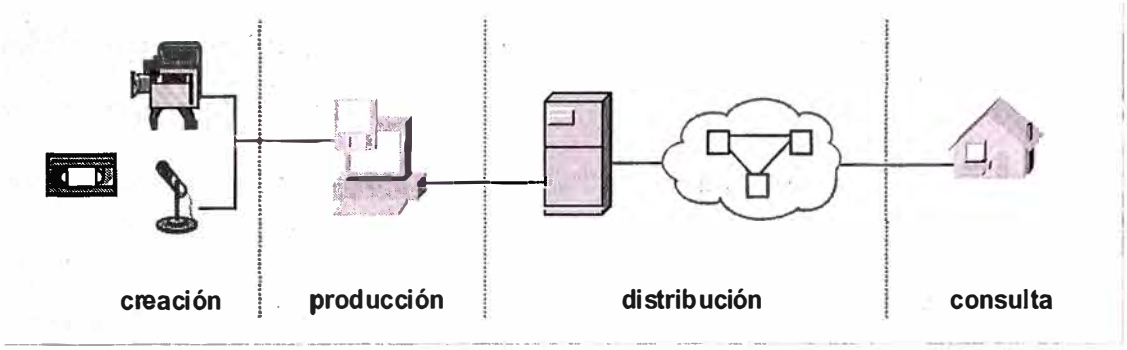


Figura 2.30 Cadena de Valor de Servicios Streaming

Creación

Se refiere a cualquier tipo de contenido por ejemplo: conferencias, presentaciones, informes, etc., que se desee publicar. La etapa de creación de la cadena de valor significa capturar ese contenido a través de una tarjeta que permita capturar video y audio ó por algún medio magnético ó electrónico.

Producción

La etapa de producción reúne todos los elementos de información recolectados durante la creación de contenido, y los transforma en archivos para ser transmitidos hacia otras redes en forma de datos ininterrumpidamente.

Distribución

Los archivos obtenidos durante la etapa de producción pueden ser distribuidos en la red a través de un flujo ininterrumpido de datos. Este método de distribución de contenido se conoce como streaming. La distribución de contenido es responsabilidad de uno ó varios servidores especializados que mantienen el flujo de datos fluyendo ininterrumpidamente hacia el usuario final. Los servidores de streaming se adaptan tanto a las variaciones de congestión de la red como a la velocidad de conexión de cada usuario final, garantizando de esta manera la entrega de la mejor calidad posible de imagen y sonido. Estos

servidores no necesariamente son instalados dentro de las mismas instalaciones donde se encuentran los servidores de producción.

Consulta

Representa al usuario final ó los clientes que a través de su computadora ó teléfono y usando un navegador (por WEB ó WAP) pueden acceder al contenido solicitado.

2.5.3 Protocolos de Streaming

Los protocolos que soportan la comunicación en tiempo real son los siguientes:

2.5.3.1 RTP

RTP son las siglas de "Real Time Transport Protocol" (Protocolo de Transporte de Tiempo Real), diseñado para el transporte de datos con propiedades de tiempo real entre aplicaciones, de una manera eficaz. Como ejemplos, RTP se podría usar para transmitir las señales de audio y vídeo de una videoconferencia, para reproducir una película de vídeo en una red de área local ó como medio de transmisión de una radio en Internet.

Características principales

Las principales propiedades de RTP son las siguientes:

- Los servicios que incluye RTP suministran toda la información necesaria para que una aplicación en tiempo real trabaje de manera interactiva y eficaz. Estos servicios suministran información como:
    - el formato de datos a transmitir.
    - números de secuencia en los paquetes para la reconstrucción de los datos.
    - marcas de tiempo para su posterior uso.
    - control del transporte.
- RTP puede funcionar sobre cualquier protocolo de transporte, aunque lo más habitual es usarlo sobre UDP.
- Soporta la transmisión mediante multienvío, si ésta es soportada por los protocolos de nivel inferior.

- No proporciona medios para la gestión de errores en la transmisión. Éste se deja en manos de los protocolos de niveles inferiores.
- Es un protocolo extensible, es decir, proporciona mecanismos para añadir nuevos servicios.
- Proporciona un mecanismo de confidencialidad, para lograr que únicamente los receptores sean capaces de decodificar los paquetes.
- Permite la negociación del medio de transporte y de los parámetros que se utilizarán para transmitir los distintos flujos.
- En la especificación de RTP (RFC 1889) se le define como un conjunto de dos protocolos:
    - RTP (Real-Time Transport Protocol), encargado de la transmisión de los datos.
    - RTCP (Real-Time Transport Control Protocol), destinado al control de la calidad de servicio y a la gestión de la información de los participantes que forman parte de la comunicación.

Formato de los Paquetes

El formato de un paquete RTP es el siguiente:

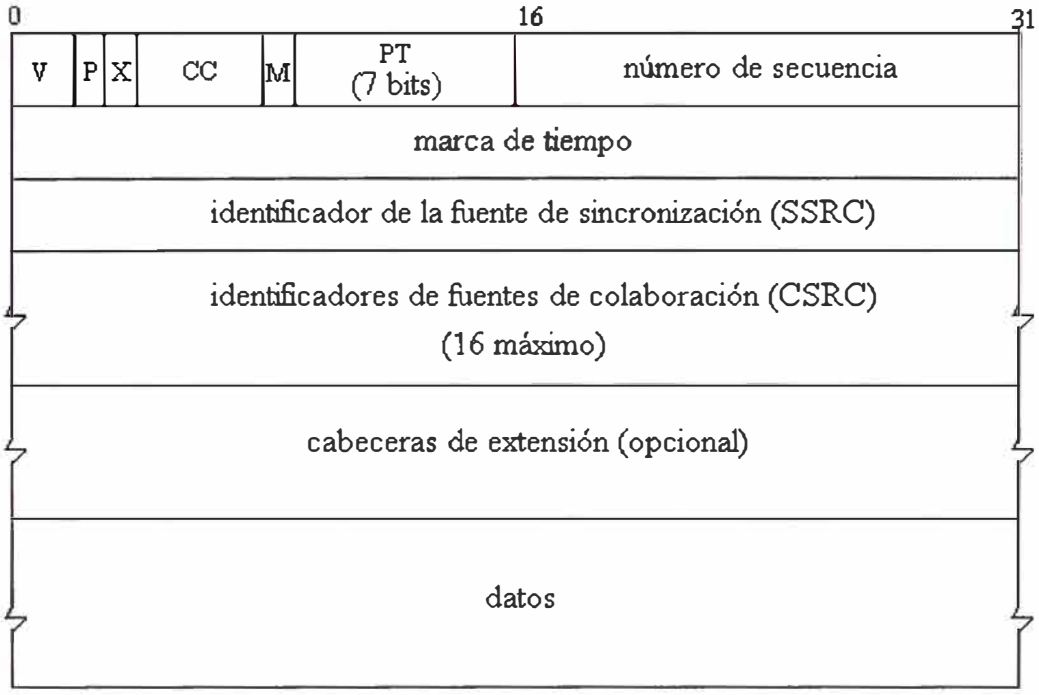


Figura 2.31 Formato de un Paquete RTP

- V: versión del protocolo.
- P: indica si el campo de datos contiene información adicional, que no pertenece a la parte de datos.
- X: especifica si se van a usar cabeceras que extienden el protocolo y que no están definidas en la RFC 1889.
- CC: número de identificadores CSRC (ver campo CSRC).
- M: campo con uso no definido en esta especificación.
- PT: tipo de datos transmitido.
- SEQ: número de secuencia. Este número permite al receptor ordenar los paquetes y determinar si alguno se ha perdido, para volverlo a solicitar.
- TS: marca de tiempo. Permite determinar el instante de tiempo al que pertenece la primera muestra que contiene el campo de datos y así sincronizar su reproducción en tiempo real.

- SSRC: identificador de la fuente de sincronización elegido de forma aleatoria, para evitar que dos mismas fuentes en una misma sesión posean el mismo identificador.
- CSRC: identificadores de las fuentes que han colaborado en la creación del paquete.

Detrás de la cabecera fija existe un número indeterminado de cabeceras de extensión (siempre que el bit-X se haya activado) y a continuación, les sigue el campo de datos.

2.5.3.2 SDP

El Protocolo Descriptor de Sesiones (SDP ó Session Descriptor Protocol) se encuentra diseñado para proporcionar información de los flujos que pertenecen a una sesión multimedia. De esta manera, lo que se pretende es informar a los receptores de la existencia de una sesión multimedia y de cómo participar en ella.

La información que puede suministrar es la siguiente:

- Nombre de la sesión
- El momento en el que la sesión está activa y su duración
- Descripción de los flujos, como puede ser el tipo (audio, video, etc.), el formato (MPEG, Quicktime, H.261), etc.
- Métodos de transporte de dichos flujos (RTP/AVP, RTP/UDP, etc.) y las direcciones de origen (unicast ó multicast)

El mensaje, en el que se indica dicha descripción, puede incluirse como el cuerpo de paquetes diseñados para realizar invitaciones a una sesión ó de información de sesión como ocurre en RTSP.

2.5.3.3 RTSP

RTSP ó "Real Time Streaming Protocol" (Protocolo de Streaming en Tiempo Real) es un protocolo cliente - servidor del nivel de aplicación, destinado al control del transporte en demanda de datos con propiedades de tiempo real y multimedia, como pudieran ser audio y vídeo.

Características principales

Las principales características de este protocolo son las siguientes:

- Permite el control de un conjunto de flujos (streams).
- Suele utilizar como protocolo de transporte TCP, aunque también se pueden usar otros protocolos como UDP.
- El formato de los mensajes es idéntico al del protocolo HTTP.
- La interacción cliente - servidor se basa en el concepto de sesión, no en el de conexión.
- Es decir, si se trabaja sobre TCP, un cliente, en una misma conexión, puede abrir distintas sesiones en el servidor, pudiendo realizar un número indefinido de solicitudes.
- El método de transporte de los flujos no es fijo, aunque se recomienda usar RTP.
- Permite la negociación del medio de transporte y de los parámetros que se utilizarán para transmitir los distintos flujos.
- La descripción e información para manipular un flujo viene dada por una presentación definida por un protocolo, como puede ser SDP.
- El servidor posee estado. Tras un conjunto determinado de operaciones, el servidor llega a un estado, en el que solamente se puede ejecutar otro conjunto determinado de operaciones.
- Establece los mismos métodos de seguridad de HTTP.
- Soporta el control remoto de dispositivos grabadores.

Métodos

Existen distintos métodos que proporcionan los servicios necesarios para que un cliente y servidor se comuniquen. Los métodos más usuales son:

- OPTIONS - La respuesta que obtiene el cliente a esta petición es el conjunto de métodos que soporta el servidor.

- DESCRIBE - Este método permite obtener la presentación ó información de un flujo. En dicha presentación se encuentra información de todo tipo, como puede ser: los distintos flujos de video y audio que posee el archivo, la duración del mismo, el medio de transporte, el ancho de banda, etc. Toda esta información permitirá al cliente configurar de una manera adecuada y acorde a sus posibilidades la posterior sesión.
- SETUP - Una petición de este tipo inicia una sesión (la primera vez que se solicita) y proporciona al cliente la capacidad de configurar el medio de transporte, para un determinado flujo, que permitirá la reproducción del mismo en tiempo real. Pueden enviarse varias peticiones para configurar todos los parámetros deseados.
- PLAY - Esta petición indica al servidor que comience a enviar los datos de un flujo, mediante el método de transporte especificado en los mensajes SETUP. Además, se puede solicitar empezar la reproducción a partir de un determinado tiempo.
- PAUSE - Una vez enviada el servidor deja de enviar datos hasta que no reciba otra petición PLAY.
- TEARDOWN - Mediante este método, el cliente solicita la finalización de la sesión abierta en el servidor, indicando a éste la liberación de todos los recursos reservados para dicha sesión.

El resto de métodos son ANNOUNCE, RECORD, REDIRECT, SET_PARAMETER y GET PARAMETER.

Funcionamiento del Protocolo

El funcionamiento básico del protocolo RTSP se puede resumir de la siguiente manera: Un cliente, mediante una petición SETUP establece una sesión en el servidor y configura ciertos parámetros de control para dicha sesión. Una vez que la negociación haya sido completada correctamente, el cliente solicitará el comienzo de la reproducción mediante una petición PLAY. En ese instante el servidor iniciará el envío de los datos del flujo. En el momento en que el cliente quiera finalizar la sesión enviará un mensaje TEARDOWN. El

siguiente diagrama de estados refleja, tanto para cliente como para servidor, la manera de actuar de RTSP.

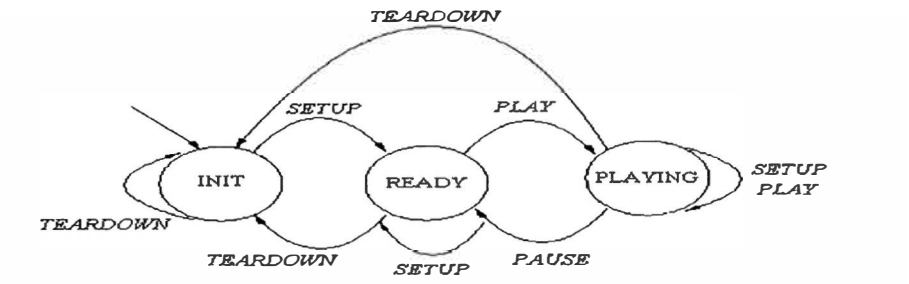


Figura 2.32 Diagrama de Estados del RTSP

Los estados definidos son los siguientes:

- Init: es el estado inicial en el que se encuentran el servidor y cliente, hasta que se recibe y se responde correctamente a un mensaje SETUP. En este estado, no se pueden manejar los mensajes PLAY ya que no se ha establecido aún la sesión.
- Ready: se pasa a este estado si se ha recibido y respondido correctamente al último mensaje SETUP ó a un mensaje PAUSE. La primera vez que el servidor recibe un mensaje SETUP y lo interpreta correctamente, debe asignar una sesión al cliente que ha efectuado la petición, devolviendo su identificador en la respuesta.
- Playing: el servidor ha respondido correctamente al último mensaje PLAY y se encuentra enviando los datos. No se pueden manejar mensajes SETUP en este estado.

2.5.4 Técnicas de Codificación y Compresión

El termino Codificación (coding) es un nombre general en sistemas multimedia que puede hacer referencia a muchas cosas. Puede representar el proceso de Captura de la información multimedia, puede representar el proceso de colocar la información multimedia en un formato dado ó puede representar el proceso de compresión de la información así como una combinación de los procesos anteriores.

En el caso de los sistemas de Streaming, el término Codificación se va a referir al proceso de compresión de medios en formatos específicos. La fuente de información para el proceso de Codificación puede ser:

- Archivos en formatos no comprimidos como AVI ó comprimidos en formatos estandarizados como MPEG1 ó MPEG2.
- Hardware de Captura, como tarjetas que capturen video ó audio. En el caso de video se suele generar la información para el Codificador en formatos como RGB (Red, Green and Blue format) ó YUV 4:2:2 (es uno de los formatos más conocidos, que usa una combinación matricial del RGB para reducir la cantidad de información de la señal) ó en el caso de audio en formato PCM (Pulse Code Modulation – representa a una modulación digital para la transmisión de datos análogos).

Compresión de medios

El audio y video son susceptibles de comprimirse, de manera similar a como se realiza con los gráficos; tal como los formatos JPEG (Joint Photographic Experts Group) y GIF (Graphics Interchange Format), los más utilizados para la publicación de imágenes en la Web, son formatos de compresión que se desarrollaron para superar las limitaciones de formatos como BMP (BitMaP) ó TIFF (Tagged Image File Format), que producen archivos voluminosos y difíciles de enviar a través de Internet ó una red inalámbrica de reducido ancho de banda, en especial a usuarios cuya conexión es inferior a los 56 Kbps. En las imágenes, la compresión elimina información que el ojo humano no puede percibir, de manera que la perdida de calidad resulta imperceptible, aunque, aumentar demasiado la compresión reduce el nivel de calidad. Tal como, un gráfico con color de 24 bits (16.7 millones de colores) hace que el archivo que lo contiene sea voluminoso; al cambiar la misma imagen a 16 bits (65.536 colores) ese tamaño disminuye, sin que en el monitor se aprecie una diferencia marcada. Al bajar el color a 8 bits (256 colores) la calidad disminuye, resulta un número demasiado pequeño de colores para ofrecer una imagen realista.

Al disminuir la resolución de una imagen se disminuye su tamaño. Una imagen de 800 por 600 píxeles, que llenaría la pantalla de un monitor, pesa cuatro veces más que la misma imagen a un tamaño del 50 por ciento (400 x 300 píxeles). Igual caso se presenta con el sonido; al pasar a MP3 una canción de formato de CD cuyo archivo ocupa cerca de 32 MB, se reducirá a 3 MB. MP3, JPG y GIF, es sujeto a mayores tasas de compresión bajando la frecuencia del sonido (mayor frecuencia, mejor calidad) ó cambiando el modo de estereofónico a monofónico. En el video digital, se presenta una combinación de imágenes y sonido, siempre se presentará un canal de audio (MP3 es el canal de audio de MPG3); otro factor que permite realizar compresión es el número de cuadros por segundo. El cine trabaja con 24 cuadros por segundo, los videos digitales logran una calidad óptima a 30; este número se puede disminuir a 15 ó 10, siempre con pérdida de calidad ya que el video pierde fluidez. Un video a 30 cuadros x segundo, con colores reales, resolución de 640 x 480 píxeles, colores reales, sonido estéreo con calidad de CD y a 30 cuadros x segundo, genera una archivo de muchos megas – dependiendo de la duración. Este video mediante streaming no podrá ser apreciado mediante módem, se necesitará banda ancha. Para poder ser transmitido vía módem, se deberá reducir la resolución a 200 x 150 píxeles, el número de colores a 16 bits, el sonido a monofónico y el número de cuadros a 15 x segundo, esto obviamente depende del tipo de terminal donde se va a observar, por ejemplo, es diferente una configuración para un monitor de 15 pulgadas a un monitor de un PDA ó un teléfono celular.

El Codec (Compresor/Descompresor) son algoritmos matemáticos creados para permitir que los archivos multimedia estén en un formato para Streaming más pequeño para ser decodificado por el reproductor en el cliente. El software de codificación utiliza los codecs para comprimir el archivo. La descompresión ocurre durante el proceso de la reproducción en el cliente. Generalmente los codecs para streaming son procesos por software más que por hardware (vienen incluidos con el sistema operativo ó software de codificación de una plataforma de streaming específica)

La codificación en demanda se refiere al proceso explicito de codificar un archivo a un formato de streaming. La mayoría del software de codificación lleva plantillas incorporadas para hacer el trabajo más fácil; se escoge simplemente la plantilla que describe la audiencia y los codecs, tasas de bits y demás parámetros se definen automáticamente. La codificación en vivo es un poco más difícil que la codificación por demanda porque la entrada al codificador viene de tarjetas que capturan audio y vídeo dentro de la computadora de codificación.

2.5.5 MPEG (Moving Picture Experts Group)

Hacia los años 80 surgió la necesidad de compresión de imágenes digitales fijas de alta resolución con el fin de optimizar los recursos computacionales tanto de disco duro y en las transmisiones de imágenes a través de módems de baja velocidad, en esa época se adopto la norma del Grupo de Expertos Fotográficos Asociados ó Joint Photographic Experts Group (JPEG). Como recordamos que el video es una secuencia de imágenes digitales fijas, al poco tiempo, en 1998 se constituyó el Grupo de Expertos de la Imagen en Movimiento (Moving Picture Experts Group – MPEG) formalmente denominado como ISO/IEC-JTC1/SC29/WG11, que hasta la actualidad ha estado encargado de establecer las normas internacionales para codificar información de audio-video en un formato de compresión digital.

Inicialmente, hacia 1991 terminaron el estándar ISO 11172, conocido como MPEG1, cuyo formato es empleado principalmente para el almacenamiento de contenido multimedia, desarrollado como un estándar de compresión en medios fijos como Vídeo CD y CD-ROMs. La tasa típica de bits esta a 1.5Mbps, y es optimizado para trabajar con resoluciones de 352x240 pixels a 30 cuadros por segundo (NTSC) ó 352x288 pixels a 25 cuadros por segundo (PAL). Posteriormente, en el año 1994 apareció el estándar MPEG2, ó ISO/IEC-IS 13818, basado en un conjunto de circuitos integrados que presenta una tasa de bits más alto (de 2 Mbps a 8 Mbps) que MPEG1 para alcanzar la pantalla completa, y

es la base para el estándar de la televisión digital así como para el formato usado en video DVD.

El estándar MPEG3 se enfoco en aplicaciones a bajas tasas de bits para entrega inalámbrica, aunque presenta mayores características. Este grupo fue cerrado y los esfuerzos actuales se centran en el nuevo formato MPEG4, el cual promete gran variedad de usos. El inconveniente para codificación y entrega de MPEG1 es que para un adecuado nivel de calidad, requiere alta tasa de bits más altos que los actuales codecs. Para LANs corporativas ó redes multicast habilitadas esto no presenta mayor importancia, pero para streaming básico a través del celular ó en la web es difícil asegurar ó mantener una entrega constante de sus medios a más usuarios con menos retraso. En 1993, el comité del MPEG comenzó el desarrollo de MPEG4 como estándar para las aplicaciones multimedia. El comité de estándares también reconoció la necesidad de un esquema para una baja compresión de tasa de bits para manejar el creciente mercado de Internet. Por lo tanto, las tasas de bits son tan bajas como 10Kbps para el vídeo. Puesto que MPEG4 se basa en los mismos principios que sus precursores, puede alcanzar alta calidad, a pantalla completa, imágenes completas en movimiento tan altas como 10Mbps. Actualmente, MPEG4 es el algoritmo de codificación que compite con los codecs propietarios de Sorenson, RealNetworks y Microsoft en entrega de streaming media.

También existe una versión del MPEG llamado "MPEG-7", que es probablemente el estándar más ambicioso de metainformación para material multimedia. Representa el esfuerzo realizado por el comité MPEG de ISO para añadir descripción de contenidos a su lista de estándares desarrollados para el procesamiento de información multimedia, comenzada con MPEG-1, MPEG-2 y MPEG-4. Su objetivo se aparta de los estándares, que se ocupan principalmente de la representación del contenido (codificación), y añade una capa semántica por encima; por lo que depende de ellos (u otros estándares similares) para proporcionar acceso a los contenidos mismos.

MPEG-7 es un estándar reciente, la fecha oficial de publicación como Estándar Internacional (IS) es, para sus secciones más significativas, Octubre del 2001. Gracias a ello incorpora muchos avances recientes en tratamiento de la información multimedia. MPEG-7 se estructura alrededor del concepto de descriptor, una representación de una propiedad determinada de material audiovisual que caracteriza al contenido de alguna manera. Los descriptores se organizan en "esquemas de descripción", conjunto ordenado de componentes (descriptores u otros esquemas) con especificación de las relaciones entre ellos. Un grupo de esquemas de descripción aplicado a un contenido audiovisual forma la descripción de ese contenido.

Las descripciones se expresan en un lenguaje denominado "Lenguaje de Definición de Descriptores (DDL)", definido por MPEG, tomando como base el lenguaje XML del consorcio WWW. El lenguaje DDL permite también extensibilidad del estándar (en el nivel sintáctico) mediante su empleo para especificar descriptores y esquemas de descripción no previamente definidos.

Como todos los estándares producidos por MPEG, la especificación de MPEG-7 está orientada a un modelo de decodificador. Es decir, MPEG-7 detalla la sintaxis y semántica de las descripciones, de tal forma que cualquier decodificador acorde con la norma sea capaz de interpretar una descripción MPEG-7. Tanto lo que luego el decodificador haga con ella (filtrado, búsqueda, navegación ó acceso) como el método usado en el codificador para generarla no están especificados, dejando espacio para desarrollos ó mejoras posteriores, así como para la posibilidad de ofrecer valor agregado por parte de empresas que produzcan aplicaciones basadas en MPEG-7.

2.5.6 Diferencia entre un Streaming Server y un Web Server

Se puede hacer Streaming de contenidos con un servidor de streaming ó con un servidor web a un reproductor como Windows Media Player ó RealOne. Si se decide utilizar un servidor web, se tiene que ser conciente de las diferencias en la manera como se entrega el contenido, la cual puede afectar la calidad del "playback" del video.

El web server esta diseñado para enviar el mayor numero de datos que pueda enviar en un momento dado, este es el mejor método para enviar paquetes que contiene texto, imágenes estáticas, scripts de paginas web, pero no es el mejor método para enviar paquetes que contengan medios streaming. Los medios con Streaming se debe enviar en tiempo real, no en grandes ráfagas, y el player debe recibir paquetes justo antes de enviarlos. El servidor de streams mide el envío de paquetes de acuerdo al feedback de la información que el servidor recibe mientras envía el stream al player. Cuando el player recibe el paquete de esta manera, la presentación es mucho más continua. Dado que el uso del ancho de banda es controlado, se pueden conectar más usuarios concurrentes al sitio y pueden recibir los flujos libres de interrupciones.

Los servidores Web no soportan video de "multiple bit rate". Cuando se envía un stream desde un web server, la calidad de la entrega no es monitoreada, y no se puede hacer ajustes en la tasas de velocidad. Los servidores Web no pueden utilizar el protocolo UDP, por lo tanto el envío del stream seguramente será interrumpido por periodos de silencio mientras que el player hace el "buffering" de datos. No es posible hacer streaming en vivo y multicasting con un servidor Web.

2.5.7 Consideraciones acerca de la tecnología GSM/GPRS.

Las redes GSM/GPRS presentan una problemática especial que, en general, no permiten la difusión de video con la arquitectura cliente-servidor. La cuál se describe a continuación:

- **Redes GSM**

  Al ser una conexión por circuitos, la calidad de servicio, si no garantizada, sí se mantiene a muy buen nivel. El retardo en la transmisión de datos es habitualmente menor de 1 segundo. El problema es el bajo ancho de banda ofrecido.

- **Redes GPRS**

  Es una conexión de paquetes en la que por el momento no se ofrece garantía de calidad de servicio. El ancho de banda es variable, así como el retardo de transmisión.

No obstante, realizando algunas configuraciones en los codificadores, por ejemplo, habilitando diferentes tipos de distribución, se permitiría brindar servicios de streaming a usuarios, que por limitación de recursos de red del operador celular ó del teléfono, solo pudieran acceder al servicio utilizando un reducido ancho de banda.

Si bien es cierto que existen diversas clases de esquemas de codificación (CS1, CS2, CS3 y CS4) que permitirían tener anchos de banda altos en GPRS. Estos últimos casi nunca fueron desarrollados por los proveedores de tecnología celular puesto que prefirieron desarrollar directamente la tecnología de tercera generación EDGE el cual permitiría tener un mayor ancho de banda que GPRS y aseguraría una mejor calidad de servicio para este tipo de aplicaciones.

CAPITULO III
SOLUCION PROPUESTA

El presente capitulo abarca el diseño y la implementación de la solución propuesta implementado en la red GSM/GPRS. Este sistema permite la captura y codificación de videos originalmente análogos, el procesamiento para la digitalización de la señal, el almacenamiento en el servidor de streaming para finalmente implementar una aplicación que permita visualizar la información audiovisual almacenada en los servidores de streaming desde los teléfonos GSM/GPRS/EDGE ó podría ser también desde Internet.

El diseño propone una página WAP para el acceso al servicio, esto permite tener un manejo más rápido y amigable, puesto que no será necesario realizar algunas configuraciones que pudieran ser muy tediosas para usuarios que no tienen un conocimiento técnico sobre estos temas. Esta investigación solamente contempla una solución usando tecnología GSM/GPRS/EDGE y no la tecnología CDMA1X.

3.1 Productos y Soluciones para Streaming

Antes de empezar a explicar el diseño de la solución, se introduce a continuación 03 productos que básicamente son los líderes del mercado en soluciones de streaming: QuickTime de Apple, RealNetworks y Microsoft Windows Media. Estos tres son en sí arquitecturas ó formatos de plataformas. Una arquitectura es un paquete de software que permite que los datos sean intercambiados en un formato estándar, que es utilizado para que la máquina del cliente interprete el archivo comprimido.

Un gran problema de tener múltiples tecnologías de streaming de audio ó video es la proliferación de plataformas incompatibles. Se tendrían que instalar algunas aplicaciones y plug-ins diferentes para poder ver y escuchar todos los formatos que existen en la Web.

3.1.1 RealNetworks

La tecnología Real System está compuesta por una familia de productos software que permiten implementar sistemas comerciales de streaming. Los tres productos en los que se fundamenta esta tecnología son:

RealServer: Es el componente software más importante del sistema de retransmisión streaming. Su funcionamiento es análogo al de un servidor WWW: se ocupa de almacenar contenidos multimedia y servirlos a través de la Red a los usuarios que deseen acceder a ellos.

RealPlayer: Es el componente software que emplea el usuario para reproducir los contenidos multimedia. Es gratuito, y está ampliamente distribuido en Internet. Se puede descargar en pocos minutos desde la página de RealNetworks.

RealProducer: Es el software que se emplea para codificar la información multimedia (audio y video) al formato RealMedia, generando bien un archivo para almacenarlo en un servidor RealServer ó bien enviarlo en forma de stream para que éste lo retransmita en directo por toda la red.

A partir de septiembre de 2002, RealNetworks ha sacado al mercado una plataforma nueva llamada Helix, la cual incorpora todos los formatos de codificación y reproducción de la plataforma Windows Media Series además de comenzar a incorporar formatos estándares nativos como el MPEG-4.

Ventajas del RealSystem

- Emplea esquemas de compresión muy eficientes que permiten reducir el elevado volumen de datos que genera una transmisión de audio ó video para que pueda ser reproducida.
- Hace uso de nuevos protocolos de aplicación que permiten monitorear dinámicamente la calidad de la conexión y controlarla de modo que la recepción sea de la mayor calidad posible.

- Incorpora diferentes plug-ins que son capaces de funcionar con diferentes formatos de archivos multimedia, entre los que se encuentran los más utilizados (MOV, AVI).
- Incorpora la tecnología ¨SureStream", que permite modificar en tiempo de reproducción los parámetros de la conexión, ajustándose dinámicamente a la calidad de la conexión.

3.1.2 Windows Media Technologies de Microsoft

Windows Media Services es un servicio que viene con el sistema operativo Windows 2000 Server, el cual sirve para controlar, monitorear las propiedades del servidor de streaming. La tecnología de Windows Media tiene unas herramientas que se pueden utilizar para crear y manejar contenidos ASF (Advanced Streaming Format) para Windows Media Services.

Microsoft utiliza un protocolo propietario llamado: Media Server Protocol (MMS) a diferencia de Real Networks y Quicktime de Apple que utilizan el protocolo RTP/RTCP y RTSP. Windows Media Tech utiliza una serie de módulos para realizar la difusión: módulos como Windows Media Tools, las cuales son un conjunto de herramientas para la producción de streams; el servidor de streams, el cual viene con Windows 2000 Server conocido como Windows Media Services y el reproductor conocido como Windows Media Player.

Al igual que RealNetworks, Microsoft a finales del 2002 ha liberado la nueva generación de streaming conocida como Series 9 ó versión 9. Aunque sigue siendo propietaria de Microsoft, incorpora elementos avanzados para la distribución de contenido multimedia.

3.1.3 Quick Time

Quicktime es desarrollado por Apple y es una arquitectura de plataforma cruzada simple para Macintosh y Unix. Utiliza el formato MOV. Apple adoptó la tecnología ¨Sorenson Video technology¨ para la compresión de audio y video.

Los codecs y el player de Quicktime están disponibles gratuitamente en la Web. El Quicktime Streaming Server fue lanzado en 1999 como un software open-source y

basado en el protocolo RTP/RTSP. Este es un estándar abierto que puede ser utilizado en servidores multi-plataforma como UNIX ó NT, además es gratuito. El Quicktime Streaming server está diseñado para trabajar con Mac OS Server, pero también se encuentra disponible el servidor de código fuente llamado Darwin Server. Hay versiones disponibles para Linux, Solaris y Win NT/2000.

Quicktime trabaja bien con la mayoría de formatos de imágenes incluyendo JPEG, BMP, PICT, PNG, GIF y GIF animados. También toca archivos MP3 y soporta MIDI, que es el formato clásico de la música por Web. Además soporta el estándar SMIL Synchronized Multimedia Integration Language con un formato de metadatos. Los documentos SMIL organizan los tiempos y capas del contenido Multimedia, incluyendo imágenes, texto, audio y video. Quicktime tiene una característica llamada ¨Movie Alternates¨ que permite a los desarrolladores producir múltiples versiones de una película. Quicktime soporta diferentes tipos de formatos digitales de video como AVI, AVR, MPEG1 y formatos de cámaras camcorders: OpenDML, MiniDV, DVCPro and DVCam.

3.2 Diseño

El diseño que se propone para la implementación de una solución de TV Móvil esta basado en las plataformas de RealNetworks. Esto debido a que algunos proveedores de teléfonos celulares tales como: Nokia, Siemens, SonyEricsson y algunos proveedores de PDAs han implementado el cliente RealPlayer dentro de sus menús de opciones. Aunque también existen algunos teléfonos específicos que tienen instalado los clientes de Windows Media dentro de sus menús de opciones, llamados SmartPhone, estos aún no están siendo comercializados en el mercado peruano. Existen también algunas PDAs, por ejemplo las IPAQ de HP, que también soportan los clientes de Windows Media asi como el Real Player.

Las aplicaciones que pueden ser implementadas utilizando el diseño propuesto pueden también ser utilizadas para difundir contenidos multimedia, tales como contenido de entretenimiento (Música y TV), noticieros, capacitación, mensajes corporativos, soporte a

clientes, campañas publicitarias, etc, mediante una transmisión en difusión ó bajo demanda, ó también utilizado para aplicaciones de vigilancia remota en los hogares, colegios, clubes de niños hasta en pequeñas empresas.

Específicamente a través del diseño propuesto, también se pueden recibir contenido de la siguiente manera:

- Bajo demanda: contenidos previamente almacenados en el servidor de streaming, los cuales se podrán ver las veces que el usuario quiera, por ejemplo, un resumen semanal del noticiero, ó los goles del descentralizado de fútbol, etc.
- Tiempo Real: contenido generado en vivo, por ejemplo, el servicio TV Móvil lanzado el año pasado por TIM Perú.

3.2.1 Acceso al Servicio

Para el acceso al servicio, es posible entrar directamente a través de escribir la ruta completa del canal específico (éste siempre empieza con "rtsp://…"). Con el objeto de dar una mayor facilidad al usuario, se implemento una página Wap de tal forma que sirva como un "Control Remoto de Televisión", donde el usuario solo tendría que hacer click en la pantalla del celular para que le aparezca el canal de televisión deseado. Además que algunos proveedores de celulares implementaron en sus telefónos el cliente RealPlayer en una versión limitada, es decir, no se podría abrir un archivo desde esos terminales y solo se permitía usar el aplicativo para visualizar archivos previamente descargados en el terminal.

Desarrollo de la Página Wap

Debido a las limitaciones en los recursos que se tienen del teléfono celular se propone que la página Wap sea lo más sencilla posible. Si bien es cierto que usando la misma página HTML (de acceso por Internet) se puede también utilizar para acceder vía celular, podrían existir algunos banners u otras propagandas que no serán vistas por el teléfono celular debido a que el Wap GW los ha filtrado previamente. Generalmente, cuando el WAP GW realiza la traducción desde HTML a WML, éste filtra los campos que no logra

traducir y no los envía hacia el celular, dando como consecuencia que la página que el usuario ha accedido sea diferente a lo que realmente se ha implementado.

3.2.1.1 Niveles de Seguridad

En particular, para este servicio no es necesario implementar un sistema de seguridad que permita proteger la información transmitida, puesto que la información es pública y puede ser vista por cualquier televisor. Esto variará si la aplicación hubiera sido para vigilancia de hogares ó control de niños, en este caso, una de las preguntas más frecuentes al utilizar estos tipos de servicios, se refiere a la seguridad de la información, preguntas como: Si algún otro usuario puede conectarse a la cámara de su casa ó colegio ó empresa?, Que pasaría sí clonan mi teléfono?, Que pasaría si alguien intenta "interceptar" mi información?, existe algún tipo de sistema que pueda protegerme?. A continuación se dan algunas recomendaciones para responder a las dudas planteadas anteriormente:

- Para el caso de empresas (hospitales, colegios, compañías, etc.) se propone configurar APNs (Nombres de punto de acceso) propios en la plataforma GGSN de la red GPRS y restringir el tráfico entre diferentes APNs, de tal forma que solo los usuarios que se encuentren definidos en dicho APN puedan acceder al servidor de streaming específico por cada empresa.
- Para el caso de los usuarios, es casi imposible que el operador celular pueda definir un APN por cada usuario, por lo tanto, se propone que la seguridad debe estar basada en la capa de aplicación. Es decir, a través del servidor Web ó Wap, se implemente un proceso previo de autenticación a nivel de usuario, para lo cual solamente los usuarios que ingresen con el usuario y contraseña correctos puedan acceder al servicio de videostreaming.
- Acerca de la clonación y la interceptación, el estándar GSM/GPRS ha desarrollado desde sus inicios algoritmos de autenticación A3/A8 y de cifrado A5/X, que no permiten la clonación ó interceptación desde usuarios fraudulentos. Existe una

asociación de operadores y proveedores de tecnología celular denominado la GSM Association que informa si han existido casos al respecto.

- Sobre el punto anterior, los algoritmos de cifrado en la red GSM/GPRS se dan solamente en la interfase aire, aunque existen algunos equipos especiales que permiten una comunicación segura punto a punto, éste no será el caso de estudio de esta investigación puesto que el objetivo es tener una mayor cantidad de clientes con los teléfonos convencionales.
- Para lograr un cifrado hasta los servidores de las empresas se propone implementar redes privadas virtuales (llamadas también VPNs – Virtual Private Network) entre los FWs de la operadora celular y el FW de salida de la empresa. Otra forma más segura, pero a la vez más costosa es la implementación de circuitos dedicados entre estos puntos.

3.2.2 Generación del Contenido

El proceso de generación de contenidos esta basada principalmente en las 04 fases definidas en la cadena de valor de los servicios de videostreaming, es decir las fases de creación, producción, distribución y consulta.

Es importante señalar que con este diseño es posible tener dos tipos de contenido: contenido generado en vivo, por ejemplo, el servicio TV Móvil, y también contenido bajo demanda, es decir contenido previamente almacenado en los servidores.

En la siguiente figura se muestran las cuatro fases para generar cualquier tipo de contenido multimedia:

Figura 3.1 Fases para la Generación de Contenidos Multimedia

Fase 1

En esta fase se captura el vídeo ó sonido de modo que se pueda convertir posteriormente en streaming. Para esta fase se propone utilizar tarjetas capturadoras, por ejemplo tarjetas Pinnacle que aparte de capturar vídeo y sonido también tiene un sintonizador de televisión el cuál se utiliza para capturar el contenido de los canales de televisión. Existen algunos tipos de contenido (la animación, por ejemplo) en los que no hay representación, únicamente los dibujos que se crean. La idea sin embargo es la misma, es decir, los originales se capturan en el sistema de modo que puedan convertirse posteriormente en streaming.

Fase 2

Después de capturar la información se deberá editar para que el contenido que se distribuya a los usuarios sea lo que realmente se desea mostrar.

En esta fase se propone crear diferentes audiencias dentro del software de Helix Producer, de tal forma de diferenciar los accesos para los distintos tipos de celular, por ejemplo, los que soporten EDGE se les configuraría una audiencia que pueda requerir mayores anchos de banda y mejor resolución en comparación a los teléfonos que

soporten solamente GPRS ó HSCSD. Un aspecto adicional es el de verificar cuáles serían los formatos que los teléfonos celulares soportan para que estos perfiles puedan ser configurados dentro de las audiencias. En la siguiente figura se muestra un ejemplo de la creación de una audiencia:

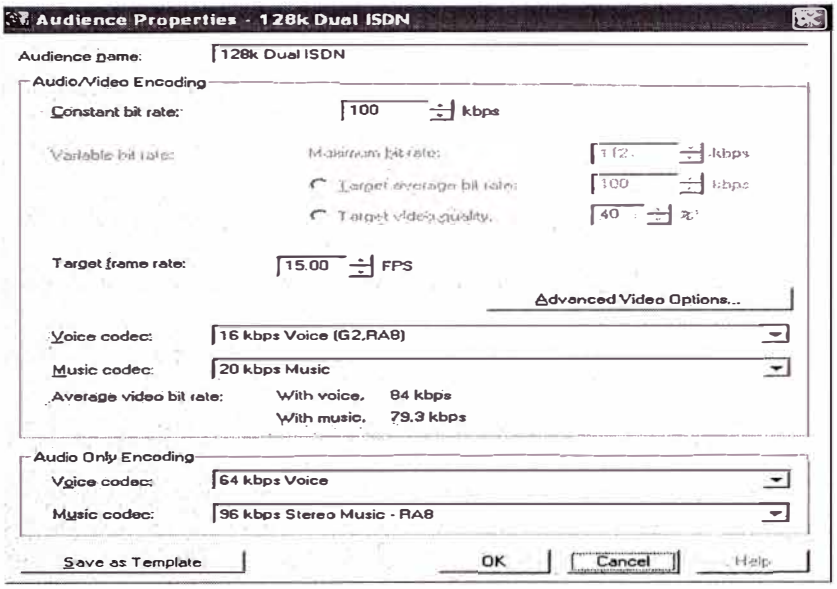


Figura 3.2 Configuración de las Audiencias

Se debe tener especial atención en los siguientes parámetros:

- Ancho de Banda
- Frames por segundo, y
- Codificación del audio y video.

puesto que colocar cualquier valor sin considerar las limitaciones que se tiene en una red celular GSM/GPRS/EDGE ó los formatos soportados por el teléfono (supuestamente para darle una mejor calidad al vídeo) podría ocasionar que los reproductores utilizados en estos teléfonos celulares no puedan abrir el contenido solicitado, ocasionando posibles molestias a los usuarios.

A su vez, para la implementación del servicio se propone no solo configurar distintas audiencias para el acceso por la red celular, sino también crear audiencias dentro del mismo rango de ancho de banda soportado en las redes celulares, de tal forma que cuando un usuario acceda para ver un contenido específico y no tenga recursos en la red,

pueda acceder a la audiencia de menor ancho de banda de forma tal de reducir los posibles cortes que podrían generarse si es que se implementa solamente una audiencia con ancho de banda alto (promedio 40 kbps), ya que al reducirse los recursos de canales disponibles en la red celular, se utiliza la información que hay en el buffer, de modo que se puede aguantar un poco ese descenso. Si la comunicación se corta demasiado tiempo, el buffer se vacía y la reproducción se interrumpe hasta que se restaurase la señal.

Fase 3

La presentación editada se codifica como flujo en base a las propuestas y recomendaciones explicadas en la Fase 2. Una vez codificado, el archivo está preparado para ser enviado vía streaming.

Fase 4

El archivo codificado se coloca en el Servidor para que los clientes puedan reproducirlo. Las emisiones en vivo se tratan de la misma manera. Al igual que la televisión en directo, las representaciones ó los eventos se retransmiten mediante cámaras y/o micrófonos y se convierten en directo a un formato que se puede enviar tan sólo unos segundos más tarde.

3.2.3 Implementación del Sistema de Métricas

Una vez implementado el servicio de videostreaming es necesario considerar herramientas que permitan no solo monitorear la calidad del servicio que se esta ofreciendo sino también considerar otros factores, como por ejemplo: el interés que despiertan determinados contenidos, evaluar la evolución del servicio ó la eficiencia del servicio.

Todas estas métricas son explicadas en el siguiente capítulo, pero se describe a continuación la propuesta de arquitectura de implementación del sistema de métricas.

3.2.3.1 Descripción del Sistema de Métricas

El sistema de métricas propuesto pretende ser un instrumento capaz de generar de forma automática informes que pudieran ser utilizados por los gestores del servicio como base para la configuración del mismo.

El sistema recoge los logs de los servidores desde los que se provee la información (Helix Server), los debe procesar y generar la información necesaria para observar la evolución de numerosos parámetros del sistema. Además de métricas clásicas como la evaluación del número de accesos y su distribución horaria, el sistema también debe mostrar los resultados de las métricas presentadas en el siguiente capítulo, como el análisis del impacto de un vídeo, la evolución del servicio, la calidad en la transmisión del vídeo, etc. Los resultados pueden ser generados en formato tipo texto para ser introducidos en otras herramientas y simuladores y en formatos gráficos a través de un conjunto de páginas Web.

3.2.3.2 Arquitectura del Sistema de Métricas

Esta arquitectura podría estar compuesta por varios módulos, cuyo elemento central sería una base de datos que almacena la información extraída de los logs de los servidores a los cuales se está supervisando. La base de datos se carga con información mediante dos módulos de adquisición dependiendo del tipo de carga, en línea "on-line" ó fuera de línea "off-line". Esto permitiría una actualización constante de la información. El gestor de base de datos podría ser MySQL, SQL Server, Oracle, etc. El sistema podría presentar la información de la base de datos a través de un servicio Web ó mediante un archivo de texto.

3.2.3.3 Proceso de Carga

El sistema de análisis permite dos modos de carga de la base de datos. El primero de ellos es la carga en línea ó on-line. Este método solamente es posible usando el servidor de streaming "Helix Universal Server". Mediante la utilización de un socket es posible

recibir la información sobre los accesos de los usuarios según se van produciendo. Este modo de carga hace que el sistema de análisis disponga de información actualizada en todo momento.

Otro método de carga es el modo fuera de línea ó off-line, que también es posible utilizarlo a través del acceso al directorio "Logs" de la plataforma Helix Universal Server. La información obtenida a partir de los logs de los servidores es variada e incluye elementos como la dirección IP del cliente, identificador único del reproductor del cliente, instante de realización de la petición, bytes enviados, tiempo de vídeo transmitido, paquetes enviados, paquetes reenviados, ancho de banda medio consumido, etc.

La arquitectura propuesta se presenta en la siguiente página:

Arquitectura del Sistema de Métricas

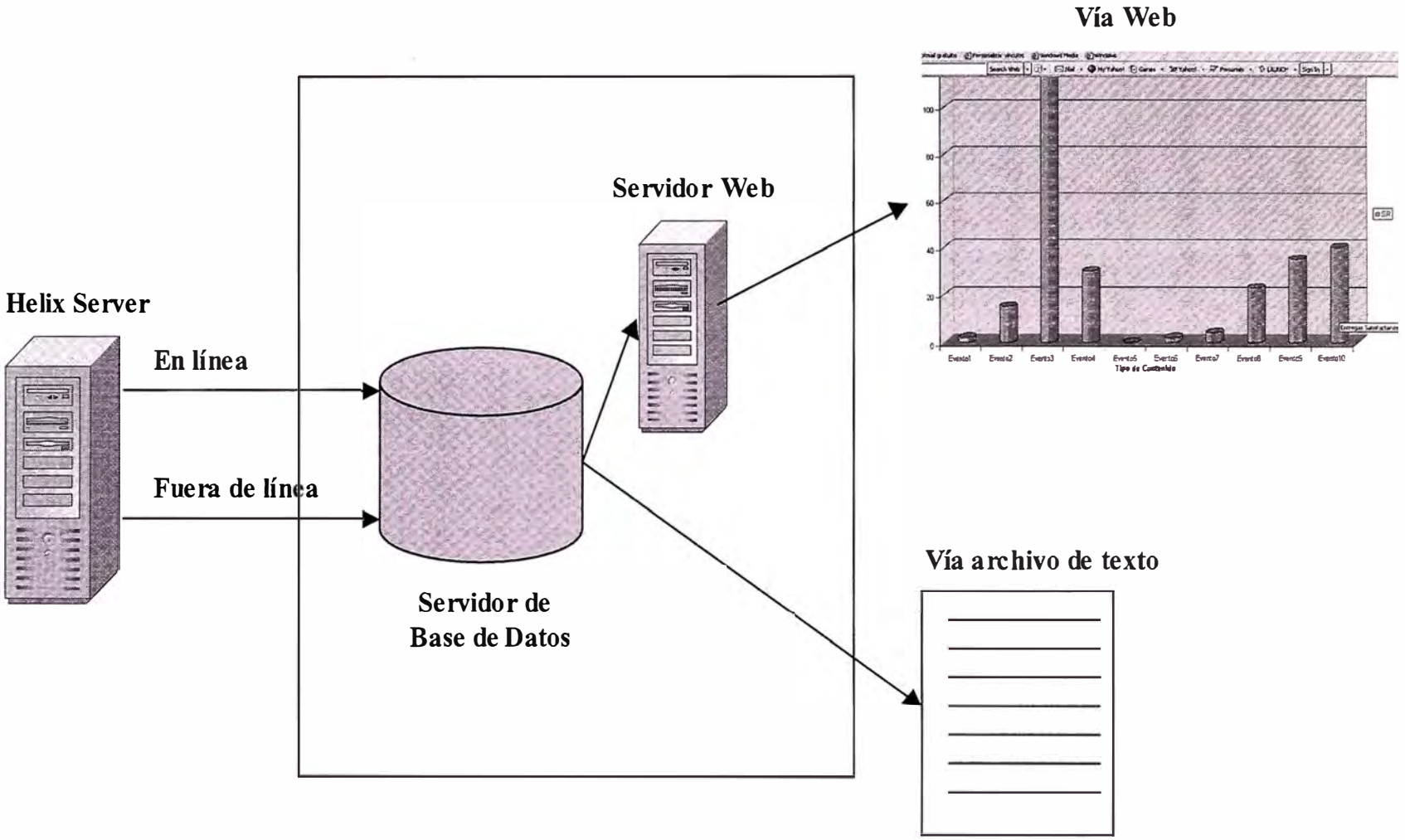


Figura 3.3 Arquitectura del Sistema de Métricas

3.3 Arquitectura

La arquitectura de solución para implementar un servicio de videostreaming, en particular el servicio de TV Móvil, se basa en utilizar un servidor central (podrían haber más de uno por motivos de redundancia) de tal forma que soporte el tráfico de todos los Producer´s (generalmente un servidor por Producer, pero existen servidores que pueden soportar más de uno).

No es necesario que los Producer´s y el Servidor se encuentren ubicados en la misma localización física, si no fuera el caso, la conectividad entre éstos puede ser usando los enlaces de Internet ó a través de líneas dedicadas. Para este caso, se recomienda usar Redes Privadas Virtuales (VPN) a través de Firewalls que permitirían proteger la información ante posibles ataques ó intrusiones.

La configuración para los usuarios, a nivel de registro en el HLR y en el GGSN de la red GSM/GPRS/EDGE del operador celular, sería usando direcciones privadas para sus usuarios y configurando un APN específico para este servicio. La ventaja de tener un APN diferente es la de darle mayor seguridad al servicio, puesto que solamente los usuarios que tengan provisionado este APN podrán acceder a la aplicación, a su vez, en el FW se podría configurar para que solamente se permitan utilizar los puertos utilizados en el aplicativo. Otra de las ventajas, desde el punto de vista del usuario, es que el operador podría utilizar este APN para diferenciar y tener mayor flexibilidad en las tarifas y por ende ofrecer mayores ofertas.

Sobre el acceso a la página WAP, que vendría a ser el Control Remoto de Televisión, podría ser implementado en un servidor dedicado, pero debido a que solamente realiza una redirección hacia el aplicativo de streaming, éste se podría cargar en el mismo servidor central de videostreaming, puesto que no consume muchos recursos en el servidor.

La siguiente figura muestra el diseño de la arquitectura:

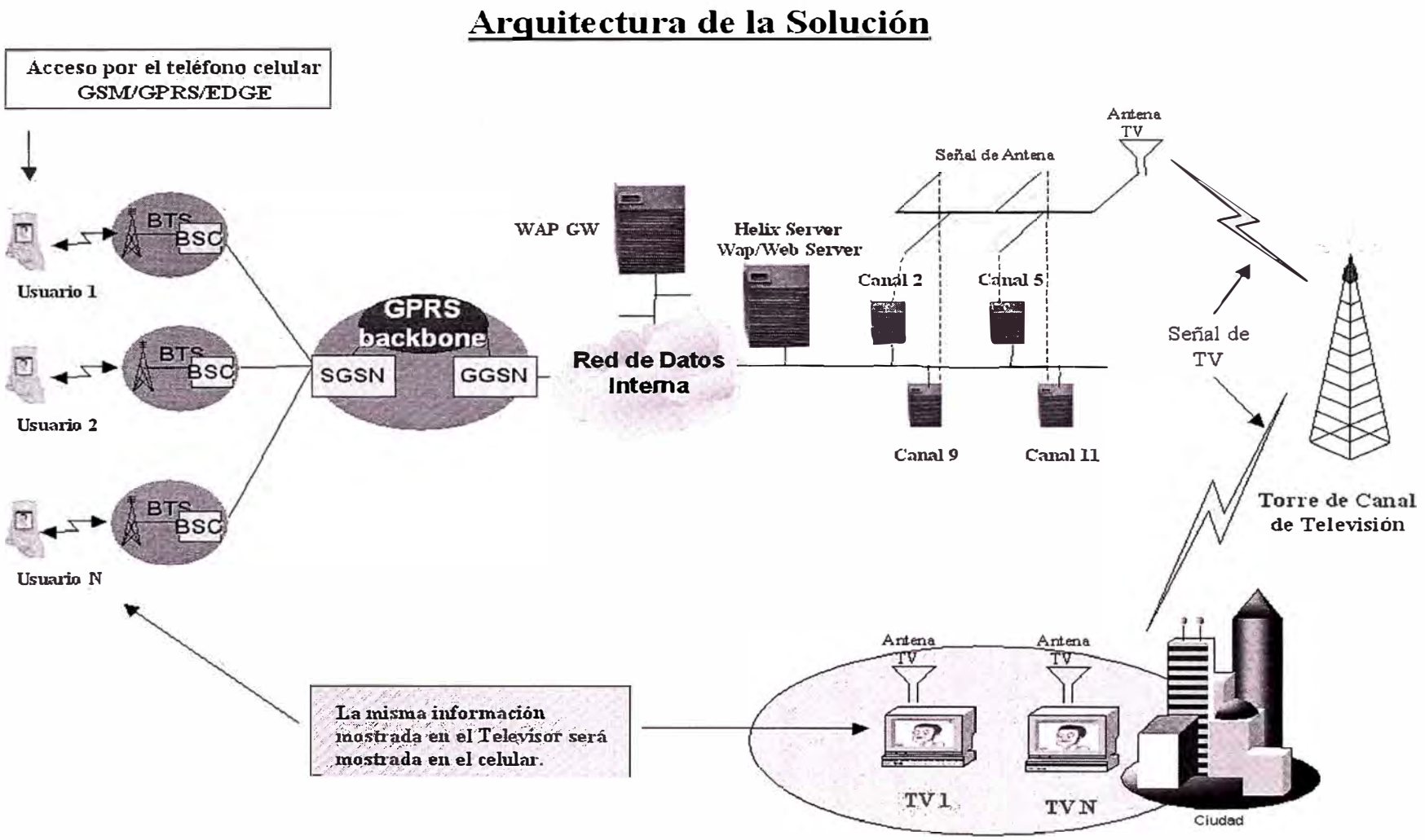


Figura 3.4 Propuesta de Arquitectura de la Solución

3.3.1 Diagrama de Flujo del Servicio

A continuación se mostrará el diagrama de flujo a través del acceso móvil que ha diferencia del acceso por Internet, cuya diagrama es demás conocida, se pretende responder a las preguntas relacionadas al Ancho de Banda, Seguridad, Canales disponibles, etc., que ayudarán a entender mejor la integración de aplicaciones de videostreaming sobre una red celular.

A continuación se describe el flujo del servicio:

Procedimiento de Registro en la Red GPRS

1. La estación móvil (MS) inicia el procedimiento de registración del móvil a la red GPRS (Attach). El Requerimiento de Attach (Attach Request – que contiene entre otros parámetros el IMSI, el PTMSI y el Classmark) es enviado al BSC y luego al SGSN que esta siendo servido por el móvil. La unidad del SGSN que se encarga de manejar este mensaje es la PAPU (Packet Processing Unit), que vendría a ser la interfase entre la red de datos GPRS y la interfaz aire. El Classmark contiene las capacidades de multislot que soporta la estación móvil y también el algoritmo de cifrado que es soportado en GPRS.
2. Si el móvil se ha trasladado entre un SGSN a otro, el nuevo SGSN interrogará al anterior para obtener la identificación del usuario a través del mensaje "Identification Request". En cambio, si el móvil es encendido por primera vez, entonces la PAPU del SGSN que está cubriéndolo, interrogará directamente a la estación móvil MS enviándole el mensaje de requerimiento de identidad, obteniendo luego el IMSI del móvil.

Procedimiento de Autenticación

3. Luego se realiza el proceso de autenticación, el cuál es enviado por la PAPU a través del mensaje "Send Authentication Info" al SMMU (Signalling and Management Unit) con el objetivo de recibir las tripletas de autenticación. El SMMU es la unidad del

SGSN cuya finalidad es el soporte de la movilidad de las estaciones móviles, llamado también Subscriber Mobility Management.

Esta unidad es la que se conecta con la red GSM a través de los enlaces de señalización número 7, utilizando las siguientes interfases: Gr (HLR-SGSN) Gd (SMS-GMSC-SGSN), Gs (MSC/VLR-SGSN) y Gf (EIR-SGSN) que conecta el SGSN a diferentes elementos de red. El SMMU soporta los protocolos MTP, SCCP, TCAP, BSSAP+ y MAP.

Luego que la PAPU envía el mensaje de "Send Authentication Info" al SMMU, podría darse el siguiente escenario:

- Si el SMMU no tiene previamente almacenado las tripletas de Autenticación, este envía el mensaje MAP "Send Authentication Info" al HLR/AuC.
- El HLR/AuC responde con el mensaje MAP "Send Authentication Info Ack" incluyendo las tripletas de autenticación (RAND, SRES y Kc).

Este último mensaje, que incluye las tripletas de autenticación, es enviado desde el SMMU a la PAPU a través de un protocolo propietario que depende del proveedor.

4. La PAPU envía el mensaje "Authentication and Ciphering Request (RAND, CKSN, Ciphering Algoritm) a la estación móvil. La estación móvil MS responde con un mensaje "Authentication and Ciphering Response (SRES)". Luego la PAPU compara el SRES recibido por la estación móvil con el contenido en las tripletas de autenticación.

   La estación móvil empieza el cifrado "ciphering" luego que éste envía el mensaje "Authentication and Ciphering Response", la PAPU empieza el Ciphering luego que recibe una respuesta válida de la estación móvil. Este procedimiento asegura la integridad de la información que se transmite sobre el aire.

Procedimiento de Verificación de IMEI

5. Luego se realiza el procedimiento de verificación de la identidad del usuario ó llamado también "Identity Check Procedure". La PAPU envía el mensaje "Identity Request" a la estación móvil MS, luego el MS responde con el mensaje "Identity Response" incluyendo el IMEI del usuario.
6. Si la PAPU decide verificar el IMEI, entonces éste interrogará al EIR enviando el mensaje "Check IMEI" al SMMU. El SMMU enviará el mensaje tipo MAP "IMEI Check" al EIR y éste verificará su estado en su base de datos. El estado de la verificación del IMEI "Check IMEI" será enviada al SMMU. El EIR es básicamente una base de datos que clasifica los IMEI's en tres listas:
    - Blanca: no tiene ninguna restricción.
    - Negra: se les impide el acceso a la red.
    - Gris: degradan la calidad de la red, pero no lo bastante como para impedir que sean utilizados.

Procedimiento de Actualización de Localización

7. Luego se realiza el procedimiento de actualización de localización ó también llamado "Location Update" al HLR. El SGSN a través del módulo SMMU envía el mensaje tipo MAP "Update GPRS Location" incluyendo algunos parámetros como el: IMSI, SGSN Number y SGSN Address hacia el HLR. Donde el SGSN Address es la dirección IP del SGSN. Para encontrar el HLR donde se encuentra definido el usuario, el SMMU deberá ejecutar el procedimiento de análisis de IMSI ó también llamado IMSI análisis.
8. Si el usuario estuvo previamente registrado en otro SGSN, entonces el HLR envía el mensaje tipo MAP "Cancel Location" al antiguo SGSN/SMMU con el propósito de borrar este registro.
9. El HLR envía el mensaje tipo MAP "Insert Subscriber Data" incluyendo algunas características del registro del móvil, como el IMSI y el GPRS subscription data al nuevo SGSN/SMMU.

10. El HLR envía la confirmación de actualización en el mensaje "Location Update" hacia el nuevo SGSN/SMMU .
11. Luego la PAPU envía el mensaje "Attach Acept" hacia la estación móvil, indicando que el procedimiento de registro del móvil a la red GPRS ha sido aceptado satisfactoriamente.
12. Por último, la estación móvil MS envía el mensaje "Attach Complete", con el que se termina todo el proceso de registro del móvil en una red GPRS.

Procedimiento de Activación del Contexto PDP

Una vez registrado el móvil en la red GPRS, éste podría acceder en cualquier momento a los servicios de datos que el operador haya provisionado al usuario.

Asumiendo, que después de cierto período de tiempo, el usuario desee acceder al servicio de streaming, el procedimiento será el siguiente:

13. La estación móvil envía un mensaje a la PAPU denominado "Activate PDP Context Request" incluyendo algunos parámetros tales como:
    - NSAPI (Network Service Access Point), que identifica la asociación entre el Contexto y la Dirección del PDP (Packet Data Protocol). El NSAPI es parte del identificador de túnel (TI – Túnel Identifier) entre el SGSN y el GGSN.
    - TI, representa la identificación de la transacción.
    - PDP Type, indica el tipo de protocolo que la estación móvil podría usar: IPv4 ó IPv6.
    - PDP Address, indica si la estación móvil requiere el uso de una dirección estática ó dinámica.
    - APN (Access Point Name), se refiere a la red de datos externa que el usuario desea conectarse.

Procedimiento de Autenticación

14. Luego se realiza el proceso de autenticación, el cuál es enviado por la PAPU a través del mensaje "Send Authentication Info" al SMMU (Signalling and Management Unit)

con el objetivo de recibir las tripletas de autenticación. Luego que la PAPU envía el mensaje de "Send Authentication Info" al SMMU, podría darse el siguiente escenario:

- Si el SMMU no tiene previamente almacenado las tripletas de Autenticación, este envía el mensaje MAP "Send Authentication Info" al HLR/AuC.
- El HLR/AuC responde con el mensaje MAP "Send Authentication Info Ack" incluyendo las tripletas de autenticación (RAND, SRES y Kc).

15. La PAPU envía el mensaje "Authentication and Ciphering Request (RAND, CKSN, Ciphering Algoritm) a la estación móvil. La estación móvil MS responde con un mensaje "Authentication and Ciphering Response (SRES)". Luego la PAPU compara el SRES recibido por la estación móvil con el contenido en las tripletas de autenticación. La estación móvil empieza el cifrado "ciphering" luego que éste envía el mensaje "Authentication and Ciphering Response", la PAPU empieza el Ciphering luego que recibe una respuesta válida de la estación móvil.

Procedimiento de Verificación de IMEI

16. Luego se realiza el procedimiento de verificación de la identidad del usuario ó llamado también "Identity Check Procedure". La PAPU envía el mensaje "Identity Request" a la estación móvil MS, luego el MS responde con el mensaje "Identity Response" incluyendo el IMEI del usuario.
17. Si la PAPU decide verificar el IMEI, entonces éste interrogará al EIR enviando el mensaje "Check IMEI" al SMMU. El SMMU enviará el mensaje tipo MAP "IMEI Check" al EIR y éste verificará su estado en su base de datos. El estado de la verificación del IMEI "Check IMEI" será enviada al SMMU.

Selección de APN

18. Si el proceso de seguridad (autenticación, cifrado y verificación de IMEI) es satisfactorio, entonces la PAPU validará el PDP Type, el PDP Address y el APN provisto por la estación móvil y almacenará en la base de datos de usuarios visitantes

localizado en el SMMU. Si la estación móvil no especifica un APN, entonces la PAPU deberá seleccionar una por defecto.

19. Luego la PAPU enviará al GGSN respectivo el siguiente mensaje GTP "Create PDP Context Request" incluyendo algunos parámetros como: PDP Type, PDP Address y APN).
20. Luego el GGSN crea una entrada en su tabla de PDP Context con el IMSI, NSAPI, PDP Type, PDP Address y APN y creará un Charging ID (para própositos de facturación). Esta nueva entrada en la tabla permite al GGSN el enrutamiento de paquetes de datos entre las redes externas y la PAPU. Si el GGSN acepta el PDP Context entonces responde el siguiente mensaje GTP "Create PDP Context Response) hacia la PAPU.
21. La PAPU crea un PDP Context en su memoria para ese usuario conteniendo algunos parámetros tales como: NSAPI, GGSN Address y TI. Si la estación móvil ha requerido una dirección dinámica, ésta dirección será incluida dentro del mensaje PDP Context. Esto permite a la PAPU enrutar el tráfico de paquetes de datos entre el GGSN y la estación móvil.

Procedimiento de Acceso vía WAP

Una vez obtenida la dirección IP y permitido el acceso a la red externa a través del GGSN, los paquetes serán transmitidos directamente desde el móvil hacia los servidores de datos externos. A continuación se muestra el diagrama de flujo en esta fase:

22. El usuario ingresa al menú de WAP de su teléfono y solicita la URL del servidor de aplicaciones. El navegador WAP del teléfono crea una petición que contiene la URL y la información que identifique al usuario y las envía al WAP GW vía el GGSN. Entonces, el GGSN realizará primeramente la autenticación usando el Radius para verificar si el usuario tiene acceso al servicio específico.
23. El Radius confirma que el usuario esta autenticado.

24. Luego, el Radius envía los datos al WAP GW indicándole la dirección IP y el MSISDN asociados al móvil.
25. El GGSN transfiere la información del móvil hacia el WAP GW.
26. El WAP GW interpreta la petición, genera una petición convencional http ó http secure (https) y la envía al servidor Web/Wap. El servidor Web interpreta a su vez la petición y determina que recuperar. Si la URL especifica un archivo estático, el servidor Web lo recupera. Si la URL especifica un programa CGI, el servidor Web inicia el programa. El Servidor Web coloca un encabezado http ó https en el archivo estático ó programa CGI y lo envía de nuevo al WAP GW.
27. El usuario observará en su pantalla la página WAP solicitada.

Procedimiento de Acceso y Distribución al servidor de Streaming

Una vez que los usuarios entran a la página WAP (Control Remoto de Televisión), existirá un enlace que hará una redirección hacia el servidor de streaming. El flujo de acceso y distribución se muestra a continuación:

28. Usuario ingresa a la página WAP donde está localizado el enlace para ver el streaming.
29. El WAP GW convierte y envía la información al servidor WAP.
30. El móvil ingresa al enlace de streaming y envía un requerimiento de broadcast al Helix Server.
31. El servidor envía los paquetes al móvil, él cual empieza a decodificarlo y mostrarlo en la pantalla del terminal

Por otro lado, el flujo de información entre el Helix Producer y el Helix Server se muestra a continuación:

30a. El Helix Producer establece una conexión inicial con el Servidor de Streaming. Con esta conexión, el Helix Producer envía el usuario y contraseña con la intención de autenticarse.

30b. Una vez autenticado, el servidor envía cierta información para el establecimiento de la conexión.

30c. Luego, se establece la conexión broadcast entre el Helix Producer y el Servidor, empezando a enviar los paquetes codificados (en forma de streaming) hacia el servidor, sin interesar que algún cliente se haya conectado.

Las siguientes gráficas muestran el diagrama de flujo descrito anteriormente:

Flujo del Servicio – Parte I

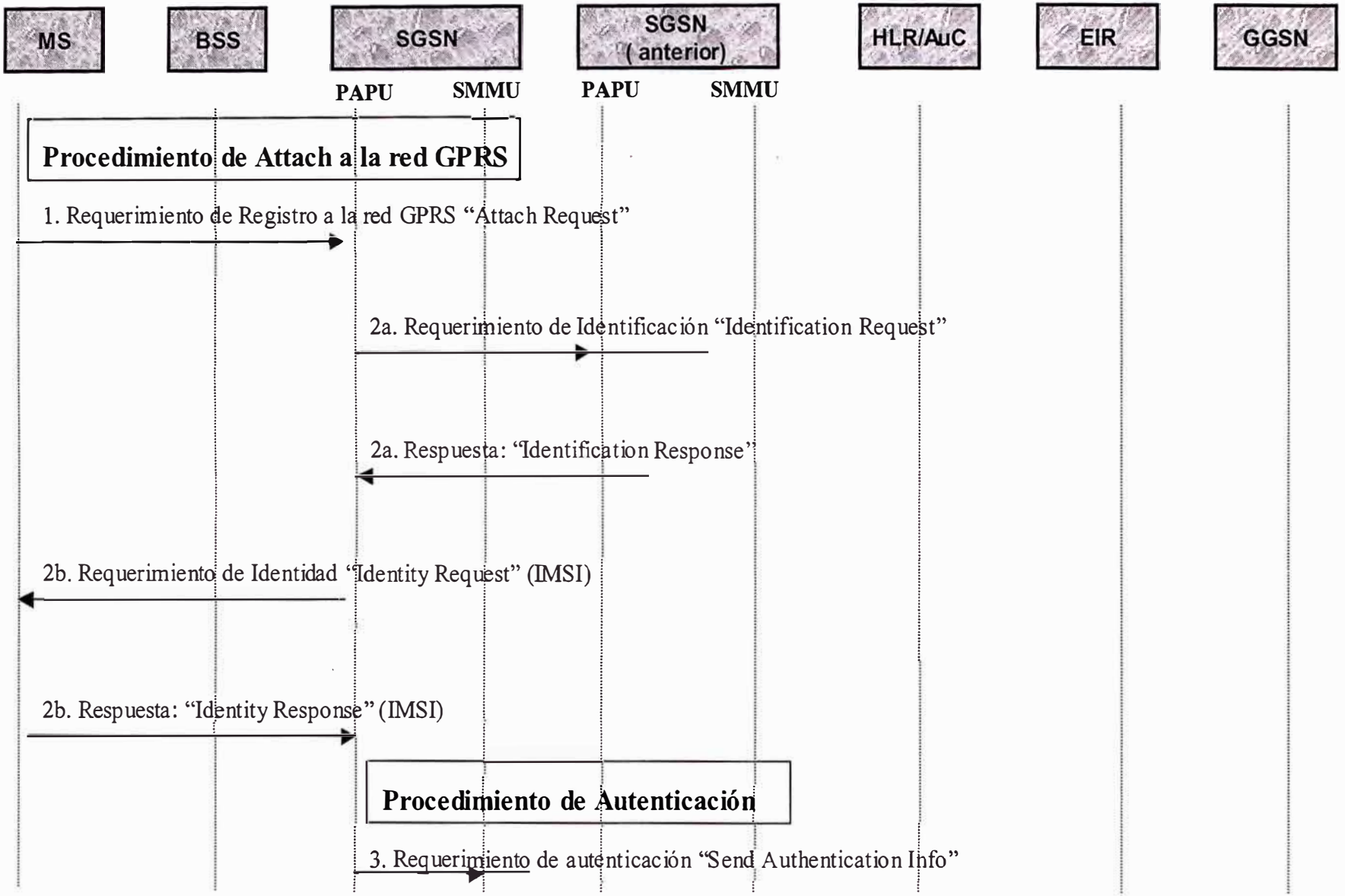
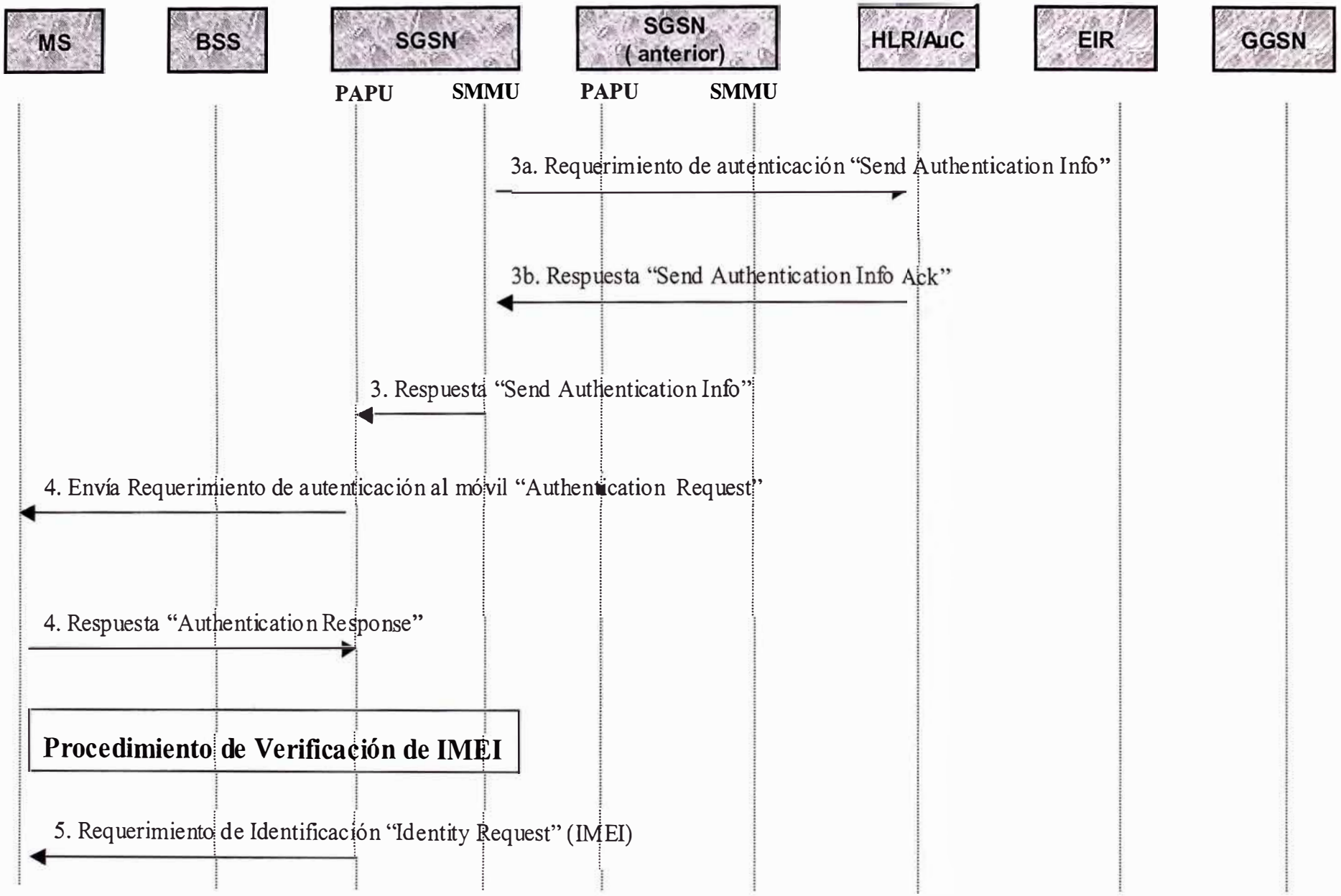
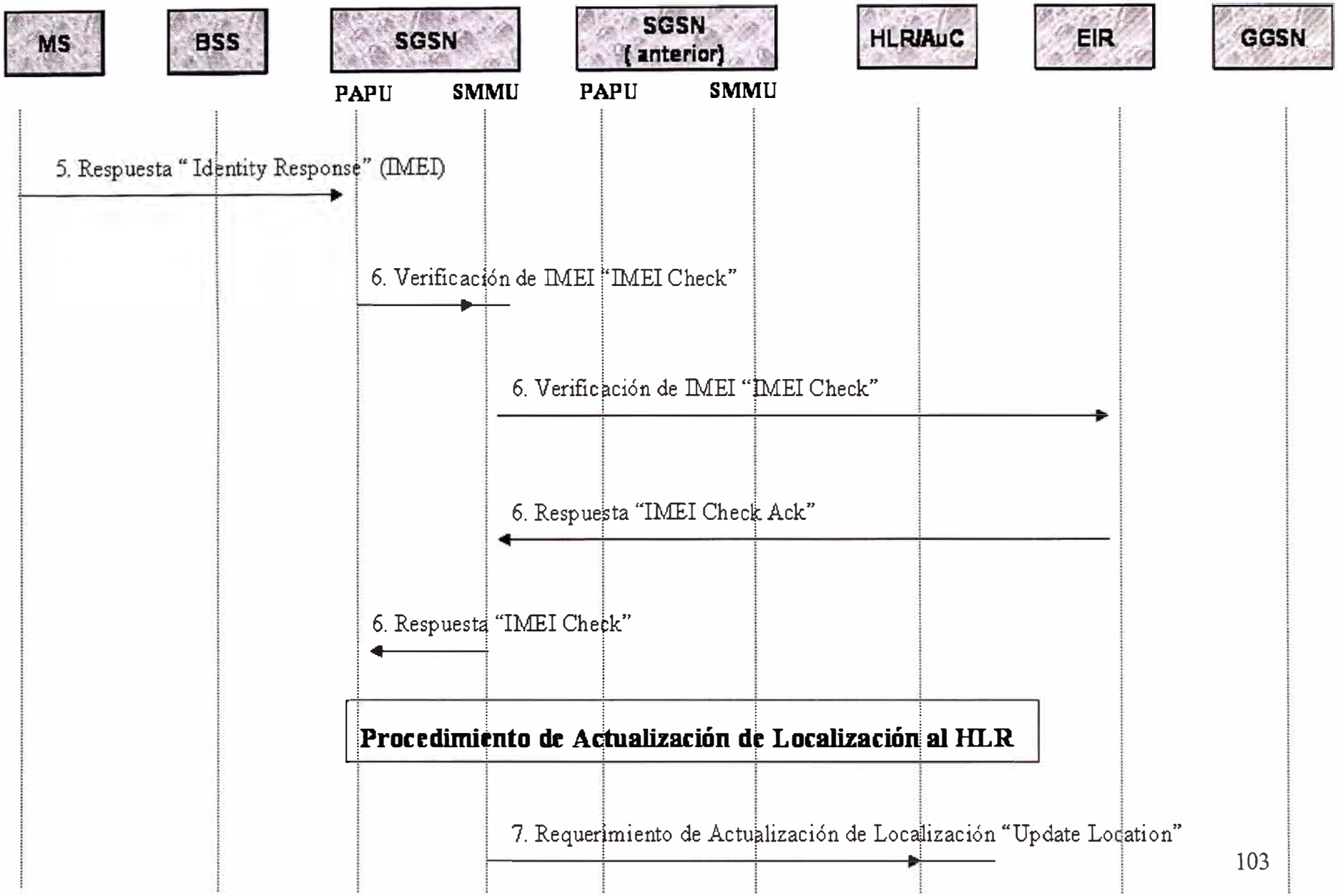


Figura 3.5 Flujo del Servicio

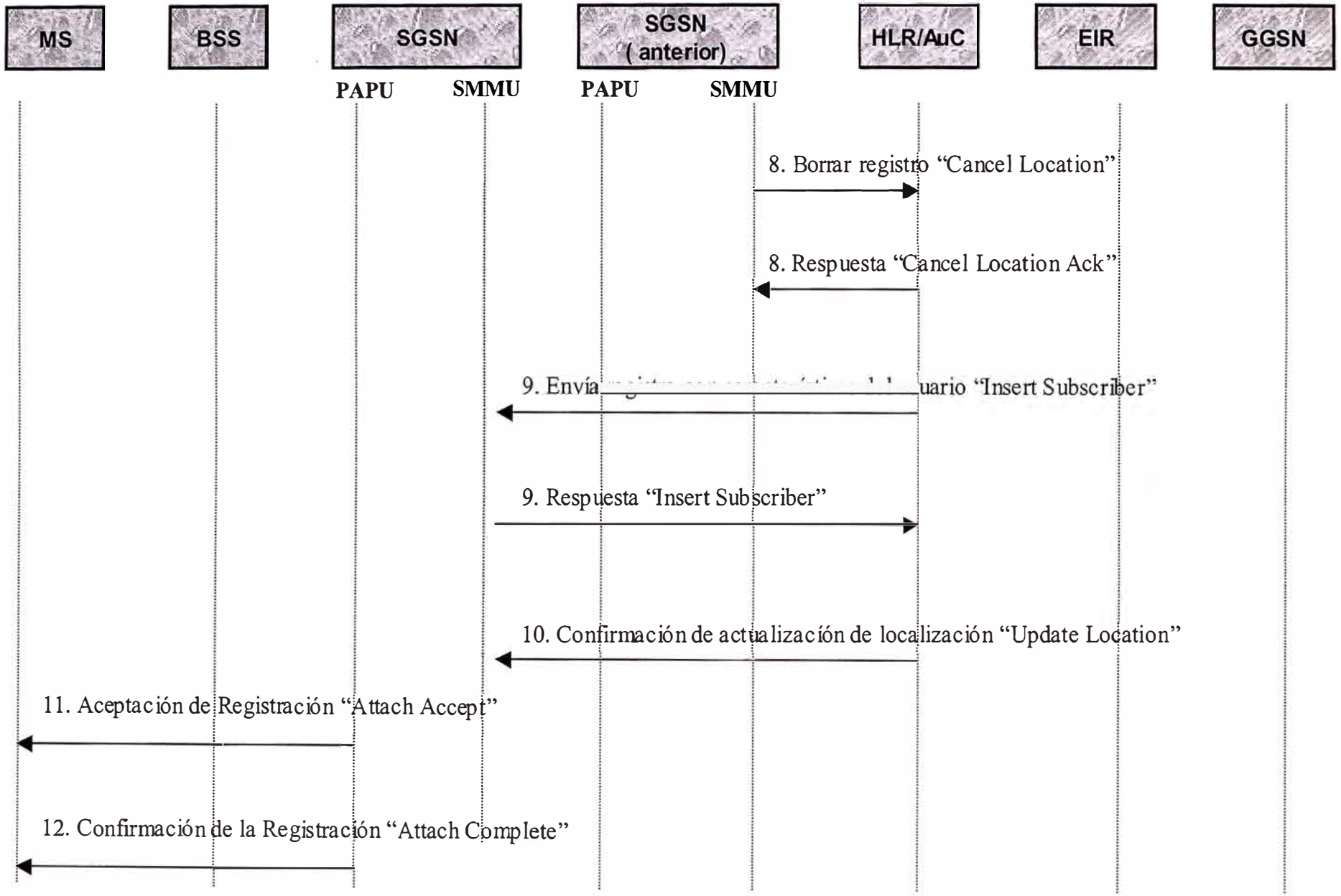
Flujo del Servicio – Parte II



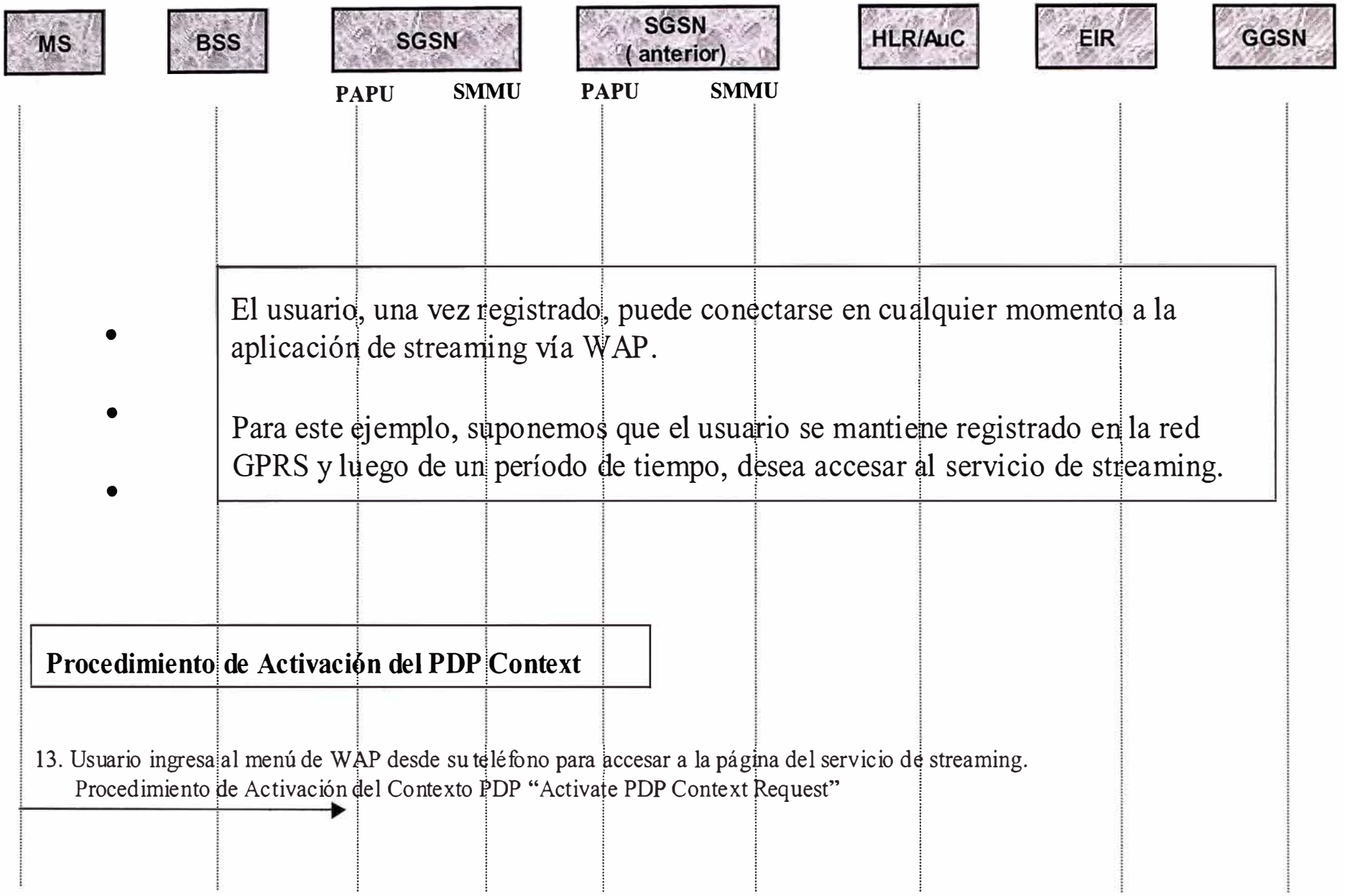
Flujo del Servicio – Parte III



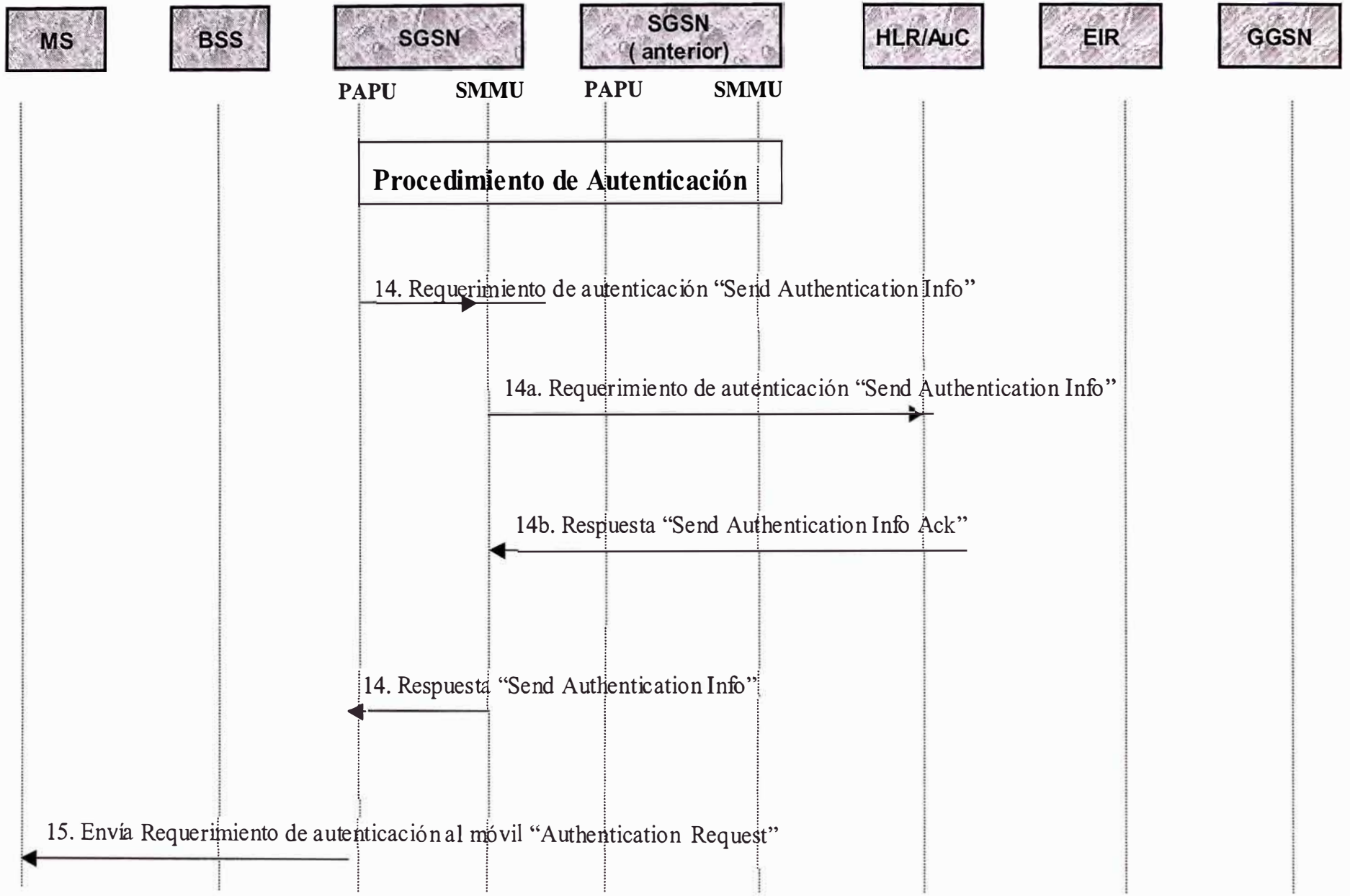
Flujo del Servicio – Parte IV



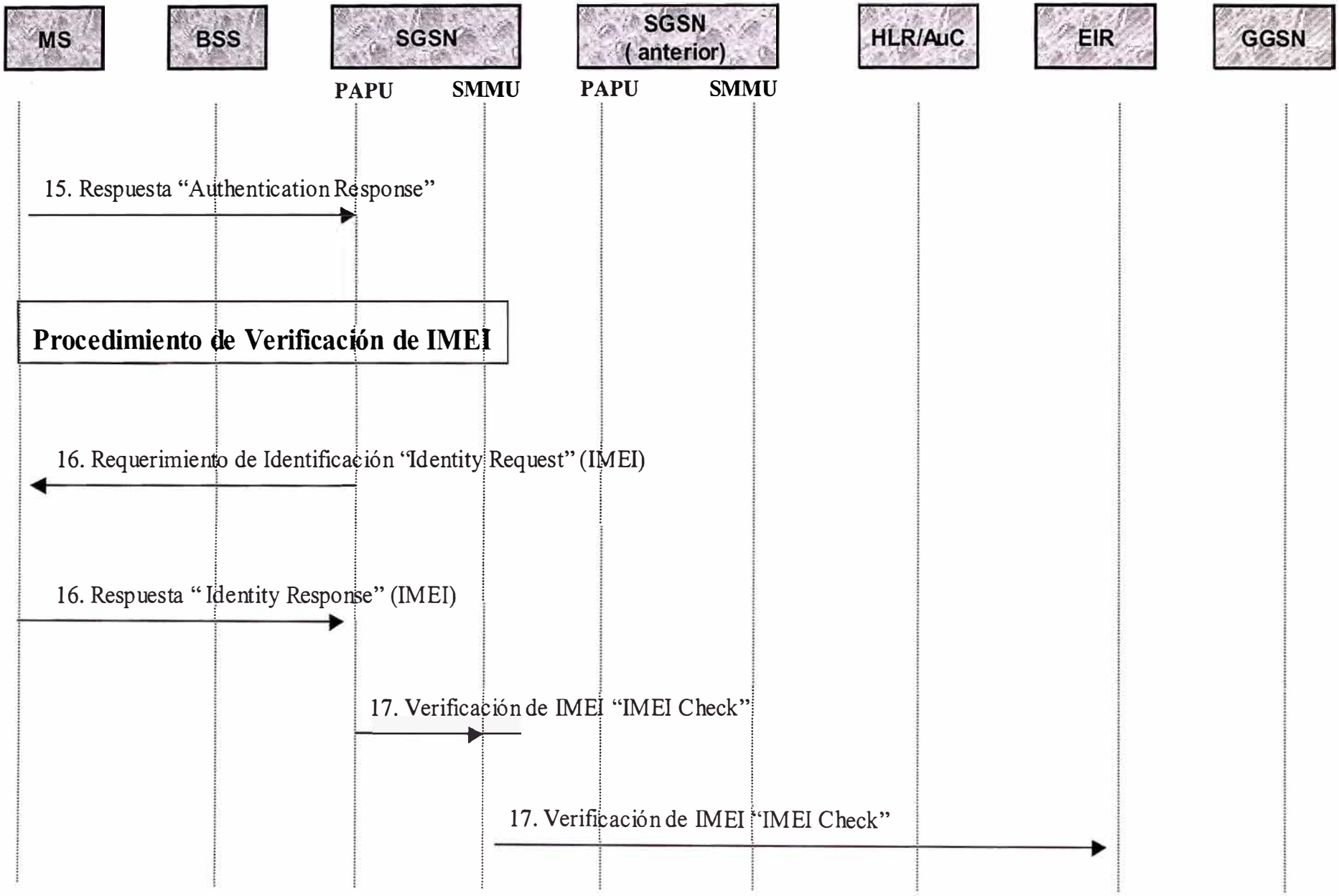
Flujo del Servicio – Parte V



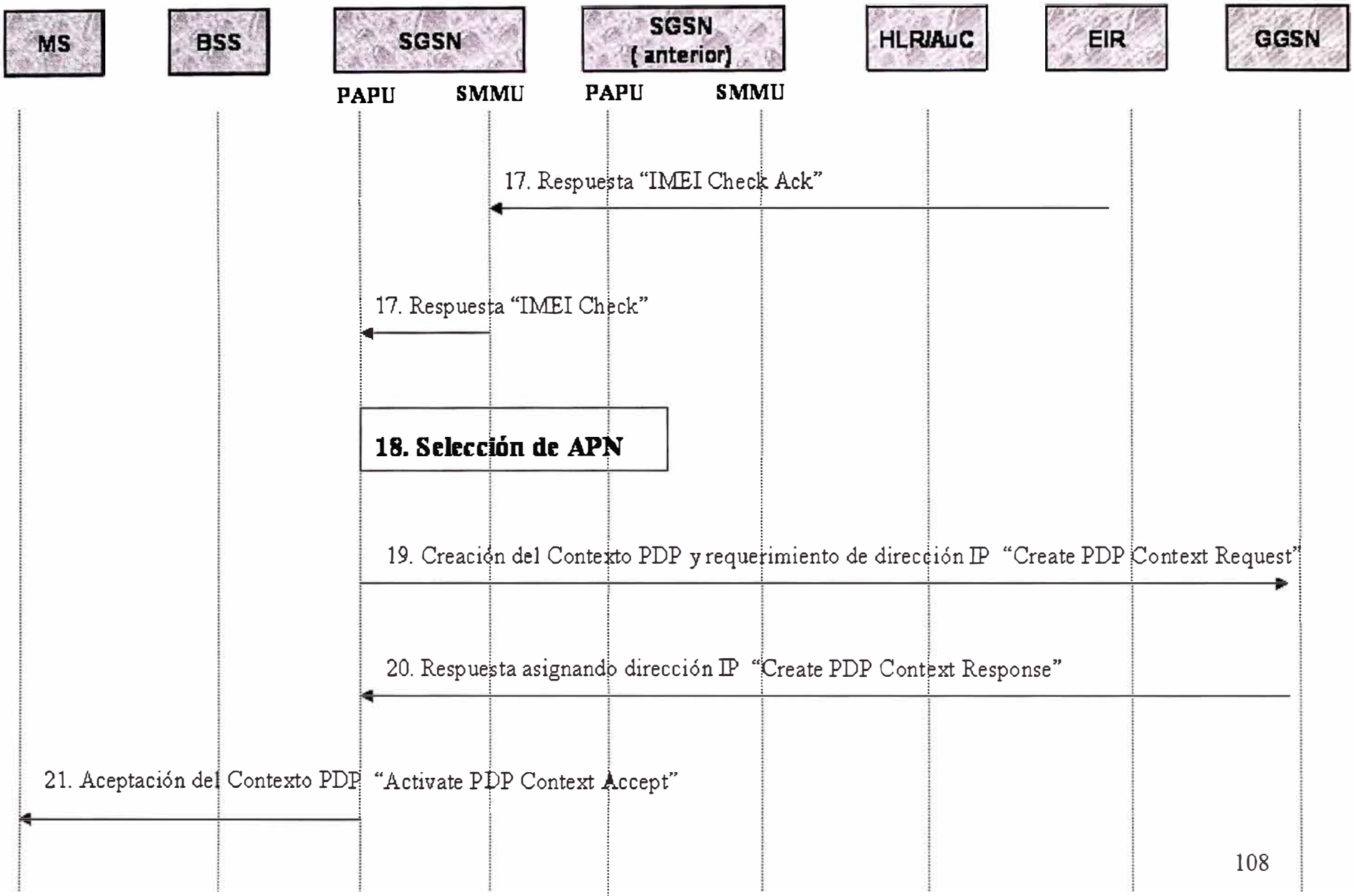
Flujo del Servicio – Parte VI



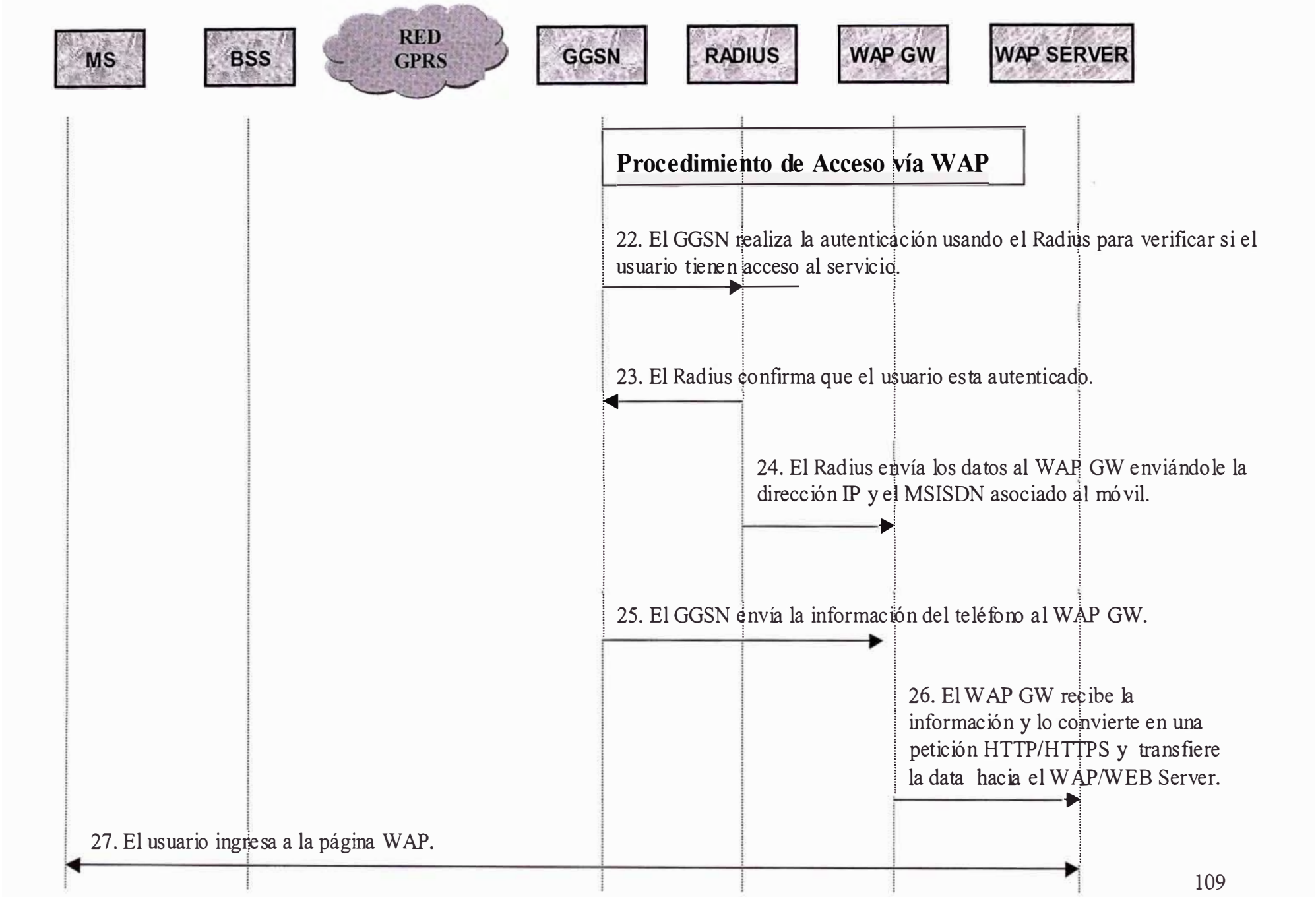
Flujo del Servicio – Parte VII



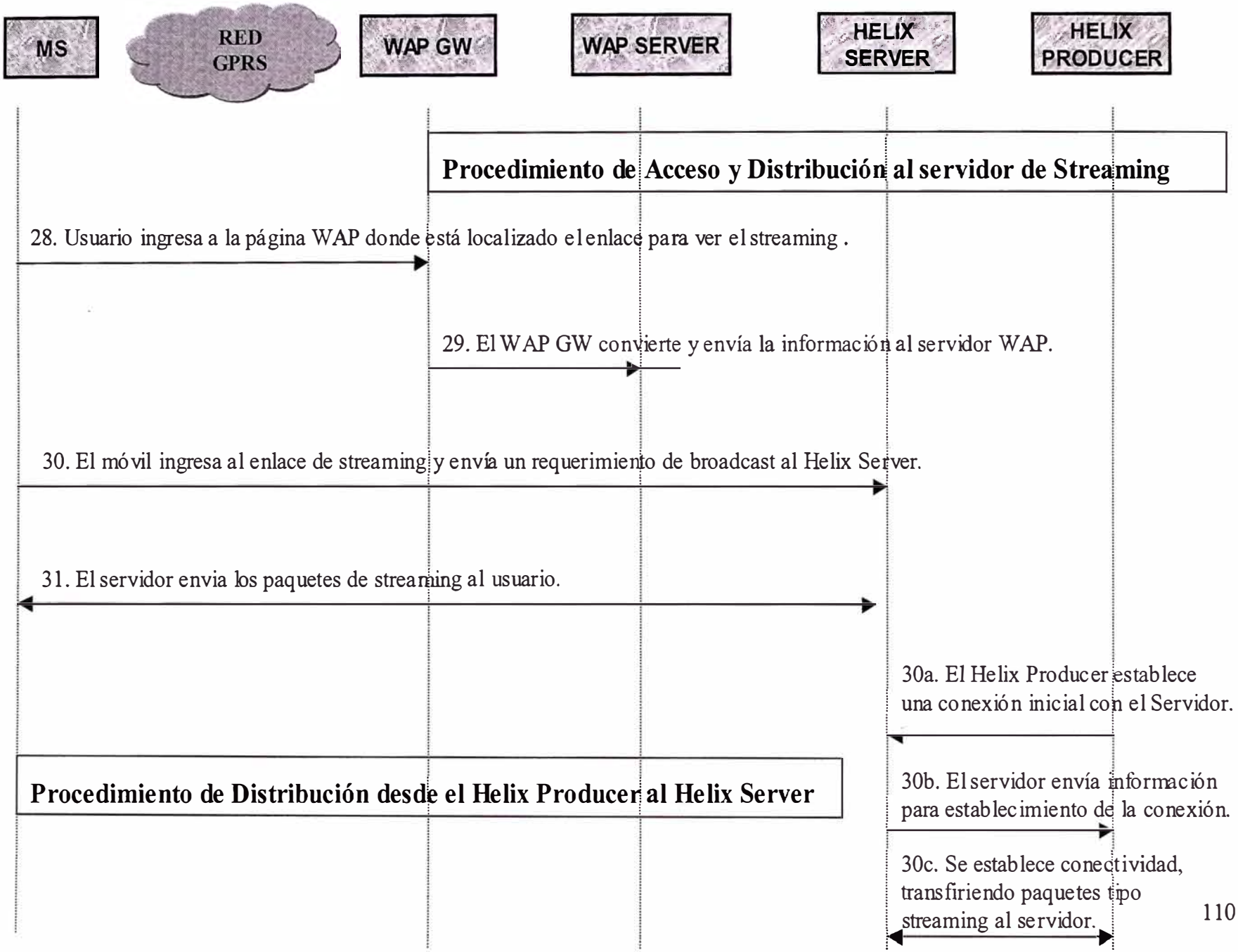
Flujo del Servicio – Parte VIII



Flujo del Servicio – Parte IX



Flujo del Servicio – Parte X



CAPITULO IV
INGENIERIA DEL PROYECTO

El presente capítulo abarca todos los aspectos relacionados a la ingeniería del proyecto, desde la configuración del servicio (Página Wap, Servidores de videostreaming, plataformas de la red GSM/GPRS/EDGE), el sistema de métricas utilizado para medir la calidad del servicio, cuya principal característica radica en que se centra su atención en el carácter continuo de la información transmitida, los tiempos utilizados para implementar el servicio, los costos asociados al proyecto, y por último, la comercialización del servicio.

4.1 Configuración del Servicio

4.1.1 Configuración en las Plataformas de Red GSM/GPRS/EDGE

La configuración en la red GSM/GPRS/EDGE para permitir el servicio de videostreaming se realiza sobre diferentes plataformas, las cuales son mostradas a continuación:

4.1.1.1 HLR

En este nodo se aprovisiona el servicio al usuario, es decir, el APN que le permitirá acceder a los servidores de streaming, así como la calidad del servicio para el acceso a la red GPRS. Esta misma configuración se realiza para el acceso por EDGE, dado que la red EDGE utiliza la misma arquitectura de la red GPRS.

Los parámetros que son configurados usualmente en los usuarios son los siguientes:

- IMSI=<international mobile subscriber identity>, representa al IMSI del usuario (número de la simcard que es único por usuario).
- PDPID=<PDP context id>, en este caso se utiliza un número específico para identificar a cada uno de los servicios (depende del operador).
- PDPTYPE=<type of the PDP context>, se refiere al tipo de versión IP soportado, generalmente por defecto es IPv4.
- PDPADDR=<address of the PDP context>, es utilizado para configurar direcciones estáticas por usuario. Para el caso del servicio TV Móvil no se requiere que el usuario tenga una dirección estática, por lo que no se utiliza este parámetro. Por

defecto, si no se asigna este parámetro, el nodo GGSN le asignará una dirección dinámica.

- APN=<access point name>, representa al nombre del punto de acceso para acceder al servicio de TV Móvil.
- GPRSACC=<add GPRS access>, es utilizado para bloquear ó desbloquear un Nombre de Punto de Acceso (APN) específico para cada usuario.
- NWACC=<network access>, este parámetro es utilizado para bloquear o desbloquear el acceso al sistema GPRS. Por ejemplo, es posible configurar para que un usuario solo pueda acceder a la red GSM y no a la red GPRS.
- QOSP=<quality of services profile>, indica el perfil de la calidad del servicio asignada al usuario.

En cambio, para el acceso por HSCSD es necesario que se habilite el servicio de transmisión de datos al usuario. En este caso, para el acceso por CSD solamente (velocidad de 9.6kbps) es necesario habilitar el servicio B16. Para habilitar el servicio de HSCSD se deberá provisionar el servicio B17 (éste incluye también las velocidades del B16 y mayores).

4.1.1.2 GGSN

En este nodo se crea y se configura los parámetros asociados al nombre del punto de acceso (APN). Los principales parámetros son los siguientes:

- APN=<Access Point Name>, representa al nombre del punto de acceso.
- Connection Type=<Type, Túnel Local IP Address, RIP, OSPF>, se especifica el tipo de conexión utilizado para acceder al servicio, en este caso, se específica la versión del IP utilizada, el default GW (generalmente el FW conectada en la interfaz Gi) y el metodo de enrutamiento.
- DHCP Servers=<IP address>, si se utilizará DHCP se debe configurar este parámetro.

- RADIUS Servers=<Authentication Server IP address, Account Server IP address, Client IP address>, se específica las direcciones de los servidores Radius encargados de la autenticación y el billing del usuario.
- Security=<Intermobile Traffic, Inter-AP Traffic>, se específica el nivel de seguridad que tendrán los usuarios a través de este APN. Estos parámetros indican si se permitido ó no el tráfico entre los móviles ó entre diferentes APNs.
- Mobile´s IP Addresses=<Dynamic IP Address Ranges, Static IP Address>, se configura el tipo de asignación IP por usuario. Este parámetro esta relacionado con el HLR, es decir, si un usuario tiene provisionado una dirección estática y el GGSN solo esta configurado para asignar direcciones dinámicas, éste rechazará el requerimiento de IP del usuario.
- DNS=<Primer DNS, Segundo DNS>, se asignan las direcciones IPs de los DNS´s.
- Session Timeouts=<Session Timeout, Idle Timeout>, se específica el tiempo máximo de duración de una sesión, es decir una vez alcanzado el tiempo, el GGSN desconectará la sesión establecida por el usuario (PDP Context Deactivation). El parámetro de Session Timeout indica cuánto tiempo el usuario puede utilizar el servicio transmitiendo datos continuamente. Mientras que el parámetro Idle timeout, indica en cuánto tiempo el GGSN desconectará la sesión si el usuario deja de transmitir información. Por defecto los dos tiempos son ilimitados.

4.1.1.3 DNS

Se deberá configurar el APN del servicio de TV Móvil en los DNS´s de la red GPRS.

4.1.1.4 FW – FIREWALL

Generalmente en la interfaz Gi del GGSN estará siempre conectado un Firewall (FW), esto debido a que cualquier servidor conectado a esa interfase siempre sera accesado por cualquier móvil cuando se conecta a la red GPRS/EDGE. Por este motivo, los servidores de aplicaciones siempre estarán conectados después del FW, quién será el

responsable de configurar las políticas de acceso de determinados APN´s hacia los servidores de aplicaciones.

4.1.1.5 ROUTERS

Se deberán configurar las rutas tanto de acceso como de retorno entre las direcciones IP´s de los usuarios móviles con los servidores de aplicaciones.

4.1.1.6 RAS – REMOTE ACCESS SERVER

Para el acceso por HSCSD/CSD es necesario realizar las siguientes configuraciones:

- Dial Number=<# Marcación>, se deberá definir el número de acceso remoto para el cuál los usuarios móviles discarán para acceder al servicio.
- Pool IP Address=<IP Ranges>, se deberá definir un rango de direcciones IP´s, asignadas al número de marcación anterior, que accederán a los servidores de aplicaciones.
- Permisos de Acceso=<Authorization>, se deberá configurar en el RAS un usuario y password de tal forma que sólo los usuarios que tengan esa cuenta configurada en el terminal puedan acceder al servicio.
- Reglas en FW, se deberán definir las políticas de seguridad y acceso de ese pool de direcciones IP´s hacia los servidores de aplicaciones.
- Configuración de Rutas – Routers, se deberán configurar las rutas de acceso y de retorno entre el pool de direcciones IP´s asignadas a los móviles con los servidores de aplicaciones.

4.1.2 Configuraciones de Acceso

A continuación se describe la configuración para el acceso al servicio de TV Móvil. Este acceso vendría a ser el control remoto para la elección de los canales de televisión.

4.1.2.1 WAP GW

Una vez configuradas las políticas de seguridad en el FW tanto del GGSN como del RAS para que puedan acceder a los servidores de aplicaciones (servidores de videostreaming, WAP GW, WAP/WEB Servers, etc.), se deberá crear una ruta directa en el WAP GW de

tal forma que redireccione directamente el URL del control remoto de televisión hacia los servidores de aplicaciones, puesto que estos servidores se localizarían dentro de la red interna del operador y no tienen porque ser publicadas en la Internet (en casos que los servidores esten localizados fuera de las instalaciones del operador y no existan conexiones dedicadas entre ellos, entonces es necesario configurar el nombre del dominio (URL) en los DNS´s del operador.

4.1.2.2 WAP/WEB PAGE

Usualmente cuando se desarrollan páginas WAP se utiliza el código XML, puesto que es el código nativo para estas aplicaciones, las cuales permiten por ejemplo hacer interacciones con bases de datos entre el teléfono celular y un servidor de aplicaciones. Por otro lado, en el caso del proyecto TV Móvil, se podría utilizar simplemente una página Web desarrollada en HTML dado que sólo realizará una redirección hacia una aplicación simulando ser un Control Remoto de Televisión.

A continuación se muestra un ejemplo del código HTML que simula el control remoto de Televisión:

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<HTML><HEAD><TITLE>TV Movil</TITLE>
<META http-equiv=Content-Type content="text/html; charset=windows-1252">
<META content="MSHTML 6.00.2800.1226" name=GENERATOR></HEAD>
<BODY bottomMargin=0 leftMargin=0 topMargin=0 rightMargin=0>
<TABLE border=0>
  <TBODY>
  <TR>
    <TD vAlign=top><IMG src="logos/uni2.gif"></TD></TR>
  <TR>
    <TD vAlign=top align="center" bgColor=red><FONT
      style="TEXT-DECORATION: none" color=#ffffff><B>Control Remoto de TV
    </B></FONT></TD></TR>
  <TR>
     <TD vAlign=top>
      <TABLE>
        <TBODY>
        <TR>
          <TD                                                    width=55><A
href="http://localhost:81/ramgen/broadcast/frecuencia.rm"><IMG
            alt=image src="logos/ch2.gif"></A></TD>
          <TD vAlign=top>
            <TABLE>
              <TBODY>
              <TR>
```

```
                <TD><FONT        face=Verdana        size=1><B>Frecuencia
Latina</B></FONT></TD></TR>
              <TR>
                <TD><FONT            face=Verdana            size=1>Canal
2</FONT></TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></TD></TR>
  <TR>
    <TD vAlign=top>
      <TABLE>
        <TBODY>
        <TR>
          <TD                                                    width=55><A
href="http://localhost:81/ramgen/broadcast/america.rm"><IMG
            alt=image src="logos/ch4.gif"></A></TD>
          <TD vAlign=top>
            <TABLE>
              <TBODY>
              <TR>
                <TD><FONT          face=Verdana          size=1><B>America
TV</B></FONT></TD></TR>
              <TR>
                <TD><FONT            face=Verdana            size=1>Canal
4</FONT></TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></TD></TR>
  <TR>
    <TD vAlign=top>
      <TABLE>
        <TBODY>
        <TR>
          <TD width=55><A

href="http://localhost:81/ramgen/broadcast/panamericana.rm"><IMG
alt=image
            src="logos/ch5.gif"></A></TD>
          <TD vAlign=top>
            <TABLE>
              <TBODY>
              <TR>
                <TD><FONT face=Verdana size=1><B>Panamericana
                TV</B></FONT></TD></TR>
                <TR>
                <TD><FONT            face=Verdana            size=1>Canal
5</FONT></TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></TD></TR>
  <TR>
    <TD vAlign=top>
      <TABLE>
        <TBODY>
        <TR>
          <TD                                                    width=55><A
href="http://localhost:81/ramgen/broadcast/tnp.rm"><IMG
            alt=image src="logos/ch7.gif"></A></TD>
          <TD vAlign=top>
            <TABLE>
              <TBODY>
              <TR>
                <TD><FONT face=Verdana size=1><B>TNP</B></FONT></TD></TR>
                <TR>
                <TD><FONT            face=Verdana            size=1>Canal
7</FONT></TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></TD></TR>
  <TR>
    <TD vAlign=top>
      <TABLE>
        <TBODY>
```

```
        <TR>
          <TD                                                    width=55><A
href="http://localhost:81/ramgen/broadcast/andina.rm"><IMG
            alt=image src="logos/ch9.gif"></A></TD>
          <TD vAlign=top>
            <TABLE>
              <TBODY>
              <TR>
                <TD><FONT          face=Verdana          size=1><B>Andina
TV</B></FONT></TD></TR>
              <TR>
                <TD><FONT             face=Verdana             size=1>Canal
9</FONT></TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></TD></TR>
  <TR>
    <TD vAlign=top>
      <TABLE>
        <TBODY>
        <TR>
          <TD                                                    width=55><A
href="http://localhost:81/ramgen/broadcast/oktv.rm"><IMG
            alt=image src="logos/ch11.gif"></A></TD>
          <TD vAlign=top>
            <TABLE>
              <TBODY>
              <TR>
                <TD><FONT             face=Verdana             size=1><B>OK
TV</B></FONT></TD></TR>
              <TR>
                <TD><FONT             face=Verdana             size=1>Canal
11</FONT></TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></TD></TR>
  <TR>
    <TD vAlign=top>
      <TABLE>
        <TBODY>
        <TR>
          <TD                                                    width=55><A
href="http://localhost:81/ramgen/broadcast/redglobal.rm"><IMG
            alt=image src="logos/ch13.gif"></A></TD>
          <TD vAlign=top>
            <TABLE>
              <TBODY>
              <TR>
                <TD><FONT          face=Verdana            size=1><B>Red
Global</B></FONT></TD></TR>
              <TR>
                <TD><FONT             face=Verdana             size=1>Canal
13</FONT></TD></TR></TBODY></TABLE></TD></TR></TBODY></TABLE></TD></TR>
  <TR>
    <TD align=middle><IMG height=5 src="logos/null.gif"
  width=1></TD></TR>
  <TR>

<TD                                                    align="center"><IMG
src="logos/uni1.GIF"></TD></TR></TBODY></TABLE></BODY></HTML>
```

A continuación se muestra la página de ejemplo que simula el Control Remoto de Televisión (esta página es mostrada de la misma manera en el terminal telefónico):

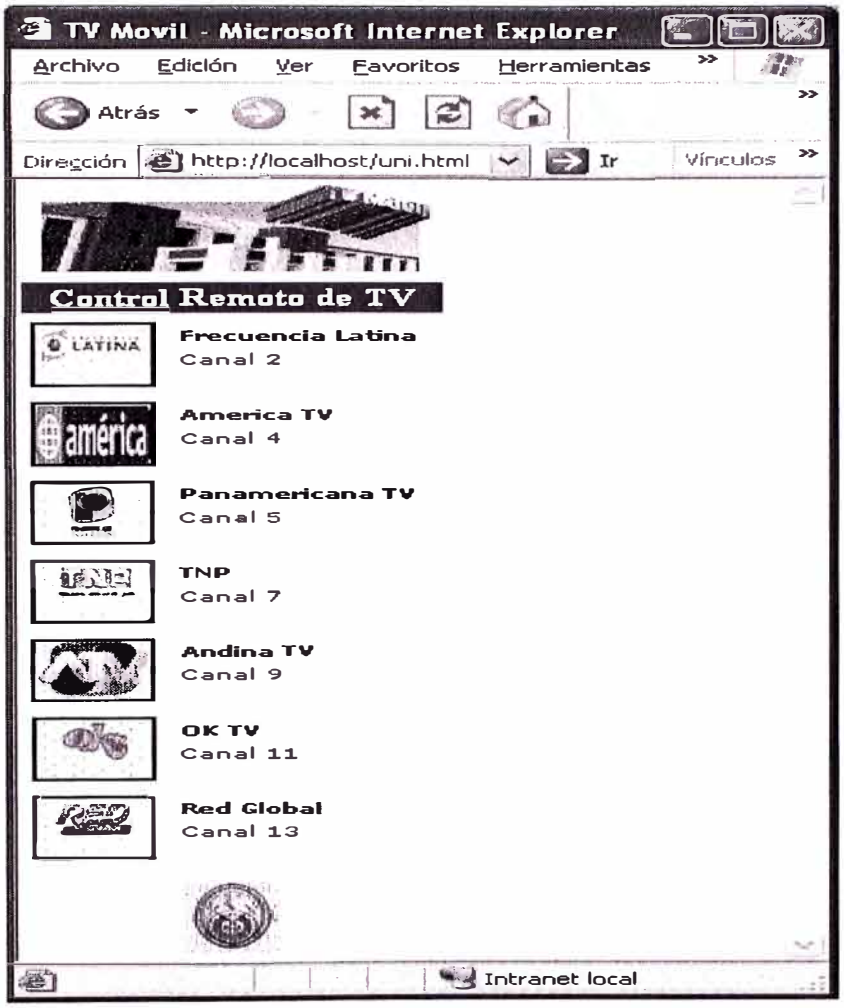


Figura 4.1 Control Remoto de Televisión

4.1.2.3 WEB SERVER

El servidor WEB utilizado es el APACHE WEB SERVER, éste es un servidor web de libre disponibilidad para la mayoría de sistemas operativos basados en Windows, Unix y Linux. El servidor Apache es uno de los servidores web más populares en Internet, una encuesta realizada en Octubre del 2003 por Netcraft Web Server Survey indica que más del 64% de sitios en Internet utilizan Apache como servidor HTTP. La siguiente gráfica muestra la pantalla de instalación del Servidor Apache:

Figura 4.2 Configuración del Web Server

4.1.3 Configuraciones de los Servidores de Streaming

A continuación se detalla los pasos a seguir para instalar y configurar los servidores de videostreaming.

4.1.3.1 HELIX PRODUCER

Para instalar el software de Helix Producer es necesario que la computadora cumpla con los siguientes requerimientos mínimos:

Requerimientos de Windows

Requerimientos	Mínimos
CPU	400 MHz
RAM	96 MB
Sistema Operativo	Windows 98 hacia adelante
Espacio de Disco Duro (Software)	20 MB
Espacio de Disco Duro (Datos)	500 MB
Pantalla a Color	16 bit
Tarjeta de Sonido	16 bit ó mejor

Tabla 4.1 Requerimientos de Windows (Helix Producer)

En general el procedimiento de instalación es el siguiente:

1. Descargar el programa desde la página web www.real.com
2. Cerrar todas las aplicaciones abiertas.
3. Entrar parámetros de personalización, licencias y aceptar las condiciones de la instalación.
4. Especificar ubicación del programa.

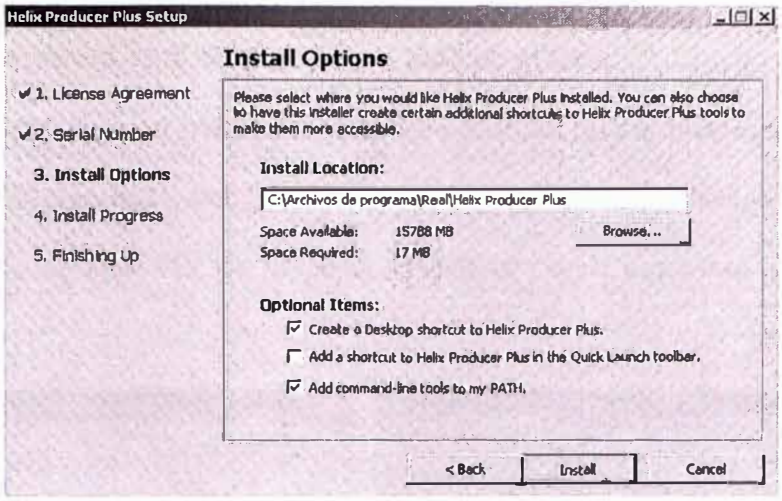


Figura 4.3 Instalación del Helix Producer

5. Elegir desde que lugar se ejecutará el Helix Producer y presionar "Finish" para terminar la instalación.
6. La pantalla del SW se muestra a continuación:

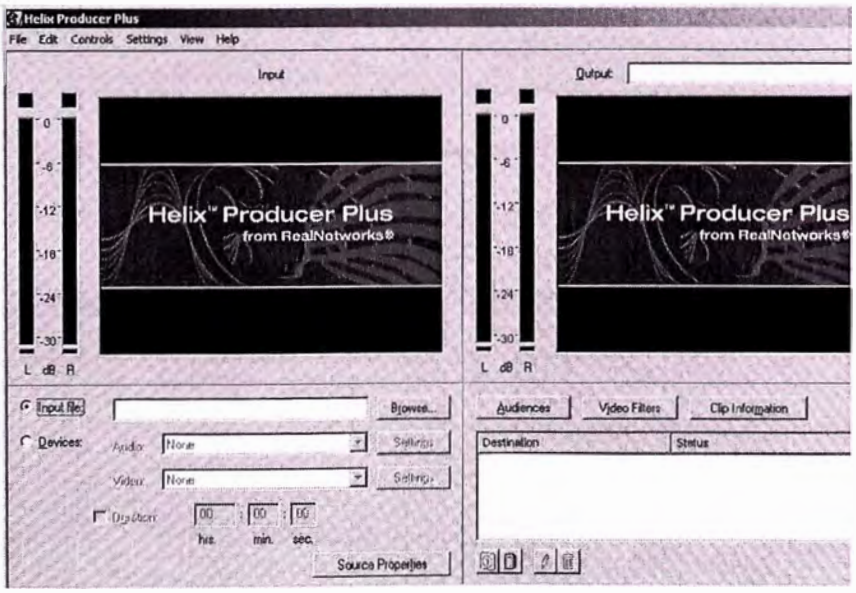


Figura 4.4 Pantalla de Inicio del Helix Producer

Configuración del Streaming

Básicamente a nivel de aplicación, la configuración se realiza en el Helix Producer. En este caso, para el acceso por HSCSD se han considerado 02 tipos de audiencias, la primera de 14kbps y la segunda de 28kbps. Para el acceso por GPRS se ha agregado

una audiencia de 36kbps, y por último, para el acceso a una red EDGE se han agregado 02 audiencias adicionales, una de 60kbps y la otra de 100kbps.

Es importante señalar que en casos de no tener recursos de canales disponibles en la red GPRS/EDGE, la negociación del throughput entre el móvil y el terminal podrían tomar algunas audiencias del HSCSD. Un ejemplo se muestra en la siguiente gráfica:

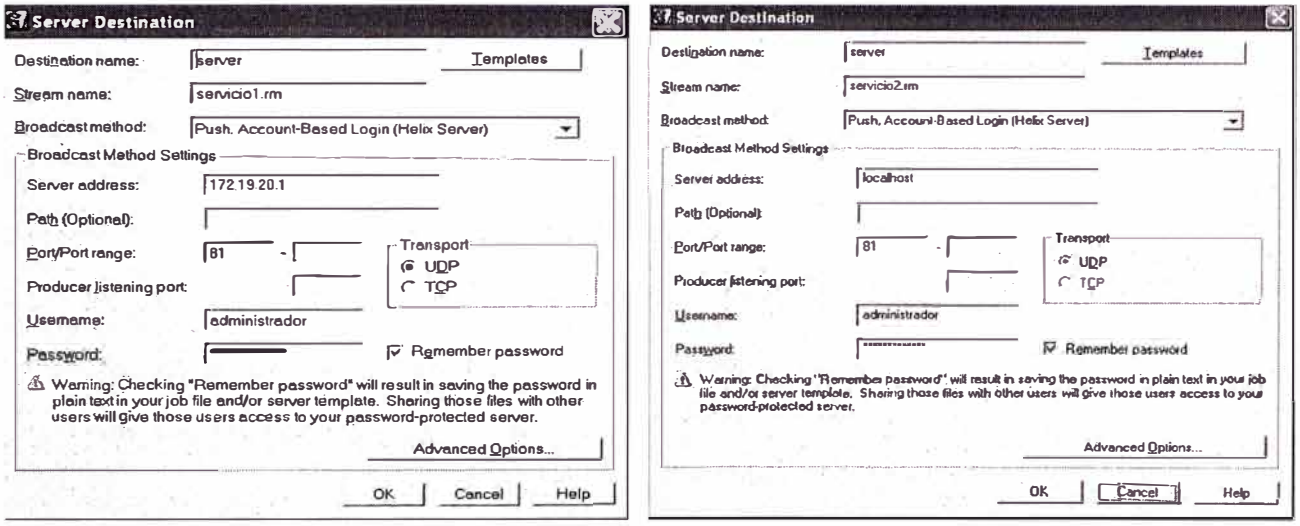


Figura 4.5 Configuración de los servicios en el Helix Producer

Los parámetros en cada audiencia se muestran a continuación:

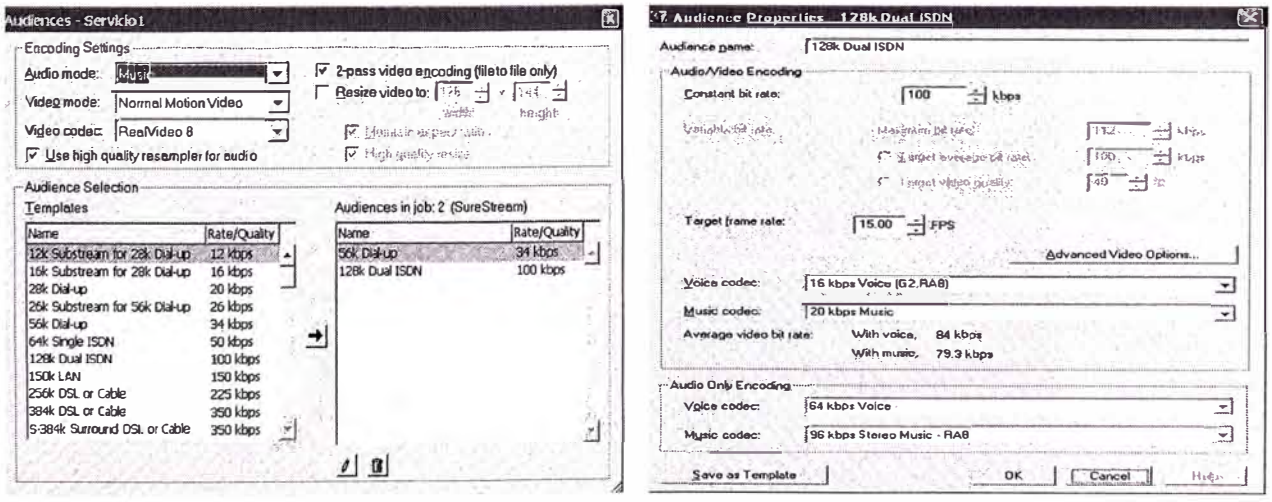


Figura 4.6 Configuración de las audiencias en el Helix Producer

4.1.3.2 HELIX SERVER

Para instalar el software del Helix Server es necesario que la computadora cumpla con los siguientes requerimientos mínimos:

Requerimientos de Windows

Requerimientos	Mínimos
CPU	500 MHz
RAM	256 MB
Sistema Operativo	Windows 2000 hacia adelante
Espacio de Disco Duro Requerido	("X bit rate del video en kbps" multiplicado por "Y longitud del video en segundos") / 8 = KB espacio de disco requerido.

Tabla 4.2 Requerimientos de Windows (Helix Server)

En general el procedimiento de instalación es el siguiente:

1. Descargar el programa desde la página web www.real.com
2. Cerrar todas las aplicaciones abiertas.
3. Aceptar las condiciones de la instalación y entrar parámetros de personalización y licencias.
4. Especificar ubicación del programa.
5. Ingresar Usuario y Contraseña de administrador.

Figura 4.7 Instalación del Helix Server

6. Especificar los puertos a utilizar en cada aplicación. Es importante considerar en este paso, que si se utiliza en el mismo servidor de Streaming el servidor Web Apache, éste podría ocasionar conflicto de puertos dado que las dos aplicaciones utilizan por defecto el puerto 80. Por lo tanto, es recomendable cambiar el puerto HTTP del Helix Server al puerto 81.

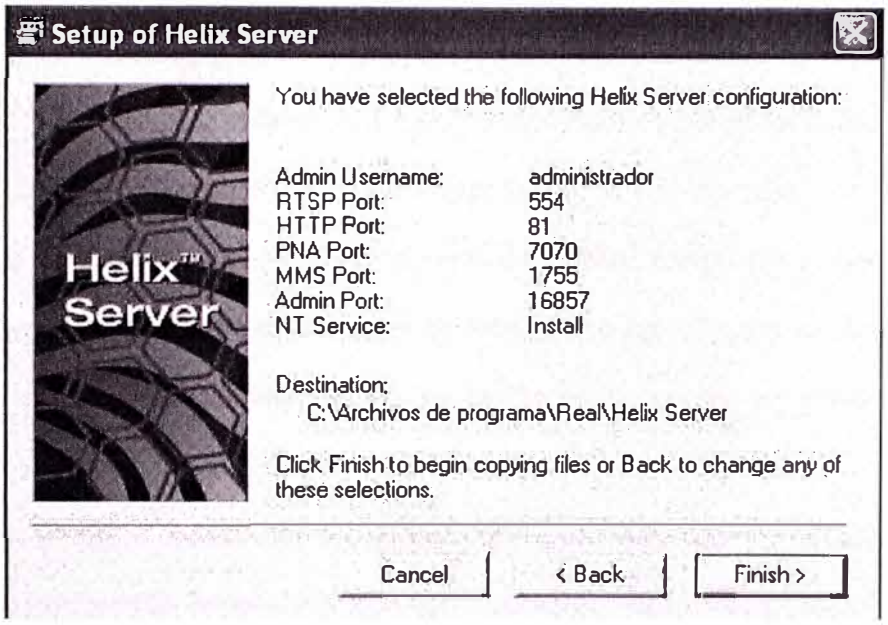


Figura 4.8 Configuración del Helix Server

7. La siguiente gráfica muestra la página de administración del Helix Server.

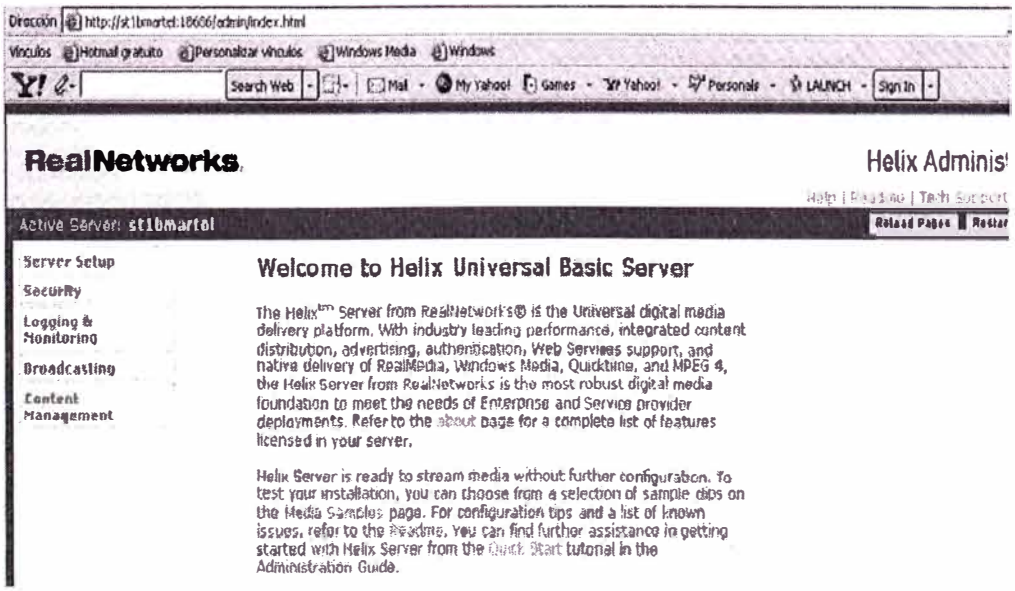


Figura 4.9 Pantalla de Inicio del Helix Server

4.2 Métricas para el Análisis del Servicio

Un aspecto fundamental en todo proyecto de ingeniería, a parte del diseño, desarrollo é implementación, representa el mantenimiento del servicio. Para ello, se deberán contar con herramientas que permitan monitorear el servicio, principalmente si estos son servicios en tiempo real.

Es importante además considerar, que el hecho de empezar a ofrecer servicios en tiempo real, como el TV Móvil, posicionan a las empresas como líderes tecnológicos, lo cuál da como consecuencia, en una mayor demanda debido a las posibles expectativas de los clientes por la novedad del servicio. Esto también podría ser contraproducente, si es que no se toma en cuenta la calidad del servicio a brindar a los clientes así como el consumo de los recursos utilizados. Es imprescindible, por lo tanto, mantener una calidad aceptable con el menor costo y consumo de recursos posibles.

En los últimos tiempos, se han implementado una gran variedad de servicios así como de sistemas y herramientas de análisis que en un principio solo comprobaban el número de accesos de los usuarios, que luego fueron mejoradas con herramientas más sofisticadas que podían generar reportes muy variados. Con la aparición del vídeo inicialmente en Internet, estas herramientas se han comenzado a utilizar para analizar este nuevo tipo de servicio. Sin embargo, se deben realizar algunas configuraciones adicionales que permitan manejar el carácter continuo de la información. Actualizar estas herramientas obliga a disponer de métricas capaces de evaluar parámetros que no están presentes en los servicios Web clásicos. Por el lado del operador celular, las métricas pueden ser basadas en las plataformas de GPRS (específicamente: GGSN y el Charging GW), así como también a través del acceso a la página WAP. Aún así, no es posible obtener información como para administrar adecuadamente este tipo de servicio, puesto que los logs recolectados por esas plataformas no consideran el carácter continuo de la información. En este campo son de especial relevancia los aspectos relacionados con la calidad del servicio. Mientras que en los servicios Web la calidad se limitaba a conseguir

un tiempo de respuesta mínimo, en los servicios de video evaluar la calidad resulta una tarea más compleja. Será necesario comprobar cómo la información va llegando al usuario a lo largo de la reproducción, es decir: si hay cortes cuando se está mirando el video, si se pierden tramas ó "frames" tanto de vídeo como de audio, si la calidad ha tenido que ser reducida por falta de ancho de banda, etc.

Este capítulo abarca un conjunto de métricas de calidad adaptadas para el análisis de servicios en tiempo real. Su principal característica radica en que se centra su atención en el carácter continuo de la información transmitida. Además, se hace una distinción de diferentes métricas que ayudarán al administrador del sistema así como al área de Marketing tomar decisiones respecto al servicio que puedan estar ofreciendo a sus clientes.

4.2.1 Descripción de las Métricas

El objetivo primordial de cualquier empresa que desea brindar un servicio en tiempo real es el de ofrecer una calidad de servicio óptima con la menor utilización de recursos posible. Para ello, es necesario controlar los diferentes problemas que pudieran ocurrir durante la reproducción de los vídeos que distribuye.

Los datos necesarios para el cálculo de las métricas que a continuación se presentan pueden extraerse con facilidad de los mecanismos de logs proporcionados por el servidor de streaming.

Las métricas se clasifican atendiendo a los diferentes tipos de análisis que se pueden realizar a la hora de evaluar un servicio en tiempo real:

- Métricas de Calidad.
- Métricas de Contenidos.
- Métricas de Popularidad; y
- Métricas de Eficiencia.

4.2.2 Métricas de Calidad

Las métricas de calidad pretenden evaluar la calidad con la que los clientes acceden al servicio de streaming. Es importante conocer cómo se visualizan los vídeos ofrecidos, debido a que puede ser necesario realizar modificaciones durante la producción del servicio.

Durante este proceso es posible configurar parámetros como el ancho de banda que serán distribuidos a los clientes, pero el ancho de banda ideal no se sabe a priori, sino que hay que ir refinándolo en un proceso iterativo de análisis y configuración. Aunque también es posible obtenerlos a través de los parámetros de cada teléfono específico.

Por ejemplo, podría darse el caso que el administrador configure los vídeos con una calidad demasiado elevada, ocasionando problemas a los clientes que no tienen esa disponibilidad de recursos. Mediante las métricas ofrecidas podemos saber si las calidades configuradas no se ajustan a las capacidades de acceso de los usuarios al servicio.

4.2.2.1 Entregas Satisfactorias – SR

Esta métrica pretende contabilizar todas aquellas peticiones que llegan a entregar un mínimo de contenido multimedia a los clientes. Se consideran satisfactorias las peticiones que son mayores que 0.

4.2.2.2 Entregas Erróneas

Por otro lado, es también interesante controlar el porcentaje de peticiones fallidas, es decir, aquellas peticiones en las que no se han podido transmitir contenidos multimedia. Este tipo de peticiones puede ser detectado pues el tiempo de video transmitido es de 0 segundos.

La existencia de un elevado porcentaje de transmisiones erróneas puede deberse a diferentes motivos. En la mayoría de casos se trata de problemas en el ancho de banda de las conexiones implicadas, pero hay ocasiones en las que el problema puede ser diferente. Es posible que los usuarios no dispongan de las aplicaciones cliente necesarias

para la visualización de los contenidos multimedia. También, es posible que haya problemas en la capacidad de la conexión de salida del servidor de vídeo. En este caso, será necesario solicitar un aumento del ancho de banda de subida al proveedor del servicio correspondiente.

A través del servidor es posible obtener las dos métricas, explicadas anteriormente, a través de los logs proporcionados por este servidor de streaming. A partir de este momento, nos referiremos como servidor de streaming al Helix Server, que es la solución de servidor de RealNetworks para servicios de streaming.

El Helix Server provee 6 diferentes estilos, numerados desde 0 hasta el 5, de las cuales los estilos del 1 al 5 proveen información sobre los parámetros utilizados en el streaming. El estilo 0 solo contiene información acerca de la dirección IP del cliente, la hora de conexión (sin especificar el tiempo transmitido), el tipo de protocolo, el tipo de contenido y las características del cliente.

Para nuestro caso, se ha utilizado el estilo 4, que incluye los estilos 0, 1, 2 y 3. La información contenida en el estilo 4 se muestra a continuación:

IP_address - - [timestamp] "GET filename protocol/versión" http_status_code bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time ***sent time*** *resends failed_resends [stream_components] [start_time] server_address average_bitrate packets_sent.*

Donde:

Sent_Time: Representa la duración total en segundos de transmitir el contenido multimedia al cliente. Este parámetro será utilizado para obtener las dos métricas explicadas anteriormente.

4.2.2.3 Indicador de Calidad de Audio – QA

Un factor fundamental durante la difusión de vídeos es una correcta transmisión de la señal de audio. Los defectos en la imagen no son tan críticos, debido a que no suelen ser fundamentales a la hora de facilitar la comprensión de un vídeo. Por el contrario, los

problemas en la transmisión de audio representarían un verdadero problema a los clientes a la hora de entender lo que se ha expuesto en el vídeo.

Esta métrica pretende servir como indicador a la hora de evaluar la calidad de transmisión del sonido a los clientes. Corresponde al porcentaje de peticiones sin problemas en la distribución de la señal de audio, es decir, sin reenvíos fallidos, sin paquetes de audio perdidos y sin paquetes retrazados.

Para evaluar este indicador se utilizan dos tasas que son mostradas a continuación:

4.2.2.3.1 Tasa de Pérdidas de Audio – AL

Esta métrica proporciona un enfoque alternativo a la hora de evaluar la calidad de transmisión de audio, centrándose en el estudio de la relación existente entre el número de paquetes perdidos con respecto al número total de paquetes enviados.

Para su cálculo se utiliza la siguiente fórmula:

$$AL = \frac{Paquetes\ Perdidos\ Audio}{Paquetes\ Totales\ Audio}$$

Fórmula 4.1

4.2.2.3.2 Tasa de Retrasos de Audio – APD

Otro problema existente durante la transmisión del audio es el del retraso de los paquetes de sonido. La expresión utilizada para su cálculo es la siguiente:

$$APD = \frac{Paquetes\ Retrasados\ Audio}{Paquetes\ Totales\ Audio}$$

Fórmula 4.2

A través del Helix Server, es posible obtener 04 tipos de estadísticas del tráfico de contenido multimedia. Específicamente, los parámetros utilizados para obtener las métricas relacionadas al indicador de calidad de audio esta relacionada al primer tipo de estadística, la cuál es mostrada a continuación:

*[Stat1: **received** out_of_order **missing** early **late** codec]*

Donde:

Received: Representa al número total de paquetes recibidos por el cliente.

Missing: Representa al número de paquetes que el cliente requirió pero nunca llego.

Late: Representa al número de paquetes recibidos con retraso.

Entonces, la fórmula sería la siguiente:

$$AL = \frac{Missing}{Received}$$

Fórmula 4.3

$$APD = \frac{Late}{Received}$$

Fórmula 4.4

4.2.2.4 Indicador de Calidad de Vídeo – QV

El segundo factor en relevancia para la retransmisión de vídeo es la calidad de recepción de la imagen. Aunque los problemas con la calidad de imagen no tienen tanto impacto como los problemas con el sonido, las altas expectativas que podría tener el servicio hacen que este tipo de incidencias lleguen a defraudar a los usuarios.

Esta métrica intenta determinar la calidad de transmisión de vídeo percibida por los clientes. Para ello se calcula el porcentaje de peticiones sin problemas durante la transmisión de vídeo, es decir, sin pérdidas de paquetes de vídeo y sin reenvíos fallidos.

Para evaluar este indicador se utiliza una tasa llamada Tasa de pérdidas de vídeo, la cual es explicada a continuación:

4.2.2.4.1 Tasa de Pérdidas de Vídeo – VL

Al igual que con la Tasa de Pérdidas de Audio, la Tasa de Pérdidas de Vídeo estudia la calidad de transmisión centrándose exclusivamente en el número de paquetes de vídeo perdidos:

$$VL = \frac{Paquetes\ Perdidos\ Video}{Paquetes\ Totales\ Video}$$

Fórmula 4.5

A través del Helix Server, es posible obtener las estadísticas de esta métrica usando el cuarto tipo de estadística, cuyos parámetros se muestran a continuación:

*[Stat4: stream_number | mime_type | codec | **received** | **lost** | resent | average_bandwidth | current_bandwidth | ;...information for next stream... | transport turboplay duration clip_end]*

Donde:

Lost: Número de paquetes perdidos.

Received: Número de paquetes recibidos por el cliente.

Entonces, la fórmula sería la siguiente:

$$VL = \frac{Lost}{Received}$$

Fórmula 4.6

4.2.2.5 Indicador de Espera – WI

Tal y como se había comentado con anterioridad, los reproductores disponen de un buffer que les ayuda a mitigar posibles problemas de transmisión de datos durante la reproducción de los vídeos.

Este buffer se carga al inicio de la reproducción. Por tanto, cuando se solicita el visionado de un vídeo se invierte cierto tiempo en la realización de la gestión asociada al protocolo correspondiente (RTSP, MMS, PNA, etc.) y un pequeño tiempo durante el cuál se carga el buffer de reproducción. Si este tiempo de inicio es demasiado elevado, los usuarios pueden llegar a inquietarse provocando un súbito abandono de la petición.

El Indicador de Espera intenta detectar este tipo de problemas, mediante el cálculo del porcentaje de peticiones con tiempo de inicio menor de 10 segundos. La utilización combinada de esta métrica y la de Entregas Erróneas permite detectar problemas durante la distribución de los contenidos.

A través del Helix Server es posible extraer esta métrica usando el parámetro "timestamp" que se encuentra incluido en el estilo 4, cuyos parámetros se muestran a continuación:

*IP_address - - **[timestamp]** "GET filename protocol/versión" http_status_code bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time* sent_time *resends failed_resends [stream_components] [start_time] server_address average_bitrate packets_sent.*

Donde:

Timestamp: Indica el tiempo que el cliente acceso al servicio de vídeo streaming. El tiempo se calcula a través de una diferencia aritmética entre el primer log generado en la inicialización del vídeo y el log generado cuando se visualiza el vídeo.

4.2.2.6 Indicador de Interrupción Deseada – ES

También es importante que los vídeos terminen mediante expreso deseo del usuario ó cuando se agoten los contenidos, que no es el caso para TV Móvil, puesto que es una información continua. Otro de los problemas que podrían reducir la satisfacción de los usuarios de los servicios tipo streaming es el de los cortes durante la reproducción de los vídeos. En este caso no se trata de paradas momentáneas, sino cortes que obligan al usuario a volver a solicitar la reproducción del vídeo.

El Indicador de Interrupción Deseada intenta contabilizar las peticiones que han terminado correctamente. Para ello se calcula el porcentaje de peticiones que terminan con la interacción *STOP* ó alcanzan el tiempo máximo de reproducción. A través del Helix Server es posible extraer esta métrica usando el tercer tipo de estadística, el cual contiene la siguiente información:

*[Stat3: **timestamp** | **elapsed_time** | **action** |;]*

Donde:

Timestamp: Indica el tiempo en milisegundos de cuando la acción ocurrió. Es relativo al tiempo de conexión del cliente.

Elapsed_time: Representa a la duración en milisegundos que duro la acción.

Action: Representa las diversas acciones presentadas, tales como: STOP ó PAUSE.

4.2.2.7 Indicador de Calidad Esperada de Reproducción

Uno de los parámetros que es necesario configurar durante la producción de los vídeos es el ancho de banda al que van destinados. Durante el proceso de producción debe proporcionarse un cierto ancho de banda para que el software correspondiente realice los ajustes necesarios en la calidad del vídeo. Este software se encargará de adaptar esa calidad a las capacidades de conexión de los clientes.

Si se producen contenidos con una calidad alta es posible que los clientes no puedan reproducir los vídeos debido a la capacidad de sus conexiones, principalmente si es que usan GPRS, cuya tasa bordea los 40kbps. De igual forma, si los vídeos se producen con una calidad muy baja, es posible que no se cumplan las expectativas de los clientes en cuanto a la calidad esperada de reproducción.

Es necesario realizar un estudio continuo de la capacidad de los clientes para realizar un ajuste más preciso de este parámetro. Para medir este indicador se utilizan dos métricas que son descritas a continuación:

4.2.2.7.1 Deterioro en la Calidad Esperada de Audio – AD

Durante la producción de los vídeos, se suponen ciertas capacidades de transmisión en los clientes, escogiendo los parámetros de calidad oportunos. Las diferencias de anchos de banda entre lo que se espera y lo que es realmente disponible para los clientes puede redundar en una pérdida de calidad notable.

Esta métrica pretende detectar problemas durante la transmisión de audio debido a esta diferencia de anchos de banda. Para calcular el Deterioro en la Calidad Esperada de Audio se utiliza la siguiente ecuación:

$$AD = \begin{cases} OAB \geq EAB & 0 \\ OAB < EAB & 1 - \frac{OAB}{EAB} \end{cases}$$

Fórmula 4.7

Donde OAB es la tasa de transferencia de audio obtenida durante la reproducción (bitrate) y EAB es la tasa de transferencia esperada durante la producción del video. A través del Helix Server y el Helix Producer, es posible obtener las estadísticas de esta métrica usando el segundo tipo de estadística, tal como se muestra a continuación:

*[Stat2: **bandwidth** available highest lowest average requested received late rebuffering transport startup codec]*

Donde:

Bandwidth: Es el ancho de banda del audio en bits por segundo. Este parámetro representaría al OAB.

EAB: El EAB esta representado por el parámetro configurado en el Helix Producer.

4.2.2.7.2 Deterioro en la Calidad Esperada de Vídeo – VD

La métrica del Deterioro en la Calidad Esperada de Audio tiene su homóloga para el vídeo, que es capaz de detectar problemas durante la transmisión de los paquetes de vídeo debidos a las diferencias de anchos de banda. Para su obtención se utiliza la siguiente fórmula:

$$VD = \begin{cases} OVB \geq EVB & 0 \\ OVB < EVB & 1 - \frac{OVB}{EVB} \end{cases}$$

Fórmula 4.8

Donde OVB es la tasa de transferencia obtenida durante la reproducción (bitrate) y EVB es la tasa de transferencia esperada durante la producción de los vídeos. A través del

Helix Server y el Helix Producer, es posible obtener las estadísticas de esta métrica usando el cuarto tipo de estadística, tal como se muestra a continuación:

*[Stat4: stream_number | mime_type | codec | received | lost | resent | **average_bandwidth** | current_bandwidth | ;…information for next stream… | transport turboplay duration clip_end]*

Donde:

Average_Bandwidth: Representa al ancho de banda promedio del video en bits por segundo. Este parámetro representaría al OVB.

EVB: El EVB esta representado por el parámetro configurado en el Helix Producer.

4.2.3 Métricas de Contenidos

Las Métricas de Contenidos pretenden evaluar la aceptación que los vídeos ofrecidos tienen entre los usuarios del servicio. Si bien es cierto que las métricas planteadas anteriormente permitiría al operador mejorar la calidad del servicio, es importante también tener una perspectiva menos técnica y más práctica del servicio, es decir se deben considerarse otros factores como por ejemplo el interés que despiertan los contenidos del servicio.

Estas métricas son usadas para conocer la calidad de los contenidos ofrecidos a través de parámetros como el porcentaje de visionado, el impacto respecto al resto del servicio, etc. Como resultado de su aplicación pueden sacarse una serie de conclusiones importantes.

La producción de los vídeos es un proceso muy costoso en tiempo y recursos. A través de estas métricas es posible saber si la cantidad de vídeo producida es suficiente, demasiado corta ó demasiado larga. La comparación de los resultados obtenidos por las métricas puede indicar qué secciones ó qué tipo de contenidos son los más interesantes para los usuarios del servicio, así como para determinar si es necesario implementar un servicio continuo ó solamente bajo demanda, por ejemplo, las últimas noticias, algunas

novelas ó goles del descentralizado, etc. El resultado de estas comparaciones indicará qué contenidos hay que promocionar y qué contenidos deben abandonarse por constituir una total pérdida de tiempo y recursos.

4.2.3.1 Interés a Priori

Como sucede en las páginas Web, a los vídeos se accede desde un enlace situado en otra página. En este enlace pueden proporcionarse datos sobre el vídeo como el título, el autor ó un resumen de sus contenidos. Esta descripción levanta una serie de expectativas en los usuarios que les incita a la reproducción del vídeo. En ese momento los usuarios no son conscientes de aspectos como la calidad de reproducción, la capacidad de su conexión, la calidad de redacción de los contenidos, etc.

Es importante por tanto diferenciar entre la expectativa que tiene un vídeo a partir de su descripción y el interés real mostrado por los usuarios durante la reproducción. Es posible que un usuario se sienta defraudado por el contenido del vídeo una vez que ha contemplado unos segundos del mismo.

El Interés a Priori solamente evalúa las intenciones iniciales de los usuarios, para ello se contabilizan las peticiones registradas en el sistema para usuarios diferentes. A través de este indicador puede comprobarse la calidad de la descripción aportada en la página en la que residen los enlaces a los vídeos. Además, esta métrica puede utilizarse para orientar las temáticas del servicio, es decir, utilizando esta métrica es posible detectar qué temáticas tienen una mayor aceptación en los usuarios.

A través del Helix Server es posible obtener esta métrica usando el estilo 4, cuyos parámetros se muestran a continuación:

IP address *- - [timestamp] "GET filename protocol/versión" http_status_code bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time sent_time resends failed_resends [stream_components] [start_time] server_address average_bitrate packets_sent.*

Donde:

IP_address: Representa la dirección IP asignada a cada cliente cuando accede al servidor de streaming.

4.2.3.2 Interés Real del Servicio

Como se había comentado en el Interés a Priori, es importante diferenciar entre las expectativas que tiene un vídeo y el interés real mostrado por los usuarios durante la reproducción del mismo. Es posible que un usuario se sienta defraudado por los contenidos de un vídeo, una vez que ha contemplado unos segundos del mismo. O quizás, es posible que los usuarios se sientan decepcionados con la calidad en la que están producidos los vídeos. Habría entonces que analizar un posible incremento en la calidad de producción, teniendo en cuenta que deben evitarse posibles consecuencias sobre la calidad de reproducción posterior.

El Interés Real puede calcularse contabilizando las peticiones de usuarios diferentes en las que el tiempo enviado sea mayor de 10 segundos. A través del Helix Server es posible obtener esta métrica utilizando el estilo 4, que esta compuesta por los siguientes parámetros:

IP_address - - [timestamp] "GET filename protocol/versión" http_status_code bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time ***sent time*** *resends failed_resends [stream_components] [start_time] server_address average_bitrate packets_sent.*

Donde:

Sent_Time: Representa la duración total en segundos de transmitir el contenido multimedia al cliente.

4.2.3.3 Indicador de Visionado – VP

Una vez que un usuario ha elegido visualizar un vídeo, mostrando así su interés a priori, y que ha visto determinado tiempo de reproducción, mostrando un interés real, es importante cuantificar cuánto se ve del vídeo.

Esto último es importante, pues el hecho de implementar servicios de video, por ejemplo para el caso de vídeos bajo demanda, acarrearian en gastos adicionales por la producción de estos videos. Por lo tanto, es importante saber a ciencia cierta qué porcentaje de los vídeos se está visualizando. Si el porcentaje de visualización es muy pequeño, entonces es porque están produciendo vídeos demasiado largos. Puede reducirse la duración de los vídeos ahorrando espacio de disco duro y en tiempo de producción. Si por el contrario el porcentaje de visualización es muy grande, puede ser interesante producir vídeos más largos, ya que los usuarios han mostrado un alto grado de interés en la información solicitada.

La métrica se basa en contabilizar los porcentajes de vídeo visualizados por los usuarios, contrastándolos con el número de peticiones totales. A través del Helix Server es posible obtener esta métrica usando el estilo 4 compuesta por los siguientes parámetros:

IP address *- - [timestamp]* ***"GET filename protocol/versión"*** *http_status_code bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time sent_time resends failed_resends [stream_components] [start_time] server_address average_bitrate packets_sent.*

Donde:

IP_address:	Representa la dirección IP del cliente. Esta puede ser utilizada para calcular la cantidad de clientes.
GET_filename_protocol/versión:	Representa la ruta y el archivo que el usuario accede, así como el tipo de protocolo y la versión que utiliza.

4.2.3.4 Impacto de Contenido – CI

No obstante, las métricas anteriores siguen sin contemplar casos extremos. Es posible que un único usuario acceda a un vídeo determinado y vea el total del vídeo. De esta forma se estaría falseando la información del Indicador de Visionado.

Esta métrica permitiría comparar los vídeos ó secciones entre sí, permitiendo decidir cuál de ellos es el mejor ó cuál debe potenciarse más. Para ello se utiliza una métrica que

evalúa la aceptación que un vídeo ha tenido entre los usuarios. Esta métrica, ó Métrica de Impacto, combina el porcentaje de visualización con la popularidad que tiene un vídeo. La fórmula es la siguiente:

$$CI_{video} = VP_{video} \times PS_{video}$$

Fórmula 4.9

4.2.4 Métricas de Popularidad

Las Métricas de Popularidad pueden utilizarse para cuantificar la aceptación que el servicio tiene entre los usuarios y la difusión del servicio. Al contrario que las métricas anteriores, que trataban de comprobar la calidad de las reproducciones y el grado de satisfacción de los usuarios que ya han accedido al servicio, este tipo de métricas intentan evaluar aspectos evolutivos del servicio.

Una aplicación de estas métricas es de conocer el número de usuarios diferentes que han visitado el servicio. Otra aplicación es saber cuántos usuarios vuelven al servicio, es decir, cuántos usuarios realizan más de un acceso. Esto es un indicativo de la satisfacción que los clientes sienten a la hora de reproducir los vídeos.

4.2.4.1 Popularidad del Servicio – PS

Puede definirse la Popularidad del Servicio ó de un vídeo, como el número de accesos registrados por usuarios diferentes. Se consideran solamente accesos de usuarios diferentes para evitar situaciones en las que sólo un usuario realiza múltiples peticiones al servicio ó a un vídeo específico, caso en el que no se puede hablar de popularidad.

Puede hablarse de popularidad a nivel del servicio, pero también de popularidad a nivel de una sección ó un vídeo determinado. Una alta popularidad de una sección se traduce en que debe fomentarse esa sección con la creación de nuevos vídeos. Por otro lado, una alta popularidad de un vídeo quiere decir que el vídeo en sí ha tenido una gran aceptación. Podría darse el caso por ejemplo, que un vídeo presente una alta popularidad pero en una sección de bajo interés. Esto podría ser aprovechado por el área de Marketing como punto de palanca para aumentar el interés en esa sección. A través del

Helix Server esta métrica podría ser obtenida usando el estilo 4, que esta compuesta por los siguientes parámetros:

IP_address *- - [timestamp] "GET filename protocol/versión" http_status_code bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time sent_time resends failed_resends [stream_components] [start_time] server_address average_bitrate packets_sent.*

Donde:

IP_address: Representa la dirección IP del cliente. Esta puede ser utilizada para calcular la cantidad de clientes diferentes.

4.2.4.2 Fidelidad del Servicio

Siempre que un usuario realiza más de un acceso al servicio ó a un vídeo en particular, se está ante un caso de fidelidad. Es importante estudiar este factor, debido a que se podría encontrar ante usuarios que son ampliamente receptivos a ciertos contenidos. Los usuarios que están satisfechos con el servicio ofrecido pueden volver, casi con toda probabilidad, a reproducir otros vídeos. Igualmente, pueden servir como método de difusión del servicio, al recomendar este servicio a otras personas.

Esta situación es indicativa de que el servicio presenta unos estándares de calidad muy elevados, aunque esta lectura puede también realizarse desde una perspectiva de un vídeo en particular ó de una sección determinada.

Son de especial interés aquellas secciones que presentan tanto una alta popularidad como una alta fidelidad. Estas secciones pueden aumentar el número de accesos realizados al servicio, por lo que se debería poner especial atención para la planificación de las plataformas ó licencias de los servidores.

Una fórmula para contabilizar la fidelidad es la de calcular como el porcentaje de usuarios que utiliza el servicio, una sección ó un vídeo más de 2 veces. A través del Helix Server es posible obtener esta métrica usando el estilo 4, que esta compuesta por los siguientes parámetros:

IP address *- - [timestamp]* ***"GET filename protocol/versión"*** *http_status_code bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time sent_time resends failed_resends [stream_components] [start_time] server_address average_bitrate packets_sent.*

Donde:

IP address:	Representa la dirección IP del cliente. Esta puede ser utilizada para calcular la cantidad de usuarios.
GET_filename_protocol/versión:	Representa la ruta y el archivo que el usuario accede, así como el tipo de protocolo y la versión que utiliza. Este parámetro puede ser utilizado para saber cuál es el vídeo que el usuario acceso.

4.2.5 Métricas de Eficiencia

Estas métricas intenta evaluar la eficiencia del servicio, es decir, se comprueba hasta qué punto los recursos disponibles están siendo utilizados ó no. Métricas de este tipo han sido desarrolladas para otro tipo de servicios, como por ejemplo la utilización del procesador, el aprovechamiento del espacio en disco ó la ocupación de memoria. Sin embargo, los servicios de vídeo tienen una limitación que es la restricción impuesta por las licencias adquiridas.

Estas licencias se pueden materializar en dos limitaciones diferentes: un número limitado de conexiones simultáneas ó un ancho de banda de salida limitado. Si bien es cierto que el consumo de las licencias no es constante debido al carácter aleatorio en los accesos, se debe considerar para la implementación la cantidad máxima de usuarios concurrentes que podría soportar el servicio en hora de alto tráfico.

Estas métricas permitirán determinar el tipo de licencia que debe ser adquirida, considerando los márgenes de seguridad necesarios.

4.2.5.1 Aprovechamiento de Licencias

Esta métrica es útil cuando la limitación impuesta por las licencias esté en el número de accesos simultáneos. La contratación del número de licencias del servidor multimedia depende de la demanda real que tiene el servicio, con lo que es necesario comparar el número de licencias disponibles con el número de licencias consumidas.

Debe observarse con detalle la evolución de las licencias, fijándose en los picos de consumo máximos. Son estos picos los que determinarán el número de licencias a adquirir. En caso de que el consumo de licencias máximo se mantenga durante un tiempo prolongado, deberá estudiarse la adquisición de una licencia superior, con un número de accesos simultáneos mayor.

A través del Helix Server esta métrica puede ser obtenida usando el estilo 4, que esta compuesta por los siguientes parámetros:

IP_address *- -* ***[timestamp]*** *"GET filename protocol/versión" http_status_code bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time* sent_time *resends failed_resends [stream_components] [start_time] server address average_bitrate packets_sent.*

Donde:

IP_address: Representa la dirección IP del cliente. Esta puede ser utilizada para calcular la cantidad de usuarios concurrentes en un determinado momento.

Timestamp: Indica el tiempo que el cliente acceso al servicio de vídeo streaming. El aprovechamiento de licencias se calcula a través de la cantidad de usuarios concurrentes en un determinado período de tiempo.

4.2.5.2 Aprovechamiento del Canal de Salida

Otros servidores multimedia utilizan el ancho de banda de salida como limitación en las licencias adquiridas. Al igual que sucedía con el número de accesos simultáneos, el

consumo de ancho de banda real del servicio será el que indique el tipo de licencia a adquirir.

A través del Helix Server esta métrica puede ser obtenida usando el estilo 4, que esta compuesta por los siguientes parámetros:

IP address *- - [timestamp] "GET filename protocol/versión" http_status_code bytes_sent [client_info] [client_ID] [client_stats_results] file_size file_time sent_time resends failed resends [stream_components] [start_time] server_address* ***average bitrate*** *packets_sent.*

Donde:

IP_address: Representa la dirección IP del cliente.

Average_bitrate: Representa la tasa promedio del video en bits por segundo. Esta puede ser utilizada para calcular el ancho de banda simultáneo en un determinado momento.

4.3 Comercialización del Servicio

Una de las principales diferencias entre la red GPRS/EDGE y la red GSM en el manejo de llamadas de datos, es que la primera utiliza una red de conmutación por paquetes mientras que la segunda utiliza una red de conmutación por circuitos. La ventaja en utilizar GPRS para los usuarios es que ahora el operador tiene la posibilidad de facturar solamente por los paquetes de datos transmitidos y/o recibidos, mientras que usando la conexión por circuitos se tendría que facturar por el tiempo conectado, aun si no se ha pasado ninguna información durante el tiempo de conexión.

Debido a que estas aplicaciones representarían servicios de valor agregado para el operador celular, además de innovadores, no se sabría a ciencia cierta cuál sería el comportamiento ó la penetración que tendrían este tipo de servicios. Es por ello, que el factor "precio del servicio" es muy importante para no colocar una barrera demasiado alta, que podría ser contraproducente para el operador. Otro aspecto importante a considerar es el modo de comercialización del producto, no sería recomendable que se hable con

terminologías, que solamente pocas personas técnicas ó leídas puedan entender, por ejemplo al hablar de "Bytes Transmitidos / Recibidos". A las personas les interesa saber el costo pero de una manera más sencilla, sin necesidad de aprenderse esos términos y/o tener la necesidad de calcularlos. Esto también podría provocar una barrera más para el éxito de estos tipos de servicios.

Una recomendación para los operadores celulares sería facturar el servicio de videostreaming a través de un cargo fijo diario ó mensual, de tal forma, que basta que un usuario acceda a ver su casa por solo 5 minutos, ya estaría pagando por todo el día. Del mismo modo, una barrera para el servicio sería implementar una facturación por tiempo transcurrido, dado que los usuarios pensarán más de dos veces si es que realmente quieren utilizarlo debido a lo caro del producto.

Otro aspecto importante es el Marketing del producto, en este caso se debería sacar ventaja que los usuarios poseen un terminal móvil con capacidad no solo de recibir llamadas, sino también mensajes de texto e imágenes. Por todo ello, las herramientas de marketing y comercial basadas en el teléfono móvil, SMS, WAP ó MMS (Mensajería Multimedia), también llamadas de **"m-marketing"**, pueden efectivamente conseguir incrementar los ingresos y fidelizar a los clientes que tienen un dispositivo móvil. Se podría decir que los teléfonos móviles se han convertido en dispositivos indispensables para las personas principalmente por la necesidad de estar siempre comunicado. Justamente, el uso del teléfono móvil es superior al del teléfono fijo, y ya existen aplicaciones para fuerza de ventas que están utilizando el teléfono móvil como una herramienta indispensable para su trabajo.

En los últimos años varias empresas se han enfocado en el mercado de las soluciones móviles de marketing desarrollando herramientas de m-marketing orientadas a potenciar los negocios de las empresas. Siguiendo todas las premisas anteriores, existen empresas que comercializan productos con el objeto de permitir a las compañías la realización de acciones de fidelización y promoción de una manera fácil y barata a través del teléfono

móvil. De este modo, se trata de un canal de comunicación por SMS, WAP ó MMS, totalmente complementario con los ya existentes carteles, web, anuncios de prensa, radio, etc., que permite comunicarse en tiempo real, y de forma absolutamente controlada por el operador celular.

4.4 Tiempos de Implementación

Para describir en forma más detallada los pasos y tiempos que se requiere para implementar un servicio de TV Móvil se ha desarrollado un plan de proyecto (Gantt Chart) la cuál es mostrada a continuación.

Para este proyecto, se ha considerado las configuraciones que deberá realizar el operador celular de tal forma que permita el acceso de sus usuarios por la red de circuitos HSCSD y por la red de paquetes GPRS/EDGE. A su vez, se ha considerado que el tiempo de disponibilidad de los servidores desde que se envia la orden de compra al proveedor hasta recibir los servidores, tarjetas, softwares, licencias, etc., en la sala de equipos del operador es de 01 mes.

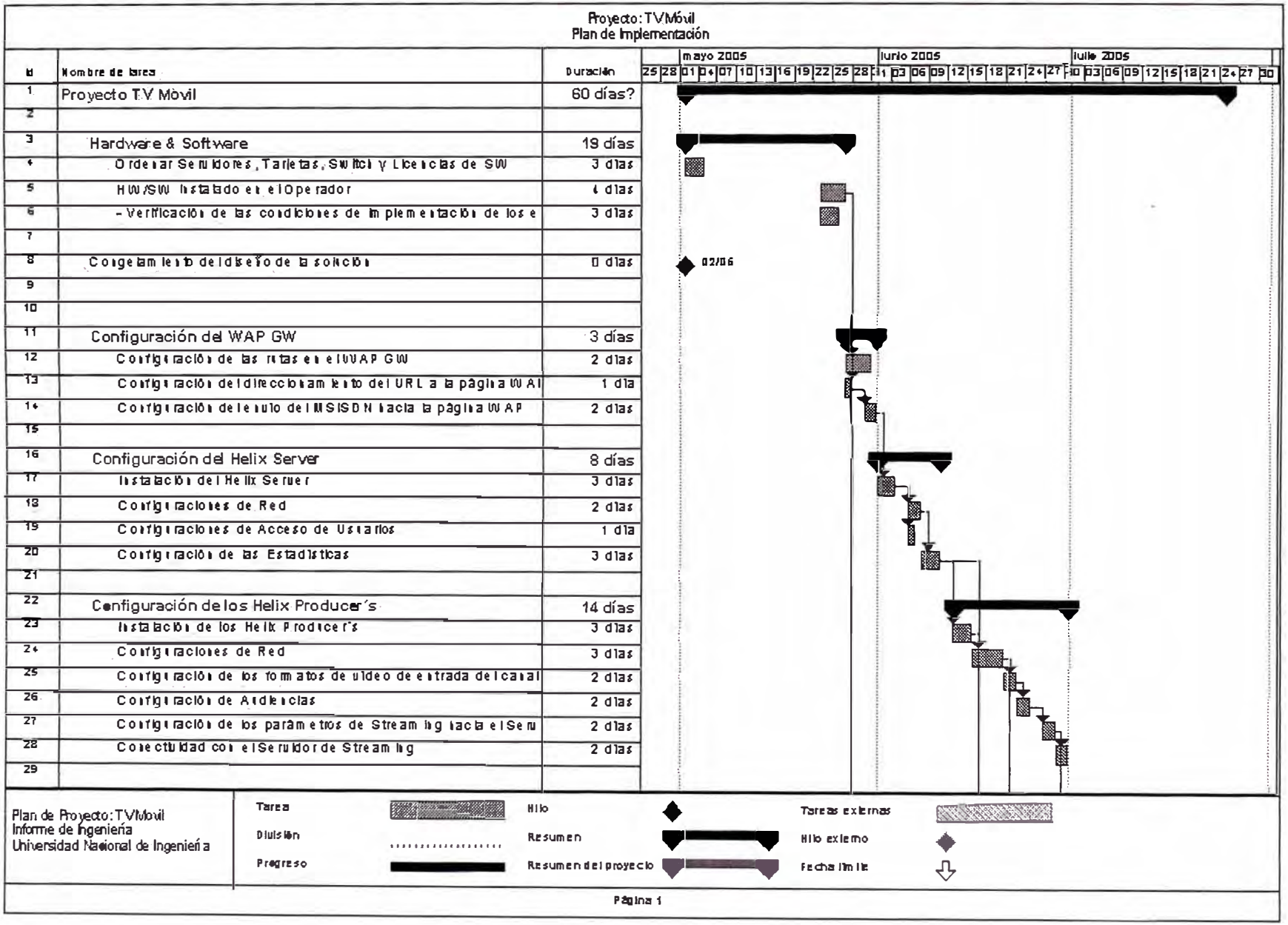
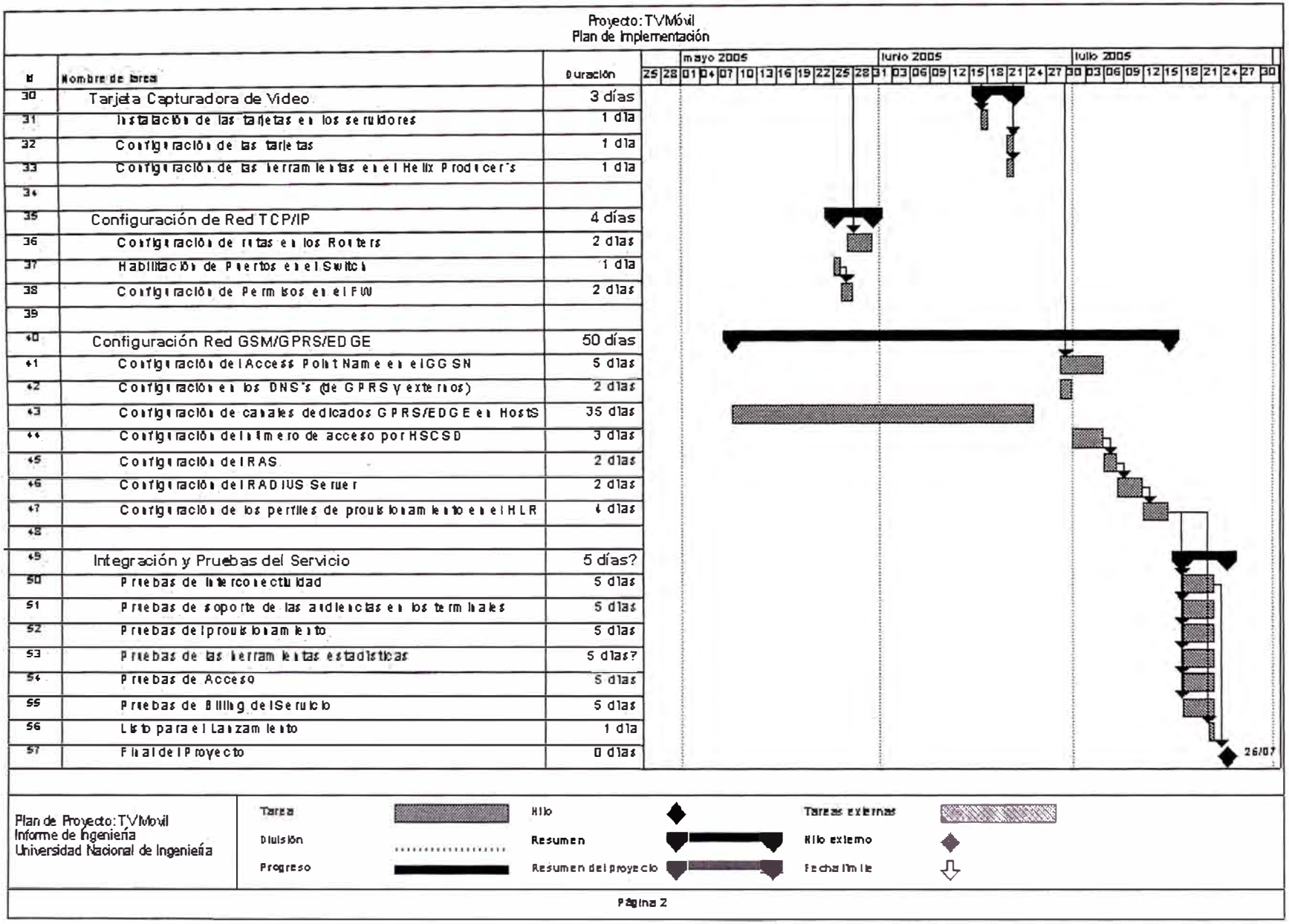


Tabla 4.3 Gantt Chart – 1era Parte



Id	Nombre de tarea	Duración
30	Tarjeta Capturadora de Video	3 días
31	Instalación de las tarjetas en los servidores	1 día
32	Configuración de las tarjetas	1 día
33	Configuración de las herramientas en el Helix Producer's	1 día
34		
35	Configuración de Red TCP/IP	4 días
36	Configuración de rutas en los Routers	2 días
37	Habilitación de Puertos en el Switch	1 día
38	Configuración de Permisos en el FW	2 días
39		
40	Configuración Red GSM/GPRS/EDGE	50 días
41	Configuración del Access Point Name en el GGSN	5 días
42	Configuración en los DNS's (de GPRS y externos)	2 días
43	Configuración de canales dedicados GPRS/EDGE en Hosts	35 días
44	Configuración del número de acceso por HSCSD	3 días
45	Configuración del RAS	2 días
46	Configuración del RADIUS Server	2 días
47	Configuración de los perfiles de provisionamiento en el HLR	4 días
48		
49	Integración y Pruebas del Servicio	5 días?
50	Pruebas de Interconectividad	5 días
51	Pruebas de soporte de las aplicaciones en los terminales	5 días
52	Pruebas del provisionamiento	5 días
53	Pruebas de las herramientas estadísticas	5 días?
54	Pruebas de Acceso	5 días
55	Pruebas de Billing del Servicio	5 días
56	Listo para el Lanzamiento	1 día
57	Final del Proyecto	0 días

Tabla 4.4 Gantt Chart – 2da Parte

4.5 Análisis de Costos

Los costos relacionados para la implementación real de un sistema de videostreaming están basados principalmente en los costos de HW/SW de los equipos y plataformas a instalar.

Para realizar un análisis de costos para detectar la viabilidad del proyecto se han considerado los siguientes puntos:

- Inicialmente el SW del Helix Server como del Servidor Apache estarían instalados en una única plataforma. Dependiendo de la demanda del servicio, se puede planificar de separar los productos en distintas plataformas. En este caso se debe tener cuidado de no generar conflicto de puertos entre el servidor de Helix y el Apache, ya que ambos utilizan el puerto 80 como HTTP (en este caso, se le configura el puerto 81 en el servidor de Helix).
- Se ha considerado que los usuarios pagarían mensualmente por dos cosas: Derecho de Activación del servicio correspondiente a USD $1 y otro pago por el uso del Servicio correspondiente a USD $5. Estos precios son bastante bajos, pero aun cobrando de esa manera se demostrará que el proyecto es viable económicamente.
- Se ha considerado un crecimiento anual progresivo de: 4500, 8600, 13800, 18700, 24600 y 35200 usuarios. Estos valores representan a menos del 1.5% de la base total de usuarios del operador celular, es decir, son números muy conservadores.
- Además se ha considerado que sólo un 30% de estos usuarios se activan el servicio y que un 15% lo utiliza por lo menos una vez. Con estos porcentajes se trata de castigar aun más el análisis.
- Estos costos son solo referenciales, pero pueden ser obtenidos de las páginas de RealNetworks (http://www.real.com) y de HP (http://www.hp.com).

Bajo estas consideraciones el estado de pérdidas y ganancias arrojan los siguientes valores:

Balance Inicial			
Intangibles			62,000.00
	Software (Helix Server, Helix Producer, Apache Server, MySQL)	60,000.00	
	Implementación / Configuración	2,000.00	
Inmueble Maquinas&Equipos		Servidores	20,000.00
	03 Servidores	15,000.00	
	Racks, Tarjetas, Cables, Switch	5,000.00	
Total Activo			82,000.00

Activación	1
Tasa de Activación	30%
Tasa de Conexión	15%
Costo*Mes	5

Gastos Fijos	
Operadores	2,000.00
Upgrade Licencias SWs / Soporte	5,000.00
Internet	1,000.00
Teléfono Fijo	200.00
Celular	200.00
Publicidad	3,000.00
Total Gastos Fijos Mensuales	11,400.00

Tabla 4.5 Estado de Pérdidas y Ganancias – 1era parte

ESTADO DE PERDIDAS Y GANANCIAS								
	Proyección de Usuarios	4,500	8,600	13,800	18,700	24,600	35,200	
		Año 0	Año 1	Año 2	Año 3	Año 4	Año 5	Total
Ingresos	Derecho de Uso del Servicio	16,200.00	30,960.00	49,680.00	67,320.00	88,560.00	126,720.00	379,440.00
	Conexión / Mes	40,500.00	77,400.00	124,200.00	168,300.00	221,400.00	316,800.00	948,600.00
	Total Ingresos	56,700.00	108,360.00	173,880.00	235,620.00	309,960.00	443,520.00	1,328,040.00
Egresos	Gastos Fijos	136,800.00	136,800.00	136,800.00	136,800.00	136,800.00	136,800.00	820,800.00
	Total Egresos	136,800.00	136,800.00	136,800.00	136,800.00	136,800.00	136,800.00	820,800.00
Ingresos - Egresos		(80,100.00)	(28,440.00)	37,080.00	98,820.00	173,160.00	306,720.00	507,240.00
Activos		82,000.00						
	Utilidad Neta	(162,100.00)	(28,440.00)	37,080.00	98,820.00	173,160.00	306,720.00	425,240.00

0.00	1.00	2.00	3.00	4.00	5.00	
(162,100.00)	(25,854.55)	30,644.63	74,244.93	118,270.61	190,448.39	
(162,100.00)	(187,954.55)	(157,309.92)	(83,064.99)	35,205.62	225,654.61	
1.00	1.00	1.00	1.00	0.00	0.00	4.00
1.00	1.00	1.00	1.00	0.00	0.00	

TIR	35%
VAN	225,654.61
PAYBACK (Años)	4.70
TASA	10.0%

Tabla 4.6 Estado de Pérdidas y Ganancias - 2da parte

Donde:

VAN – Valor Actual Neto

Mide la contribución neta, en valor presente, de todos los flujos del proyecto del operador celular. Es el valor monetario que resulta de restar la suma de los flujos descontados a la inversión inicial. Compara todos los Ingresos y Egresos esperados del proyecto en un solo momento.

La mayor dificultad en la aplicación de este método es la determinación de una tasa de descuento apropiada. Para el VAN, la tasa de descuento es la Tasa Mínima Atractiva de Retorno (TMAR), que se define como el rendimiento de la mejor alternativa del mercado supuesto que no se llevará a cabo el proyecto analizado. Para su determinación hay que tener en cuenta factores tales como: riesgo, tiempo, utilidad, sector industrial, estructura de financiamiento, etc. En general, se considera un TMAR del 10% anual.

Regla de Decisión

- Para un solo Proyecto:

  VAN > 0 : Acepta el proyecto.

  VAN = 0 : Indiferencia.

  VAN < 0 : Rechazar el proyecto.

- Para varios Proyectos:

  Escoger el proyecto de mayor VAN.

TIR – Tasa Interna de Retorno

Es la tasa de interés que hace el Valor Presente Neto igual a cero. La TIR es un índice de rentabilidad, que busca determinar hasta cuánto podría el inversionista aumentar la TMAR, para que el proyecto siga siendo aceptado.

Regla de Decisión

- Para un solo Proyecto:

  TIR > 0 : Acepta el proyecto VAN > 0.

  TIR = 0 : Indiferencia VAN = 0.

TIR < 0 Rechazar el proyecto VAN < 0.

En el análisis de estado de pérdidas y Ganancias, se observa que tanto el TIR como el VAN son mayores que cero, comprobándose entonces la viabilidad económica del proyecto (aun siendo muy conservadores con las proyecciones de usuarios). El Retorno de Inversión (Payback) para el proyecto de "TV Móvil" es de aproximadamente 4.7 años.

CONCLUSIONES

1. Se demostró que es posible ofrecer servicios en tiempo real a pesar que los requerimientos para implementarlos sean exigentes. Es decir, no es necesario esperar a redes de Tercera Generación Celular (3G) ó enlaces con anchos de banda dedicados para poder implementar esta solución. Justamente, la factibilidad técnica para la implementación de estas aplicaciones, se basa en establecer mecanismos de medición de la calidad, de tal forma de ofrecer servicios de streaming considerando los problemas y limitaciones existentes en las redes actuales (celular e Internet), por ejemplo, anchos de banda reducidos, asignación de canales en forma dinámica, variaciones del retardo, etc.
2. Se realizó un diseño e implementación del servicio TV Móvil, que es una aplicación de vídeo en tiempo real sobre una red celular de 2G-GSM / 2.5G-GPRS/ 3G-EDGE.
3. Se proveyó un conjunto de métricas específicas para el análisis y gestión de servicios de streaming facilitando la detección de problemas en la distribución del contenido, además de proporcionar un enfoque práctico a estas métricas.
4. Del trabajo realizado se concluye que la hipótesis ha sido validada, pues el diseño y arquitectura propuestos permitirían la integración de aplicaciones de Videostreaming sobre una red celular (servicio TV Móvil), haciendo posible su medición y gestión.

RECOMENDACIONES

1. Que deberían evaluarse la implementación de aplicaciones de streaming para que sea soportado por cualquier tipo de tecnología, sea CDMA, TDMA ó IDEN. Puesto que el trabajo de investigación esta basado en sí en la aplicación y no en el transporte del mismo. Aunque era necesario estudiar estas formas de transporte para entender el problema que se tendría al implementar un servicio de flujo continuo y en tiempo real.
2. Que deberían analizarse nuevas métricas que permitan mejorar la calidad del servicio a ofrecer. Por ejemplo, a parte de medir la calidad del servicio, la fidelidad de los usuarios, la popularidad y la eficiencia, es importante también analizar métricas que miden la cantidad de accesos satisfactorios (ingreso de contraseña correcta a nivel de aplicación), disponibilidad de los canales de radiofrecuencia, Consumo de Anchos de Banda en la conexión a Internet, etc.
3. Que se debería realizar un análisis técnico acerca de la implementación de otros servicios de streaming. El enfoque de utilizar en esta investigación el software de RealNetworks se debió puesto que algunos proveedores de tecnología celular han implementado el cliente RealPlayer dentro del menú de opciones en el teléfono móvil.

ANEXO A

INDICE DE FIGURAS

INDICE DE FIGURAS

ANEXO B

INDICE DE TABLAS

INDICE DE TABLAS

ANEXO C

INDICE DE FORMULAS

INDICE DE FORMULAS

ANEXO D

GLOSARIO DE TERMINOS

GLOSARIO DE TERMINOS

3GPP: Third Generation Partnership Project – Proyecto de Alianza para la Tercera Generación, creado para facilitar el desarrollo de especificaciones técnicas abiertas aceptadas para los servicios 3G, al que pertenecen varios organismos de estandarización regionales.

A: Interfaz estándar entre la BSC y el MSC, en las redes GSM.

A-bis: Interfaz entre las BTS y el BSC asociado, en las redes GSM.

Algoritmo A3: Es un algoritmo que se utiliza en el sistema GSM de telefonía móvil para la autenticación.

Algoritmo A5: Es un algoritmo que se utiliza en el sistema GSM de telefonía móvil para la encriptación de la información transmitida.

Algoritmo A8: Es un algoritmo que se utiliza en el sistema GSM de telefonía móvil para la generación de las claves de cifrado: autenticación y encriptación.

AMPS: Advanced Mobile Phone System – Sistema de Telefonía Móvil Avanzada. Estándar móvil analógico por los laboratorios Bell en la década de los 70.

ANSI: American Nacional Standards Institute – El Instituto Nacional Americano de Estándares es el organismo de normalización de Norteamérica.

ANSI-136: Estándar móvil digital norteamericano antes conocido como Interim Standard IS-136, utilizado en los sistemas TDMA.

Ancho de Banda: Bandwidth – Capacidad de información de un recurso de comunicaciones, que suele medirse, sí es digital, en bits por segundo.

APN: Access Point Name – Nombre de punto de acceso.

AUC: Authentication Center. Centro de Autenticación.

BS: Base Station – Estación Base.

BSC: Base Station Controller (Controlador de Estación Base).

CDMA: Code Division Multiple Access – El Acceso Múltiple por División de Códigos, es la técnica de acceso múltiple empleada por las interfases de aire CDMAONE (IS-95), CDMA2000 y WCDMA.

CDMAONE(IS-95): Tecnología de interfaz digital de aire de banda ancha (1.25Mhz) desarrollada por la empresa Qualcomm.

CDMA2000: Propuesta de la comunidad CDMA para un sistema estándar en los servicios 3G, como evolución de CDMA2000.

Celda: Unidad geográfica de un sistema de comunicación celular. La cobertura del servicio de un área determinada se basa en una red de células entrelazadas, cada una de las cuales tiene en el centro una estación base de radio (transmisor/receptor).

Cifrado: Proceso de transformación de la información, mediante un código y un proceso matemático, que la hace ininteligible para todo el que no conozca la clave de la comunicación.

Código PIN: Personal Identification Number – Código de identificación, de cuatro cifras, que tiene cada usuario para acceder a los servicios de su terminal móvil y que se le pide al activarlo.

Comunicaciones en tiempo real: Servicio de comunicaciones (generalmente bidireccional) en el que el destino recibe instantáneamente la información enviada en un flujo continuo.

Conmutación de circuitos: La base de la gestión de las llamadas telefónicas, en la que se establece una conexión de circuito entre la persona que llama y la que recibe la llamada. Esta conexión se mantiene abierta durante toda la llamada, aun cuando no se esté transmitiendo ninguna información (voz, datos, vídeo). Su alternativa es la conmutación de paquetes.

Conmutación de paquetes: Técnica de transmisión de red central con la que se divide la información en paquetes de datos que se encaminan de forma independiente a través de la red a los largo de distintas rutas, hasta su destino final. En este caso el espectro de

radio sólo se utiliza cuando realmente se están transmitiendo datos. Su alternativa es la conmutación de circuitos. GPRS es una tecnología basada en paquetes diseñada para redes móviles digitales.

EDGE: Enhanced Data rates for Global Evolution) – Tasa de Datos Mejorada para la Evolución Mundial. Es una técnica mejorada de modulación de radio para GSM y TDMA (ANSI-136) que amplia los intervalos de tiempo (timeslots) de radio hasta 48 kbps. Cuando se combina con GPRS, proporciona un ancho de banda máximo de 384 kbps por usuario.

ETSI: European Telecommunications Standards Institute – Instituto Europeo de Estándares de Telecomunicaciones. Su finalidad consiste en establecer estándares que permitan al mercado internacional de las telecomunicaciones funcionar como uno solo. Miembro del 3GPP.

FDMA: Frequency Division Multiple Access – Acceso Múltiple por División de Frecuencia. Técnica para compartir el espectro radioeléctrico, según la cual a cada uno de los usuarios se le adjudica un parte (frecuencia), distinta de la que se asigna a otros.

GGSN: Gateway GPRS Support Node – Nodo de Soporte GPRS de Gateway.

GPRS: General Packet Radio Service – Servicio General de Radio por Paquetes. Mejora de la red GSM que introduce la transmisión de paquetes de datos. Utiliza muy eficazmente el espectro de radio disponible y los usuarios reciben un acceso con un ancho de banda mayor que con una conexión por circuitos. También se puede aplicar a las redes TDMA (ANSI-136).

GSM: Global System for Mobile Communications – Sistema Internacional para Comunicaciones Móviles. Definido inicialmente como un estándar europeo para una red telefónica celular digital que soporte el roaming entre países. GSM es ahora el principal estándar móvil digital en el mundo. Emplea una interfaz aire TDMA.

GTP: GPRS Tunnelling Protocol – Protocolo de Túnel de GPRS.

HLR: Home Location Register – Registro Local de abonados.

HSCSD: High Speed Circuit Switched Data – Especificación de la Fase 2+ de GSM, homologada por la ETSI. Se trata de un servicio multislot de transmisión de datos a alta velocidad mediante conmutación de circuitos. El HSCSD, junto con el esquema de codificación mejorado de 14.4 kbps, permite velocidades de transmisión de datos hasta 57.6 kbps, combinando varios slots de 9.6 kbps ó 14.4 kbps.

HTML: Hyper Text Markup Language – Estándar de programación para páginas Web de Internet que trabaja con textos, imágenes y vínculos, además de soportar diferentes formatos de presentación para cada uno de estos elementos.

HTTP: HyperText Transfer Protocol – Protocolo de transferencia de hipertexto.

IDEN: Integrated Digital Enhanced Network – Lanzado por Motorota en el año 1994, es un sistema privado de radio (telefonía, datos y mensajería). Su ventaja central es la instantaneidad, es decir, basta con apretar un botón para comunicarse simultáneamente con las personas.

IMEI: Internacional Mobile station Equipment Identity – Identidad internacional de equipo móvil.

IMSI: Internacional Mobile Subscriber Identity – Identidad internacional de abonado móvil.

IMT-2000: Internacional Mobile Communications 2000 – El sistema de Comunicaciones Móviles Internacionales 2000 es una iniciativa de la UIT para disponer de un servicio que proporcione acceso de radio a la infraestructura de telecomunicaciones de todo el mundo a través de sistemas terrestres y por satélite, atendiendo a las necesidades de usuarios fijos y móviles en redes públicas y privadas. En otras palabras, servicios de tercera generación (3G).

IP: Internet Protocol.

IS: Interim Standard – ISO. Denominación asignada en Estados Unidos a las especificaciones iniciales para algunos de los sistemas de comunicaciones móviles.

IS-54: D-AMPS (Digital AMPS). Tecnología TDMA (Time Division Multiple Access) utilizada por D-AMPS en la banda de 800 Mhz.

IS-95: CDMA (Code Division Multiple Access). Tecnología CDMA en la banda de 800 y 1900 (banda PCS) Mhz.

IS-136: D-AMPS con tecnología TDMA en las bandas de 800 y 1900 Mhz.

ISDN: Integrated Services Digital Network – Red Digital de Servicios Integrados.

Itinerancia: Roaming – Posibilidad de que un usuario de teléfono móvil ó inalámbrico viaje de red en red, con absoluta continuidad de comunicación.

JPEG: Joint Photographic Experts Group.

LA: Location Area – Área de Localización.

LAN: Local Area Network – Red de área local.

MAP: Mobile Application Part – Parte de aplicación móvil.

MMS: Multimedia Messaging Service – Servicio de Mensajes Multimedia. Permite transmitir imágenes en movimiento, gráficos y sonidos, junto con el texto de los mensajes.

MPEG: Moving Picture Experts Group.

MS: Mobile Station – Estación móvil.

MSC: Mobile Switching Center – Central de Conmutación Móviles.

MSISDN: Mobile Station Integrated Service Digital Number – Número ISDN de estación móvil.

PCS: Personal Communications Service – Término genérico para referirse al servicio de comunicaciones personales móviles del mercado masivo, independiente de la tecnología empleada para prestarlo.

PDN: Packet Data Network – Red pública de datos por paquetes.

PDP: Packet Data Protocol – Protocolo de datos por paquetes.

PDU: Packet Data Unit – Unidad de datos por paquetes.

PLMN: Public Land Mobile Network – Red Pública de Comunicaciones Móviles Terrestres.

QoS: Quality of Service – Calidad de Servicio.

RADIUS: Remote Authentication for Dial In User Service – Autenticación remota para servicio de usuario de marcación.

RAS: Remote Access Server – Servidor de acceso remoto.

Roaming: La itinerancia es una funcionalidad de las redes móviles que permites utilizar los servicios incluso cuando el terminal se encuentra en otra red, distinta a la que se ha suscrito.

RTCP: Real Time Transport Control Protocol.

RTP: Real Time Protocol.

RTSP: Real Time Streaming Protocol.

Servicios 3G: Abreviatura de servicios de "tercera generación", aplicados generalmente a los servicios móviles de banda ancha.

SGSN: Serving GPRS Support Node – Nodo servidor de GPRS.

SIM: Subscriber Identity Module – Pequeño circuito impreso colocado en un soporte de plástico que se coloca en el teléfono GSM para que éste pueda ser conectado a la red móvil. La tarjeta SIM desempeña dos funciones primarias en la red GSM: la de control de acceso a la red y la de personalización del servicio. Contiene la información sobre el usuario, la clave de seguridad y la memoria para almacenar números de teléfono.

SIM Application Toolkit: Tarjeta SIM con mayores prestaciones informáticas y que incorpora facilidades de diálogo con el terminal móvil.

SMS: Short Message Service – Servicio disponible en las comunicaciones móviles digitales que permite el envío y la recepción de mensajes a través del centro de mensajes del operador celular.

SS7: Signalling System Number 7 – Sistema de Señalización No. 7.

SSN: Subsystem Number – Número de subsistema.

Streaming: Servicios multimedia sobre redes en tiempo real.

TACS: Total Access Communications System – Sistema de comunicaciones móviles analógico, similar al AMPS, desarrollado inicialmente por Motorota, que se lanzó comercialmente en el Reino Unido en el año 1985.

TCP/IP: Protocolo de datos que se usa en Internet. El primero (TCP) se encarga de dividir en paquetes la información de origen, para luego recomponerla en el destino, mientras que el segundo (IP) se responsabiliza de encaminarla, mediante routers, adecuadamente a través de la red.

TDMA (Time Division Multiple Access): El Acceso Múltiple por División de Tiempo es una técnica digital empleada por las actuales interfases de aire GSM, TDMA y PDC, que asigna períodos temporales distintos (timeslots) a cada una de las comunicaciones.

TDMA (ANSI-136): TDMA se ha adoptado como el nuevo estándar móvil digital (D-AMPS).

TIA: Telecommunications Industry Associations – La Asociación del Sector de Telecomunicaciones es el organismo estadounidense para la normalización de las telecomunicaciones.

TMSI: Temporary Mobile Subscriber Identity – Identidad temporal de abonado móvil.

UDP: User Datagram Protocol – Protocolo de Datagrama de Usuario.

UIT: Unión Internacional de Telecomunicaciones. Órgano de las Naciones Unidas responsable de la coordinación de las actividades internacionales relacionadas con las telecomunicaciones, especialmente en las áreas de definición de estándares, asignación de radio y legislación. Recientemente se ha reestructurado en tres sectores: el de normalización de telecomunicaciones (ITU-T), establecido para gestionar todas las actividades de normalización del antiguo CCITT, el de comunicaciones vía radio (ITU-R), y el sector de desarrollo, que gestiona la asistencia a países en vías de desarrollo en materia de telecomunicaciones.

UMTS: Universal Mobile Telecommunications System – El Sistema Universal de Telecomunicaciones Móviles es el sistema para prestar servicios de tercera generación,

que esta dentro del IMT-2000, desarrollado bajo los auspicios del ETSI y dentro del 3GPP.

URL: Unified Resource Locator.

VLR: Visitor Location Register – Registro de Localización de Visitantes.

VPN: Virtual Private Network – Red privada virtual.

WAE: Wireless Application Environment – Entorno de aplicación inalámbrico.

WAP: Wireless Application Protocol – El Protocolo de Aplicaciones Inalámbricas es el estándar internacional abierto para el acceso a servicios en línea (Internet) desde terminales móviles de pantalla reducida, empleando cualquier tecnología de acceso de radio.

WCDMA: Técnica de CDMA de banda ancha, que utiliza el acceso por división de códigos y portadoras con un ancho de banda de 5 Mhz para proporcionar una gran capacidad sobre las redes UMTS de 3G.

World Wide Web (WWW): Nombre que suele aplicarse a la Internet pública internacional.

WML: Wireless Markup Language – Lenguaje de programación simplificado para Internet que permite visualizar la información en los teléfonos móviles que dispongan de protocolo WAP.

WSP: Wireless Session Protocol – Protocolo de sesión inalámbrica.

WTP: Wireless Transaction Protocol – Protocolo de transacción inalámbrica.

XML: Extendend Markup Language – Lenguaje de marca extendido.

ANEXO E

EQUIPOS

Data Sheet

Cisco **AS5350**
Universal Gateway

The Cisco® AS5350 Universal Gateway is the only one rack unit (1RU) gateway supporting 2-, 4-, or 8-port T1/7-port E1 configurations that provides universal port data, voice, and fax services on any port at any time (Figure 1). The Cisco AS5350 Universal Gateway offers high performance and high reliability in a compact, modular design. This cost-effective platform is ideally suited for Internet service providers (ISPs) and enterprise companies that require innovative universal services.

Cisco Any Service, Any Port

The economic environment is prompting service providers to generate revenues quickly, improve returns from capital investments, and adapt to changing demands for various services in the market place. Cisco Any Service, Any Port (ASAP)—the architecture for rapid deployment of concurrent services on Cisco AS5000 universal gateways—allows service providers to meet these challenges. Cisco ASAP enables faster service introduction using a common platform for quick return on investment (ROI). Service providers can generate new revenue streams from multiple voice and data services such as long distance voice over IP (VoIP), managed IP telephony, VPNs, and dial-up Internet.

Your Complete Point-of-Presence Solution

The Cisco AS5350 Universal Gateway eliminates the need for switches and routers to create a point of presence (POP) or "POP-in-a-box" solution. The Cisco AS5350 has three primary universal gateway configurations: two Channelized T1 (CT1)/Channelized E1(CE1)s, four CT1/CE1s, and eight CT1/seven CE1s. It also includes integrated signaling link termination (SLT) functions for direct connection to a Common Channel Signaling System 7 (SS7/C7) signaling gateway.

The Cisco AS5350 comes with two 10/100 autosensing Ethernet ports, which are ideal for redundancy and firewall applications. Additionally, two high-speed serial ports are provided to support Frame Relay, Point-to-Point Protocol (PPP), and High-Level Data Link Control (HDLC) backhaul. All backhaul interfaces support Hot Standby Router Protocol (HSRP), and all cards and the fan tray are hot-swappable

Figure 1 Cisco AS5350 Universal Gateway

for carrier-class resiliency. The Cisco AS5350 is the only gateway in this form factor that offers universal port capability with these high-availability features.

The Cisco AS5350 also supports widely deployed routing protocols, including those generally found in high-end access servers and routers (for example, Border Gateway Protocol Version 4 [BGP v4], Open Shortest Path First [OSPF], Enhanced Interior Gateway Routing Protocol [EIGRP], and Intermediate System-to-Intermediate System [IS-IS] Protocol). This capability allows service providers and enterprises to deploy the Cisco AS5350 as a standalone universal port solution.

Cisco AS5350 Universal Gateway Enables New Cisco Services

The rich set of Cisco IOS® Software features available in the Cisco AS5350 Universal Gateway enables ISP and enterprise network managers to meet traditional dial-in access needs, including Internetwork Packet Exchange (IPX) and AppleTalk, while supporting the migration to new universal port services.

The Cisco AS5350 supports a wide range of IP-based, value-added services such as high-volume Internet access, regional- or branch-office connectivity, corporate VPNs, long distance for ISPs, international wholesale long distance, distributed prepaid calling, SS7 interconnect, wholesale dial and voice, and enhanced voice services. The Cisco AS5350 provides an ideal solution for telephony application service providers (ASPs) that would like to deploy PC-to-phone, voice portals, unified communications, IP teleconferencing, voice-enabled Web commerce, and content delivery services.

Cisco customers worldwide have proven that Cisco AS5000 universal gateways provide the flexibility, scale, reliability, and suite of services required to meet market demands. By providing the industry's broadest family of access server products with universal port digital signal processors (DSPs), Cisco Systems® makes it easy for customers to select the right starting point for a phased rollout based on revenue generation, without compromising future capabilities. Complemented by the industry's highest-rated service and support, Cisco can also provide assistance with startup, maintenance, and marketing tasks, as well as advanced and custom solutions.

Primary Features

Cisco ASAP

The Cisco ASAP architecture enables the Cisco AS5350 Universal Gateway to operate simultaneously as a network access server (NAS) and a voice gateway, delivering universal services on any port at any time. The Cisco ASAP services on the Cisco AS5350 include dial access, real-time voice and fax for local or long-distance transport, managed services (hosted IP telephony, for example), and unified communications on a call by call basis. Cisco AS5350 achieves cost savings through optimized use of the universal port access infrastructure. Service providers can now quickly capitalize on new opportunities and realize multiple revenue streams from a single access infrastructure.

Modular Architecture

All feature cards can be upgraded in the field to accommodate future technologies while providing a solution to meet today's needs. The removable system fan tray maximizes uptime.

Universal DSPs

The Cisco ASAP architecture is based on universal DSP technology. The universal DSP can execute multiple coder/decoder (codec) and modem algorithms on any DSP at any time. When the type of codec or modem required for a specific call has been determined, the DSP activates the appropriate service type in real time. When the call is determined, different signaling schemes and modem negotiations are used to determine the actual firmware code to be downloaded onto the DSP for that particular call.

Remote Access Capabilities

The Cisco AS5350 Universal Gateway takes advantage of the full-feature richness and strong routing capabilities of Cisco IOS Software. The Cisco AS5350 can be deployed in various architectures, from multiprotocol corporate networks (IP, IPX, AppleTalk, and NetBEUI, for example) to service provider IP networks. In addition, the Cisco AS5350 fully supports the specialized needs of AOL, MSN, and other content-oriented dialup services through PPP, Layer 2 Tunneling Protocol (L2TP), or Transmission Control Protocol Clear (TCP Clear) connections.

The Cisco AS5350 also supports the most complete set of access protocols of any access server, including PPP, IPX Control Protocol (IPXCP), AppleTalk Control Protocol (ATCP), AppleTalk Remote Access (ARA), NetBIOS Frame Control Protocol (NBFCP), NetBIOS over TCP/IP, NetBEUI over PPP, and protocol translation.

Table 1 Cisco AS5350 Hardware Features and Benefits

Feature	Benefit
Up to 8-T1/E1 data, voice, or fax sessions	• Offers superior density in a compact form factor that is easy to deploy
Multiple egress interface types	• Two 10/100 Ethernet LAN connections • Two 8-MB serial connections • Trunk feature cards • Offers stackable design—low initial cost • Offers a universal port solution in one product
Universal port DSPs	• Provides flexibility in deploying services—voice, dialup, fax, ISDN termination • Service providers can deliver universal services on any port at any time
Built-in resiliency	• Hot-swappable cards and spare modems • Redundant power supply option • Three redundant backhaul methods • Thermal management and environmental monitoring • Fan tray hot-swappable while in rack • Improves network and service availability, reducing time and money lost because of outages

Table 2 Cisco AS5350 System Data

System Data	
Processor	• 250-MHz RISC processor
Memory	• 128- (default) to 512-MB SDRAM (maximum) • 64- (default) to 128-MB shared I/O (maximum) • 8- (default) to 16-MB boot Flash (maximum) • 32- (default) to 64-MB system Flash (maximum) • 2-MB Layer 3 cache
Feature card slots	• Three slots
Egress ports	• Two 10/100-MB Ethernet ports • Two 8-Mbps serial ports • T1/E1 DS1 trunk feature cards

Table 3 Cisco AS5350 Chassis Data

Chassis Data	
Dimensions (H x W x D)	1.75 x 17.5 x 20.5 in. (1RU)
Weight	22 lb (fully loaded two-PRI configuration)
Normal operating conditions	0 to 40 C -200 to 10,000 ft elevation

Table 4 Cisco AS5350 Power Supply Data

Input Description	Input Specifications
Input power (AC unit)	114 to 140W (maximum)
Input voltage (AC unit)	100 to 240 VAC
Input current (AC unit)	2A (maximum), 1A (typical)
Input frequency (AC unit)	50 to 60 Hz
Input power (DC unit)	114 to 140W (maximum)
Input voltage (DC unit)	-48 to -60 VDC
Input current (DC unit)	3.0A (maximum), 2.0A (typical)

Table 5 Overview of Cisco AS5350 Protocols

Protocols	
LAN protocols	• IP, IPX, AppleTalk, DECnet, ARA, NetBEUI bridging, HSRP, 802.1Q
WAN protocols	• Frame Relay, PPP, HDLC (leased line)
Routing protocols	• Routing Information Protocol (RIP), RIPv2, OSPF, IGRP, EIGRP, BGPv4, IS-IS, AT-EIGRP, IPX-EIGRP, Next Hop Resolution Protocol (NHRP), AppleTalk Update-Based Routing Protocol (AURP)
QoS protocols	• IP Precedence • Resource Reservation Protocol (RSVP) • Weighted Fair Queuing (WFQ) • Weighted Random Early Detection (WRED) • Multichassis Multilink PPP (MMP) fragmentation and interleaving • 802.1P
Access protocols	• PPP, Serial Line Internet Protocol (SLIP), TCP Clear, IPXCP, ATCP, ARA, NBFCP, NetBIOS over TCP/IP, NetBEUI over PPP, protocol translation (PPP, SLIP, ARA, X.25, TCP, local-area transport [LAT], Telnet), and XRemote
Bandwidth optimization	• Multilink PPP (MLP), TCP/IP header compression, Bandwidth Allocation Control Protocol (BACP), bandwidth on demand, traffic shaping
Voice compression	• G.711, G.723.1 (5.3K and 6.3K), G.728, G.729ab, G-Clear, GSM-FR
DSP voice features	• Echo cancellation, programmable up to 128 ms • Transparent transcoding between A-law and mu-law encoding • Voice activity detection, silence suppression, comfort noise generation • Fixed and adaptive jitter buffering • Call progress tone detection and generation—Dial tone, busy, ring-back, congestion, and reorder tones with local country variants • Dual Tone Multifrequency (DTMF), Multifrequency continuity testing

Table 5 Overview of Cisco AS5350 Protocols (Continued)

Protocols	
Voice and fax signaling protocols	• H.323v2, H.323v3, H.323v4, SIP, MGCP 1.0, TGCP 1.0, VoiceXML, RTSP, ESMTP • T38 Real-Time Fax Relay • T37 fax store and forward • Fax passthrough • Modem passthrough • Fax detection • Open Settlements Protocol (OSP) • Media Resource Control Protocol (MRCP) • Text to Speech (TTS) servers • Automatic Speech Recognition (ASR) servers
SS7	• Integrated SLT functionality
Network security	• RADIUS or TACACS+, PAP or CHAP authentication, local user/password database • DNIS, CLID, call-type preauthentication • Inbound/outbound traffic filtering (including IP, IPX, AppleTalk, bridged traffic) • Network Address Translation (NAT) and dynamic access lists • SNMPv2, SNMPv3
VPN	• IP Security (IPSec) and policy enforcement (RADIUS or TACACS+) • L2TP, Layer 2 Forwarding (L2F), and generic routing encapsulation (GRE) tunnels • Firewall security and intrusion detection • QoS features (committed access rate, Random Early Detection, IP Precedence, policy-based routing)
Channelized T1	• Robbed-bit signaling; Loop Start, Immediate Start, and Wink Start protocols
Channelized E1	• CAS, E1 R1, E1 R2, leased line, Frame Relay, G.703, G.704
ISDN protocols supported	• Sync-mode PPP, V.120, V.110 at rates up to 38400 bps • Network- and user-side ISDN • DoVBS • NFAS with backup D-channel • QSIG, Feature Group B, Feature Group D

Table 6 Cisco AS5350 Compliance Data

Certification	Requirements
NEBS Certification	• Telcordia SR-3580 • GR-1089-CORE, Issue 2 • GR-63-CORE, Issue 1 • Level 3 certification based on usage and critical nature of equipment • All equipment CLEI coded • Available in TIRKS database
Safety Certifications	• UL 1950, third edition • CSA 950, third edition • EN 60950, with Amendments 1, 2, 3, and 4 • IEC 60950 • AS/NZS 3260 • TS 001
Electromagnetic Emissions and Immunity Compliance	• EN 55022B (CISPR22) • EN 300 386 • NZS/AS3548 Class B • VCCI II • FCC 47CFR15 Class B

Table 7 Cisco AS5350 Environmental Data

Environmental Specifications	
Heat dissipation	478 Btu/hr (maximum), 389 Btu/hr (typical)
AC power cable supplied with AC systems	Single power supply: 18 American wire gauge (AWG), 15-amp IEC 320 Type C13 standard cable Redundant power supply: 18 American wire gauge (AWG), 15-amp IEC 320 Type C6 standard cable
DC power cable required for DC systems	12-14 AWG stranded copper wire
Storage temperature	25 to 185°F (-40 to 85°C)
Acoustics	55 dBA max.; sound pressure level at 1m
Humidity	5 to 95 percent, noncondensing
Altitude	-200 to 10,000 ft
Reliability (at 40°C, 120 VAC and -48VDC, 140W)	7500 FITS per TR-332, (FIT = 1/MTBF) 1.5 x 10^6 hours MTBF per RIN

Cisco Systems

DATA SHEET

CISCO SECURE ACCESS CONTROL SERVER VERSION 3.3 FOR WINDOWS

The Cisco Secure Access Control Server provides a comprehensive identity networking solution and secure user experience for Cisco Intelligent Information Networks. It is the integration and control layer among all enterprise users, administrators, and the resources of the network infrastructure.

PRODUCT OVERVIEW

With the ever-increasing methods of accessing networks today, security breaches and uncontrolled user access are a primary concern. With the increased use of the Internet, network administrators are challenged to identify devices as well as users, to guarantee secure transactions and to prevent the spread of viruses and denial-of-service (DoS) attacks. These challenges exist not only at the perimeter but also inside a network. The wide adoption of IEEE 802.11 wireless LAN and the high-speed, always-on Internet connections (such as DSL and cable) make these challenges more severe from within an organization's network. Investing in identity networking technologies that can mitigate these ubiquitous security vulnerabilities is worth considering from both an operational and a return-on-investment perspective.

These changing network dynamics and increased security threats have driven new opportunities in access control management solutions. Stronger forms of authentication, such as public key infrastructure and two-factor authentication, now are being used to control users accessing corporate resources from public networks and VPN. Network administrators look for solutions that provide flexible authorization policies that are tied not only to who the user is at the end point but also to the service type to which the users have access and the type of machine they use to access the network. Lastly, the ability to track and monitor the behavior of network users, in a manner independent from the access medium through which users choose to connect, is of primary importance in isolating unwanted and excessive use of valuable network resources.

Identity networking and the ability to provision the network to user- or device-specific services are now possible with the Cisco® Secure Access Control Server (ACS). The Cisco Secure ACS is a highly scalable, high-performance access control server that operates as a centralized RADIUS server or TACACS+ server. The Cisco Secure ACS extends access security by combining authentication, user or administrator access, and policy control from a centralized identity networking solution, allowing greater flexibility and mobility, increased security, and user productivity gains. The Cisco Secure ACS reduces the administrative and management burden involved in scaling user and network administrative access to your network. By using a central database for all user accounts, the Cisco Secure ACS centralizes the control of all user privileges and distributes them to hundreds or thousands of access points throughout the network. As an accounting service, the Cisco Secure ACS reduces IT operating costs by providing detailed reporting and monitoring capabilities of network users' behavior and by keeping a record of every access connection and device configuration change across the entire network. The Cisco Secure ACS supports a wide array of access connection types, including wired and wireless LAN, dialup, broadband, content, storage, voice over IP, firewalls, and VPNs.

The Cisco Secure ACS is a key component of the Cisco Identity-Based Networking Services (IBNS) architecture. Cisco IBNS is based on port security standards such as 802.1X (IEEE standard for port-based network access control) and Extensible Authentication Protocol (EAP) to extend security authentication, authorization, and accounting (AAA) inside the LAN when, historically, access control was managed at the perimeter of the network. New policy controls (such as per-user quotas, virtual LANs [VLANs], and ACLs) are possible with this new architecture, now that the authenticator (switch or wireless access point) becomes a RADIUS client capable of querying an AAA server for these controls.

The Cisco Secure ACS is also a key component of Cisco Network Admission Control (NAC). Cisco NAC is a Cisco Systems® led, multivendor program focused on limiting damage from emerging security threats such as viruses and worms. With NAC, customers can allow network access only to compliant and trusted endpoint devices (for instance, PCs, servers, and personal digital assistants) and can restrict the access of noncompliant devices. Cisco NAC is the first phase of the Cisco Self-Defending Network Initiative and is the foundation for future phases. Future phases extend endpoint and network security interoperation to include dynamic infection containment capabilities. This innovation enables compliant endpoints or other system elements to report misuse emanating from rogue or infected systems during an attack. Cisco expects to use this intelligence to dynamically quarantine infected systems from the rest of the network and significantly reduce virus, worm, and blended threat propagation.

Cisco Secure ACS is a powerful access control server with many high-performance and scalability features for any organization growing its WAN or LAN connectivity. Table 1 lists the main Cisco Secure ACS benefits.

Table 1
Main Cisco Secure ACS Benefits

Ease of use	A Web-based user interface simplifies and distributes configuration for user profiles, group profiles, and Cisco Secure ACS configuration.
Scalability	Cisco Secure ACS is built to support large networked environments with support for redundant servers, remote databases, and user database backup services.
Extensibility	Lightweight Directory Access Protocol (LDAP) authentication forwarding supports the authentication of user profiles stored in directories from leading directory vendors, including Sun, Novell, and Microsoft.
Management	Windows Active Directory and Windows NT database support consolidates Windows username and password management and uses the Windows Performance Monitor for real-time statistics viewing.
Administration	Different access levels for each Cisco Secure ACS administrator—and the ability to group network devices—enable easier control and maximum flexibility to facilitate enforcement and changes of security policy administration over all the devices in a network.
Product flexibility	Because Cisco IOS® Software has embedded support for AAA, Cisco Secure ACS can be used across virtually any network access server that Cisco sells. (The Cisco IOS Software release must support RADIUS or TACACS+.)
Integration	Tight coupling with Cisco IOS routers and VPN solutions provides features such as Multichassis Multilink Point-to-Point Protocol and Cisco IOS Software command authorization.
Third-party support	Cisco Secure ACS offers token server support for any One-Time Password vendor that provides an RFC-compliant RADIUS interface (such as RSA, PassGo, Secure Computing, ActivCard, Vasco, and CryptoCard).
Control	Cisco Secure ACS provides dynamic quotas for time-of-day, network use, number of logged sessions, and day-of-week access restrictions.

KEY FEATURES IN ACS VERSION 3.3

Cisco NAC support—Cisco Secure ACS 3.3 acts as a policy decision point in NAC deployments. Using policies that you configure, it evaluates the credentials sent to it by Cisco Trust Agent, determines the state of the host, and sends the AAA client ACLs that are appropriate to the host state. Evaluation of the host credentials can enforce many specific policies, such as operating system patch level and antivirus DAT file version. Cisco Secure ACS records the results of policy evaluation for use with your monitoring system. Policies can be evaluated locally by Cisco Secure ACS or can be the result returned from an external policy server to which Cisco Secure ACS forwards credentials. For example, credentials specific to an antivirus vendor can be forwarded to the vendor antivirus policy server.

EAP-Flexible Authentication via Secure Tunneling (FAST) support for wireless authentication—EAP-FAST is a new, publicly accessible IEEE 802.1X EAP type developed by Cisco to support customers who cannot enforce a strong password policy and who wish to deploy an 802.1X EAP type that does not require digital certificates, supports a variety of user and password database types, supports password expiration and change, and is flexible, easy to deploy, and easy to manage. For example, a customer using Cisco Extensible Authentication Protocol who cannot enforce a strong password policy and does not want to use certificates can migrate to EAP-FAST for protection from dictionary attacks. Cisco Secure ACS 3.3 adds support for EAP-FAST supplicants available today on Cisco compatible client devices and Cisco Aironet® 802.11a/b/g WLAN client adapters.

Downloadable IP ACLs—Cisco Secure ACS version 3.3 extends per-user ACL support to any Layer 3 network device that supports this feature. This includes Cisco PIX® Firewalls, Cisco VPN solutions, and Cisco IOS routers. You can define sets of ACLs that can be applied per user or per group. This feature complements NAC support by enabling the enforcement of the correct ACL policy. When used in conjunction with NAFs, downloadable ACLs can be applied differently per AAA client, enabling you to tailor ACLs uniquely per user, per access device.

Certification Revocation List (CRL) comparison—Cisco Secure ACS 3.3 adds support for certificate revocation using the X.509 CRL profile. A CRL is a time-stamped list identifying revoked certificates, which is signed by a certificate authority or CRL issuer and made freely available in a public repository. Cisco Secure ACS 3.3 periodically retrieves the CRLs from provisioned CRL Distribution Points (CDP), using LDAP or HTTP, and stores them for use during EAP-TLS authentication. If the certificate presented by the user during an EAP-TLS authentication is present in the retrieved CRL, Cisco Secure ACS fails the authentication and denies access to the user. This capability is extremely important in view of the frequent organizational changes and ensures protection of valuable company assets in case of fraudulent network use.

Machine Access Restrictions (MAR)—Cisco Secure ACS 3.3 includes MARs as an enhancement of Windows machine authentication. When Windows machine authentication is enabled, you can use MARs to control authorization of EAP-TLS and Microsoft Protected Extensible Authentication Protocol (PEAP) users who authenticate with a Windows external user database. Users who access the network with a computer that has not passed machine authentication within a configurable length of time are given the authorization of a user group that you specify and which you can configure to limit authorization as needed. Alternatively, you can deny network access altogether.

Network Access Filtering (NAF)—Cisco Secure ACS 3.3 includes NAF as a new type of Shared Profile Component. NAF provides a flexible way of applying network access restrictions and downloadable ACLs on AAA client names, network device groups, or the IP addresses of AAA clients. NAFs applied by IP addresses can use IP address ranges and wildcards. This feature introduces granular application of network access restrictions and downloadable ACLs, both of which previously supported only the use of the same access restrictions or ACLs to all devices. NAFs allow flexible network device restriction policies to be defined, a requirement common in large environments.

Cisco Security Agent integration on Cisco Secure ACS Solution Engine—Cisco Secure ACS 3.3 Solution Engine now ships with a preinstalled, standalone Cisco Security Agent. This integration into the base appliance image helps protect Cisco Secure ACS Solution Engine from Day Zero attacks. By using the new behavior-based technology available with Cisco Security Agent, the Cisco Secure ACS Solution Engine can be protected against the constantly changing threats of viruses and worms.

Replication enhancements—Cisco Secure ACS 3.3 now allows you to replicate the user and group databases separately. Replicating changes to user accounts no longer automatically requires replicating groups. Likewise, replicating groups no longer requires replicating users. This increase in replication component granularity reduces the amount of data sent between Cisco Secure ACSs during a replication event. Furthermore, a configurable replication timeout option has been added to provision for slow network connectivity between Cisco Secure ACS replication partners.

SYSTEM REQUIREMENTS

Cisco Secure ACS is available in two options: *Cisco Secure ACS Windows* and *Cisco Secure ACS Solution Engine*—a 1-RU security-hardened appliance with a preinstalled Cisco Secure ACS license.

For implementation of Cisco Secure ACS Windows, your Windows Server must meet the minimum hardware requirements listed in Table 2:

Table 2

Minimum Server Specifications for Cisco Secure ACS Windows

Processor speed	550 MHZ or faster
Memory	Minimum 256 MB RAM
Hard drive	Minimum 250 MB free disk space
Resolution	Minimum of 800 x 600 (256 colors)

The Cisco Secure ACS Solution Engine is available on a Cisco 1112 platform with the specifications shown in Table 3.

Table 3

Cisco Secure ACS solution Engine Server Specifications

Processor speed	Pentium IV, 3.2 GHz
Memory	1 GB RAM
Hard drive	80 GB free disk space
Interfaces	2 built-in 10/100 Ethernet controllers and 1 floppy disk drive

ORDERING INFORMATION

Cisco Secure ACS is available for purchase through regular Cisco sales and distribution channels worldwide. Cisco Secure ACS Windows includes all the necessary components needed for an independent installation on a Microsoft Windows workstation. Cisco Secure ACS Solution Engine is shipped with a preinstalled Cisco Secure ACS software license. Refer to Cisco Secure ACS version 3.3 Product Bulletin for product numbers.

To place an order, visit the Cisco Ordering Home Page.

Cisco 2600 Series

Cisco extends enterprise/provider-class versatility, integration, and power to branch offices with Cisco 2600 Series modular access routers. With more than 2 million 2600 Series units installed worldwide, this popular series offers network managers and service providers flexibility and investment protection in a compact, single-box solution.

BENEFITS AND ADVANTAGES

Integrated Flexible Routing and Low-density Switching

With the support of an optional 16-port 10/100 EtherSwitch® network module, branch offices can take advantage of the flexibility of integrated routing and switching functions in one unit for low port densities. This offers high-speed connections between individual desktops, servers, and other network resources in a single unit for Layer 2, and allows WAN connection at Layer 3 through the router. An optional external power chassis provides power to IP phones and Cisco Aironet® 802.11 base stations.

Integration of Content Networking and Branch-office Routing

With the integration of an optional Content Engine Network Module with branch-office routing, Cisco offers the industry's first and only router-integrated content-delivery system. Combining intelligent caching, content routing and management with robust branch-office routing, WAN bandwidth is conserved for important branch IP services such as voice over IP (VoIP), while simplifying configuration, deployment, and operations.

Versatility/Investment Protection

Thousands of field-upgradable customized solutions ensure easy migration to future network requirements. More than 80 WAN interface cards (WICs) and network modules (NMs) are shared with the Cisco 1700, 1800, 2800, 3700, and 3800 Series products. The advanced integration module (AIM) slot offers expandability for integration of advanced services, such as hardware-assisted data compression, encryption, voice and ATM hardware-assisted data compression, voice mail, and encryption.

Integration of Security and Branch-office Routing

By integrating optional VPN modules, IOS-based firewall, IOS or optional hardware-based intrusion detection, or Web site-filtering using the content engine network modules or

BENEFITS AND ADVANTAGES continued

Cisco IOS software, Cisco offers the industry's most robust and adaptable security solution for branch office routers. The optional VPN modules support 3DES, AES, and hardware-based compression. Additionally, the new Cisco Intrusion Detection System (IDS) network module allows traffic inspection at the first point of entry into the network while freeing the router CPU from processor-intensive IDS tasks.

Multiservice Voice/Data Networks

Supports up to 60 simultaneous calls, using analog and digital connections to phones, faxes, key systems, PBXs, and PSTN switches, for Cisco IP telephony networks. Delivers IP telephony enriching features including Survivable Remote Site Telephony (SRST), Cisco CallManager Express (CCME) for localized call processing, Cisco Unity® Express (CUE) for voice-mail, audioconferencing and transcoding capabilities. Using Cisco IOS quality-of-service (QoS) features, such as LLQ, CB-WFQ, WRED, CAR, RSVP, and Custom and Priority Queuing, voice traffic is digitized and encapsulated in IP packet, Frame Relay, or ATM and consolidated with data to extend multiservice infrastructure to the branch office.

Business-class DSL Connectivity

The WIC-1ADSL, WIC-1ADSL-DG, WIC-1ADSL-I-DG, WIC-1SHDSL, and WIC-1SHDSL-V2 offer business-class broadband service with scalable performance, flexibility, quality of service, and security for branch and regional offices. The Cisco 2600 Series provides the perfect solution for a variety of businesses requiring high-speed business-class DSL connectivity on a secure, high-performance, modular platform.

Interoperability/Multiprotocol Support

Offers a comprehensive set of protocols and services, including virtual private networking, firewall protection, encryption, WAN optimization, and enhanced multimedia support features.

SECURITY FEATURES

VPN

- Encryption – 3DES (SW + HW), AES (SW + HW)
- VPN QoS – Preclassification support
- Easy VPN Server and client
- MAX IPsec Tunnels Supported – 800 with VPN module
- HA – High Availability
- URL Filtering – IOS or HW (Content Engine Network Module (NM-CE))-based

IPS (Intrusion Prevention Systems)

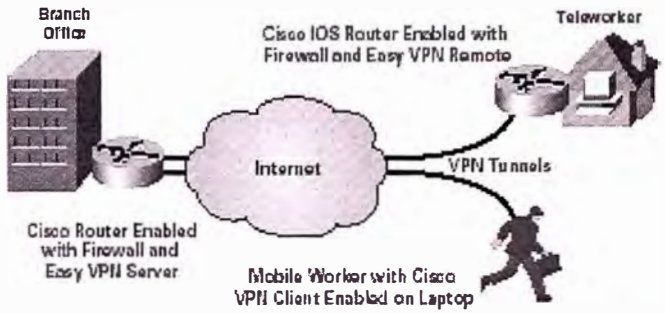
- SW-based (IOS) and HW-based options
- More than 700 signatures supported

Certifications

- ICSA – IPsec, Firewall – 2651XM
- Common Criteria – IPsec
- FIPS – 140-2, Level 2, Cisco 2821, 2821XM, 2651, 2651XM, and 2691

SECURITY FEATURES EXAMPLE

Easy VPN Server Application



WHEN TO DEPLOY

Deploy the Cisco 2600 Series when you need:

- A cost-effective solution for the long term that adapts to evolving network requirements
- Virtual private network (VPN)/extranet access with firewall protection to reduce costs and increase security for partners and employees
- Dial concentration with async, ISDN, or analog modems
- Integrated routing and switching functionality
- Complete Cisco CallManager IP Telephony Voice Gateway Router integration for analog and digital telephony interfaces
- Complete small office telephony solution using Cisco CallManager Express and Cisco Unity® Express or high-availability voice gateway for Cisco CallManager with Survivable Remote Site Telephony (SRST)
- Audioconferencing, and transcoding in conjunction with Cisco CallManager VoIP, VoFR, or VoATM toll bypass for all TDM PBXs, key systems, analog telephony devices, and the PSTN
- Integrated content delivery networking such as caching content filtering and content delivery for e-communications
- Serial device concentration of point-of-sale devices, ATMs, alarm systems, SDLC controllers with legacy terminals, and LAN devices sharing a single WAN connection
- High-speed business-class DSL connectivity on a secure, high-performance modular platform
- Support for advanced QoS features such as the Resource Reservation Protocol (RSVP), Weighted Fair Queuing (WFQ), and IP Precedence to reduce recurring WAN costs

APPLICATION EXAMPLE

Options

- Complete Cisco Voice Gateway Router functionality
- Cisco Survivable Remote Site Telephony (SRST)
- Voice-mail support with Cisco Unity Express (CUE)
- Cisco CallManager Express (CME)
- VPN-enabled routers
- Integrated stateful firewall
- Cisco IOS intrusion prevention
- WCCP for content networking
- Integrated content networking
- Dial access
- Integrated low-density switching

PLATFORM OVERVIEW

	NMs	AIMs	WICs	Fixed LAN Ports	DRAM (MB) default	DRAM (MB) max	Flash (MB) default	Flash (MB) max	Power Supply
Cisco 2610XM / 2611XM	1	1	2	1/2 FE	128	256	32	48	AC, DC, RPS
Cisco 2612	1	1	2	1 TR, 1E	32	64	8	16	AC, DC, RPS
Cisco 2620XM / 2621XM	1	1	2	1/2 FE	128	256	32	48	AC, DC, RPS
Cisco 2650XM / 2651XM	1	1	2	1/2 FE	256	256	32	48	AC, DC, RPS
Cisco 2691	1	2	3	2 FE	256	256	32*	128*	AC, DC, RPS

*Default/max

SERIES SPECIFICATIONS

Dimensions (H x W x D)	
All except Cisco 2691	1.69 x 17.5 x 11.8 in. (43 x 445 x 300 mm) 1 Rack Unit (RU) height
Cisco 2691	3.50 x 12.1 x 11.0 in. (88 x 434 x 279 mm) 2 Rack Units (RU) height
Console Port	1 (up to 115.2 Kbps)
Auxiliary Port	1 (up to 115.2 Kbps)
Integrated CSU/DSU	Yes, with optional T1/E1, 56k/64k support
Voice/Data Support	Yes
Compression	SW + HW
Encryption	SW + HW
Maximum 10/100 Ethernet Ports	18
Maximum Gig Ethernet Ports	1
Maximum Token Ring Ports	1
Maximum High-speed Serial (up to 2 Mbps)	10
Maximum Low-speed Serial (up to 128 Kbps)	22 sync, 22 async
Maximum Integrated Modems	22 analog
Maximum Number of ISDN BRI Ports	22
Maximum Number of ISDN PRI Ports	2
Minimum Cisco IOS Release	
Cisco 2610XM	IOS 12.1(14) Mainline, 12.2(12) Mainline or 12.2(8)T1
Cisco 2611XM	IOS 12.1(14) Mainline, 12.2(12) Mainline or 12.2(8)T1
Cisco 2612	IOS 12.0 Mainline
Cisco 2620XM	IOS 12.1(14) Mainline, 12.2(12) Mainline or 12.2(8)T1
Cisco 2621XM	IOS 12.1(14) Mainline, 12.2(12) Mainline or 12.2(8)T1
Cisco 2650XM	IOS 12.1(14) Mainline, 12.2(12) Mainline or 12.2(8)T1
Cisco 2651XM	IOS 12.1(14) Mainline, 12.2(12) Mainline or 12.2(8)T1
Cisco 2691	IOS 12.2(8)T1

CISCO IOS MEMORY REQUIREMENTS

Support for Cisco 2600XM Series Routers starts in Cisco IOS Mainline releases 12.1(14), 12.2(12), and in 12.2(8)T1

Cisco IOS Release 12.3 T Memory Recommendations for the Cisco 2600XM Series and 2612 Routers

Feature Set	Software Image	Flash Memory	DRAM Memory
IP Base	c2600-ipbasek9-mz	16 MB	64 MB
IP Voice	c2600-ipvoicek9-mz	32 MB	96 MB
SP Services	c2600-spservicesk9-mz	32 MB	128 MB
Enterprise Base	c2600-entbasek9-mz	32 MB	96 MB
Enterprise Service	c2600-enterservicesk9-mz	32 MB	128 MB
Enterprise Plus H.323 MCM	c2600-jk8s-mz	32 MB	128 MB
Advanced Security	c2600-advsecurityk9-mz	32 MB	96 MB
Advanced IP Services	c2600-advipservicesk9-mz	32 MB	128 MB
Advanced Enterprise Services	c2600-adventerprisek9-mz	32 MB	128 MB
Enterprise/SNASW PLUS	c2600-a3js-mz	32 MB	128 MB
Voice IP to Voice IP Gateway	c2600-js2-mz	32 MB	128 MB
Voice IP to Voice IP Gateway IPSec 3DES	ik8s2-mz	32 MB	128 MB
Int. voice/video GK, IPIP GW, TOMP GW	c2600-ipvoice_ivs-mz	32 MB	128 MB
Int. voice/video GK, IPIP GW, TOMP GW AES	c2600-adventerprisek9_ivs-mz	32 MB	128 MB
Telco feature set	c2600-telco-mz	32 MB	64 MB
Enterprise SSG	c2600-g4js-mz	32 MB	128 MB
Enterprise/SNASW Plus IPsec 3DES	c2600-a3jk9s-mz	32 MB	128 MB

Support for Cisco 2691 starts in Cisco IOS release 12.2(8)T1

Cisco IOS Release 12.3 T Memory Recommendations for the Cisco 2691 Router

Feature Set	Software Image	Flash Memory	DRAM Memory
IP Base	c2691-ipbasek9-mz	32 MB	128 MB
IP Voice	c2691-ipvoicek9-mz	32 MB	128 MB
SP Services	c2691-spservicesk9-mz	64 MB	128 MB
Advanced Security	c2691-advsecurityk9-mz	32 MB	128 MB
Advanced IP Services	c2691-advipservicesk9-mz	64 MB	128 MB
Advanc edEnterprise Services	c2691-adventerprisek9-mz	64 MB	128 MB
Advanced Enterprise Services with SNA Switching	c2691-adventerprisek9_sna-mz	64 MB	192 MB
Enterprise Base	c2691-entbasek9-mz	32 MB	128 MB
Enterprise Services	c2691-c2691-entservicesk9-mz	64 MB	128 MB
Enterprise Plus H.323 MCM	c2691-jk8s-mz	64 MB	128 MB
Enterprise/SNAGw Plus	c2691-a3js-mz	64 MB	192 MB
Enterprise/SNAGw Plus IPsec 3DES	c2691-a3jk9s-mz	64 MB	192 MB
Int. voice/video GK, IPIP GW, TOMP GW	c2691-ipvoice_ivs-mz	32 MB	128 MB
Int. voice/video GK, IPIP GW, TOMP GW AES	c2691-adventerprisek9_ivs-mz	64 MB	128 MB

ORDERING INFORMATION

The Cisco 2600 is ordered from components. You must specify:

- A 2600 Series chassis: All Cisco 2600 chassis ship with the minimum recommended memory for the most recent default Cisco IOS IP Base feature set, documentation, console, auxiliary and LAN cables, 19-inch rack-mount brackets, RJ-45 to DB-9 and DB-25 converters, and blank panels that cover unused WAN interface card and or network module slots. AC, DC, and RPS power options are available for all chassis
- A CD software pack with desired software release
- A power cord

Optional items:

- Cisco IOS feature set upgrade. The IP Base feature set is the default and included with the chassis
- Up to two WAN interface cards (up to three for Cisco 2691)
- A network module
- An advanced integration module (up to two for Cisco 2691)
- Flash memory upgrade
- DRAM memory upgrade
- Cables
- NEBS/ETSI compliance kit (not available for Cisco 2691)
- Feature license for IP Telephony

Check Point
We Secure the Internet

Data Sheet

VPN-1 Edge Wireless

Secure remote connectivity with unmatched scalability

YOUR CHALLENGE

Organizations are increasingly adopting wireless technology to enable employees and business partners to easily access corporate resources through a wireless LAN in remote or branch offices. Because network attacks are on the rise, especially on wireless networks, you need a cost-effective, reliable wireless Internet security solution that can easily be maintained and will remain effective at all times to protect your valuable resources.

OUR SOLUTION

Check Point's VPN-1® Edge™W provides secure wireless connectivity for remote sites, branch offices, and partner sites by integrating a secure wireless access point with market-leading VPN-1®/FireWall-1® technology, high availability support, and simple Web-based setup. Ideal for large-scale VPN deployments, VPN-1 Edge W is centrally managed for quick setup and management of thousands of Check Point gateways.

SECURE WIRELESS ACCESS

As your business grows, your network must grow to support it. VPN-1 Edge W will enable you to expand your remote and branch office networks without the hassle and cost of extending wiring, and to easily implement innovative new wireless services as they become available.

Superior wireless performance

VPN-1 Edge W supports both the older 802.11b and the latest 802.11g technologies, as well as the new Super-G standard that allows reaching wireless network speeds of up to 108 Mbps, unique in the industry.

VPN-1 Edge W supports unparalleled wireless network speeds of up to 108 Mbps through the new Super-G wireless standard.

PRODUCT DESCRIPTION

Check Point's VPN-1® Edge™W wireless (W) security appliance family is the first enterprise-level integrated firewall and wired and wireless VPN security solutions for remote sites, branch offices, and partner sites. Like all VPN-1 solutions, VPN-1 Edge W allows enterprises to deploy and centrally manage their network security policy for any remote location, with the added value of applying the security policy to corporate wireless networks.

PRODUCT FEATURES

- Secure wireless access point
- Supports 802.11b, 802.11g, and Super-G wireless technology
- Secure site-to-site and remote access VPN
- Patented Stateful Inspection firewall
- ISP and gateway high availability
- One-Click VPN deployment
- Large-scale management support
- Built-in print server

PRODUCT BENEFITS

- Flexible, secure, high-speed wireless access for remote sites and employees
- Industry-proven security
- Easy setup and deployment
- Simplified administration for large-scale deployments
- Always-on protection

Intelligent Security

Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.

Dual diversity antennas offer excellent range and improved signal quality to support the latest extended-range (XR) technology. With XR (extended range) enabled clients, you achieve up to three times the range of a standard access point—up to 328 yards (300 meters) indoors and up to 1,094 yards (one kilometer) outdoors.

Furthermore, VPN-1 Edge W provides full firewall isolation between wired and wireless users, and between temporary "guest users" and permanent users running VPN client software.

SECURE CONNECTIVITY

VPN-1 Edge W protects the privacy of data communications with strong encryption and authentication. The appliance also supports multiple network topologies, as well as port-based and tag-based VLAN, to meet your business needs. Optionally, the appliance may be used as an internal VPN server, which adds encryption to your LAN, allowing internal LAN and wireless users to be strongly authenticated to the appliance and completely secured from unauthenticated or guest users.

Strong encryption and authentication

VPN-1 Edge W adheres to the IPSec standard, automatically negotiating the use of the strongest possible encryption and data authentication algorithms. The device can encrypt data using AES, 3DES, and DES algorithms, and provides strong authentication by supporting industry standard X.509 digital certificates. Optionally, through an easy-to-use wizard, the user can generate self-signed X.509 certificates directly from the local management interface. To further ease deployment, VPN-1 Edge W can use digital certificates provided by the Check Point Internal Certificate Authority included with Check Point centralized management.

Multiple topology support

Some organizations prefer to deploy security in a hub-and-spoke topology, sending all traffic through a primary VPN gateway. VPN-1 Edge W allows you to route all traffic, even Internet-bound traffic, through a central VPN-1 Pro™ gateway before being sent to its final destination. OPSEC-certified products such as antivirus or URL filtering can inspect traffic at the central site, removing the need to deploy such functionality to each site. For organizations that prefer to send traffic directly to the Internet, VPN-1 Edge W also supports split tunneling.

Flexible VLAN support

VPN-1 Edge W supports VLANs for increased security within the local network by segmenting the internal networks into several virtual networks. It enables non-intrusive deployment into an existing VLAN configuration. Port-based VLAN allows splitting the four LAN ports into four segmented networks.

THE TECHNOLOGY INSIDE THE BOX

VPN-1 Edge W is based on VPN-1 Embedded NG™ technology, which incorporates Check Point's market-leading firewall and VPN software optimized for embedded platforms. VPN-1 Embedded NG is developed by SofaWare Technologies, a Check Point company.

Tag-based VLAN allows the device to be connected to a switch via a VLAN trunk, thereby expanding port density.

UNMATCHED PROTECTION

Tailored to the needs of corporate remote sites, VPN-1 Edge W safeguards corporate resources and ensures the privacy and integrity of data communications, by integrating access control, user authentication, and encryption into one easy-to-use device.

Patented Stateful Inspection firewall

VPN-1 Edge W includes Check Point-patented Stateful Inspection technology, providing the most secure Internet protection in the industry. Only Check Point Stateful Inspection can track the state and context of all network communications, to provide truly complete network protection.

Protecting confidential data

For the strongest safeguards available, VPN-1 Edge W is the answer. It isolates and controls access to your wireless network to protect your data. The appliance authenticates remote user identities, ensuring that only authorized individuals have network access. And it allows using mature, VPN (IPSec) technology to encrypt wireless communication, so that data cannot be viewed or corrupted during transmission.

Dedicated, secured W LAN interface

VPN-1 Edge W has an additional, separate WLAN interface for which you can set specific security rules. It protects the wireless interface by granting access only to authorized users, preventing hackers from invading your LAN and the crucial information it contains.

Broad application support

Through its integration of Check Point patented Stateful Inspection technology, VPN-1 Edge W secures over 150 predefined applications, services, and protocols out-of-the-box, including instant messaging and peer-to-peer applications, database applications, VoIP protocols, and Microsoft NetMeeting.

NON-STOP CONNECTIVITY

Keeping your network up and running is critical to your business. VPN-1 Edge W supports ISP redundancy and gateway high availability to enable non-stop connectivity. The device also supports the H.323 and SCCP (Skinny) VoIP protocols, enabling mission-critical voice and data to be transmitted safely and reliably to and from your corporate network.

ISP redundancy

VPN-1 Edge W supports ISP redundancy to ensure persistent connectivity. The DMZ port may be used as a secondary WAN port. When two different ISPs are connected to the appliance, VPN-1 Edge W will automatically pick up the connection from the other ISP if one fails to deliver a connection.

Gateway high availability

VPN-1 Edge W supports a backup ISP connection and automatic failover across two VPN-1 Edge W gateways to provide always-on protection. High availability is supported for the WAN interfaces, allowing the primary and secondary appliances to share a single WAN IP address for virtually uninterrupted access from the Internet to internal servers at your network.

Dialup backup
VPN-1 Edge W supports dialup backup, a cost-effective feature that provides a primary or secondary Internet connection. You simply connect a dialup modem (regular or ISDN) to the serial port of the VPN-1 Edge W appliance. Using the dialup modem as a primary Internet connection is useful in locations where broadband Internet access is unavailable. VPN-1 Edge W automatically dials the modem if it detects that the primary Internet connection has failed.

RAPID DEPLOYMENT AND MANAGEMENT

VPN-1 Edge W appliances deploy in minutes and can be centrally managed along with other Check Point gateways through Check Point's centralized management, including SmartCenter Pro™, SmartCenter Enterprise, SmartCenter Express, SmartCenter Express Plus, and Provider-1®. These management products (sold separately from the VPN-1 Edge W devices) allow you to centrally define, efficiently manage, and constantly monitor multiple Check Point gateways from a single console. Large-scale management for VPN-1 Edge W is provided by Smart Large Scale Manager (SmartLSM), which is part of SmartCenter Pro. Using SmartLSM, administrators can provision a single security policy—called a Profile—and apply it simultaneously to hundreds of gateways. For very large deployments, the optional Security Management Portal (SMP) module provides profile-based management of thousands of gateways.

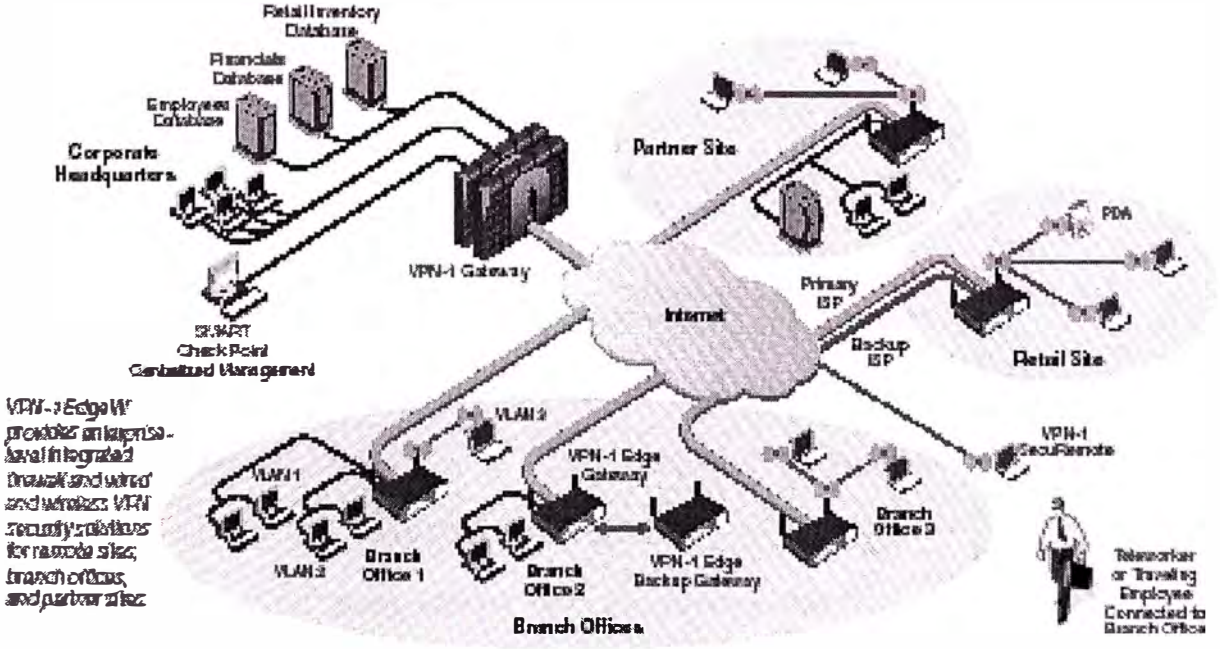
Plug and play appliance
VPN-1 Edge W includes wizard-driven Web-based management for very easy setup in minutes by non-technical staff at the remote site. To further ease large-scale deployments, Check Point can preconfigure the device to your specifications, for truly "plug and play" secure connectivity.

One-Click VPN deployment
Check Point centralized management simplifies gateway setup through One-Click VPN Communities. With VPN Communities, you simply drag the icon representing a VPN-1 Edge W appliance and drop it into a VPN community, in the same way you would drag and drop a file into a desktop folder. VPN-1 Edge W automatically inherits community security parameters, receives a X.509 digital certificate from the Check Point Internal Certificate Authority (included with Check Point centralized management), and can immediately establish secure IPSec sessions with the rest of the VPN community.

Integrated bandwidth management
Bandwidth management is important for remote offices where business-critical traffic, such as VPN and VoIP, is competing with other non-critical traffic over a single ISP connection. VPN-1 Edge W includes comprehensive bandwidth management that offers weighted priorities, guarantees, and limits. Bandwidth management is particularly important for real-time applications such as VoIP.

Comprehensive out-of-band management
VPN-1 Edge W supports multiple out-of-band management schemes: CLI (Command Line Interface) via SSH, CLI via serial port, and SNMP.

Always up-to-date security
For effective protection against evolving threats, security software must be kept up-to-date. Check Point SmartCenter Pro includes SmartUpdate which lets you centrally install and upgrade both security and operating system software. SmartUpdate can automatically distribute software updates, eliminating the time and cost associated with one-at-a-time device updates while ensuring consistent, current security across your network.



VPN-1 Edge W provides an integrated firewall and wired and wireless VPN security solutions for remote sites, branch offices, and partner sites

BIBLIOGRAFIA

1. **Bates Regis**. GPRS – General Packet Radio Service. McGraw-Hill 2002.
2. **Bernárdez Rodríguez, Rosa María**. Servicios de vídeo sobre redes móviles de nueva generación. Telefónica Investigación y Desarrollo.
3. **Bettstettet Christian**. GSM Phase 2+ General Packet Radio Service GPRS: Architecture, Protocols and Air Interface. IEEE Communications Surveys 1999.
4. **Compaq**. Operación y Administración del INS/IS41. Compaq Computers Incorporated.
5. **ETSI TS 100 605 V7.2.0 (2001-03)**. Information element mapping between Mobile Station – Base Station (MS – BSS) and Base Station System – Mobile – services Switching Centre (BSS – MSC); Signalling procedures and the Mobile Application Part (MAP). 3GPP TS 09.10 version 7.2.0 Release 1998.
6. **ETSI TS 100 974 V7.14.0 (2003-09)**. Chapters 19 – 22 (Location Update, Location Cancelation, Detach IMSI, Purge MS, Subscriber Data Management Procedures, Call Handling Procedure, Registration Procedure, Erasure Procedure, Activation Procedure, Deactivation Procedure, Interrogation Procedure, Invocation Procedure and Password Registration Procedure. 3GPP TS 09.02 version 7.14.0 Release 1998.
7. **ETSI TS 100 929 V8.1.0 (2001-07)**. Security related network functions. GSM 03.20 version 8.1.0 Release 1999.
8. **Gallagher Michael**. Mobile Telecommunications Networking with IS41.
9. **Gregory Bates**. Voice & Data Communications Handbook. McGraw-Hill 2000.
10. **Hernando Rábanos, José María**. Comunicaciones Móviles de Tercera Generación Vol. 1 y 2. Telefónica Móviles España, S.A 2001.
11. **Hernando Rábanos, José María**. Comunicaciones Móviles GSM. Fundación Airtel 1999.

12. **Hernando Rábanos, José María**. Comunicaciones Móviles. Thomson Editores Spain Paraninfo, S.A 2002.
13. **Motorola**. Introducción al CDMA. Curso de Entrenamiento 1997.
14. **Mundo Electrónico**. Telecomunicaciones Móviles. Marcombo, S.A 1995.
15. **Muratore, Flavio**. Las Comunicaciones Móviles del Futuro. CSELT 2000.
16. **Paavilainen, Jouni**. Mobile Business Strategies. Wireless Press 2001.
17. **Pañeda, Xabiel**. Métricas para el Análisis de Calidad en Servicios de Vídeo-Bajo-Demanda Reales. Departamento de Informática. Universidad de Oviedo.
18. **RealNetworks**. Helix Universal Server Administration Guide. RealNetworks 2003.
19. **RealNetworks**. Introduction to Streaming Media. RealNetowrks 2002.
20. **RealNetworks**. Helix Producer User´s Guide. 2002.
21. **RealNetworks**. RTSP Interoperability with RealSystem Server 8. RealNetworks 2000.
22. **RealPlayerPlus**. Manual de Usuario. RealNetowrks 2002.
23. www.etsi.org
24. www.3gpp.org
25. www.nokia.com
26. www.rtsp.org
27. www.catedra-tme.etsit.upm.es
28. www.wapforum.org
29. www.comsoc.org/pubs/surveys
30. www.real.com