CARACTERIZACIÓN DEL ROAMING ENTRE LA RED MÓVIL CELULAR Y LA RED INALÁMBRICA DE ÁREA LOCAL CON APLICACIÓN AL ENTORNO COLOMBIANO

ANEXOS

LUIS CARLOS COLLAZOS MUÑOZ
HELMUT ALEXANDER RUBIO WILSON

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
GRUPO I+D EN NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2005

CARACTERIZACIÓN DEL ROAMING ENTRE LA RED MÓVIL CELULAR Y LA RED INALÁMBRICA DE ÁREA LOCAL CON APLICACIÓN AL ENTORNO COLOMBIANO

ANEXOS

LUIS CARLOS COLLAZOS MUÑOZ
HELMUT ALEXANDER RUBIO WILSON

Trabajo de grado presentado como requisito para obtener el título de Ingeniero en Electrónica y Telecomunicaciones

Director
GUEFRY AGREDO MENDEZ
INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
GRUPO I+D EN NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2005

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

ANEXO A. ARQUITECTURA DE LAS TECNOLOGÍAS MOVILES CELULARES Y DE ACCESO INALÁMBRICO UTILIZADAS ACTUALMENTE EN COLOMBIA

1. REDES MÓVILES CELULARES

1.1 TDMA/IS-136

El estándar actual TDMA/IS-136 utiliza portadoras de 30 Khz y divide un canal simplex en 6 TS. Entre las características principales de TDMA/IS-136 se encuentran:

- La voz se digitaliza y se envía en diferentes TS asignados, utilizando una portadora común de 30 Khz.
- TDMA/IS-136 utiliza canales dúplex de radio frecuencia, que constan de dos frecuencias, una para transmisión y otra para recepción.
- Brinda una velocidad de 16,2 Kbps por canal.
- Utiliza Modulación Diferencial en Cuadratura de Fase (DQPSK Differential Quadrature Phase Shift Keying).
- Los canales de control son los mismos utilizados en el Servicio Telefónico Móvil Digital Avanzado (DAMPS - Digital Advanced Mobile Phone Service).
- El mismo canal de radio no puede ser utilizado en celdas o sectores adyacentes, para evita interferencia co-canal y de canal adyacente.
- Utiliza un plan de frecuencia N=7, lo que significa que divide todos los canales simplex de frecuencia disponibles en veintiún grupos, con un canal de control por grupo y los grupos son distribuidos en siete celdas formando un clúster.
- TDMA/IS-136 permite jerarquización de celdas (macroceldas, microceldas, picoceldas) por medio de las diferentes clases de Estaciones Base (BS – Base Stations). La microcelda sirve para cubrir espacios sin cobertura o para resolver problemas de capacidad en ambientes de macrocelda (nivel metropolitano). Este sistema permite cubrir puntos activos/inactivos de la macrocelda y de igual forma descargar su tráfico; cuanto más tráfico pueda captar la microcelda hay mas recursos disponibles para que la macrocelda preste un buen servicio a los subscriptores.

La red CDPD que se utiliza para la transmisión de datos es una red superpuesta que hace uso de la infraestructura de la red TDMA/IS-136 existente; incluye transceptores de datos en la Estación Base (BS – Base Station) que utilizan Modulación por Desplazamiento Mínimo Gausiano (GMSK – Gaussian Minimum

Shift Keying) y un sistema para datos en la Central de Conmutación Móvil (MSC - Mobile Switching Center).

Arquitectura de red TDMA/IS-136:

La arquitectura completa de la red TDMA/IS-136 se muestra en la figura A.1. Ésta permite la prestación de servicios de transmisión de voz y datos con ciertas restricciones a los usuarios móviles que aún cuentan con terminales TDMA.

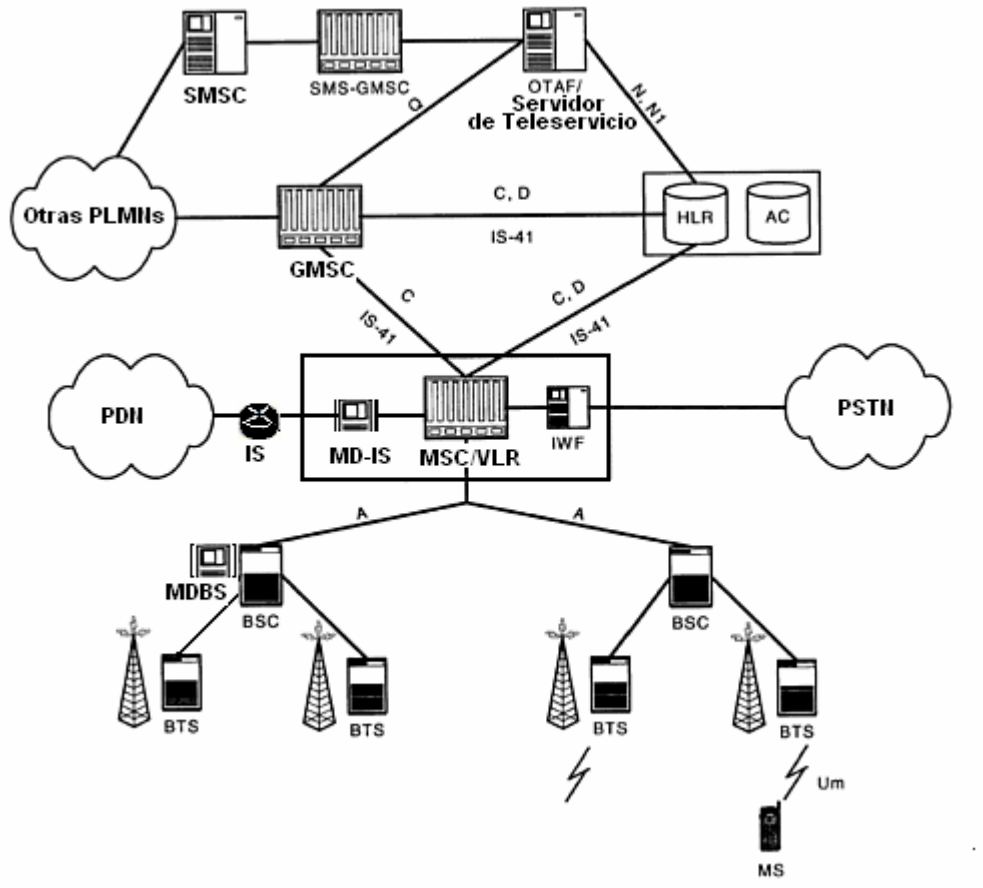

Figura A.1. Arquitectura de red TDMA/IS-136. [1]

Los elementos de la red TDMA/IS-136 asociados al manejo del tráfico de datos y que se encuentran en la figura A.1 son:

Centro de Conmutación Móvil/Registro de Localización de Visitantes (MSC/VLR – Mobile Switching Center/Visitor Location Register): Se encarga del control de las llamadas originadas o terminadas desde una Estación Móvil, de realizar tanto la gestión de movilidad como de recursos de radio y de capturar información de cobro acerca de los servicios utilizados por la Estación Móvil para que sea posible la facturación de los mismos. Adicionalmente, el MSC contiene la función VLR, el

cual contiene información de subscriptor necesaria para servicios de *roaming* en redes visitantes.

Gateway MSC: permite la conmutación y enrutamiento hacia y desde otras Redes Terrestres Móviles Públicas (PLMNs - Public Land Mobile Networks)[1] o Redes Telefónicas Públicas Conmutadas (PSTNs - Public Switched Telephone Networks).

Registro de Localización de Residentes (HLR – Home Location Register): Es la base de datos central para el almacenamiento de información de suscripción de usuarios, además de información relacionada con el perfil del servicio, la localización y el estado actual de actividad del subscriptor.

Central de Autenticación (AC - Authentication Center): Como su nombre lo indica, se encarga de autenticar las estaciones móviles a través de la verificación de la información recibida por el MSC. Como resultado de una autenticación exitosa, la AC proporciona parámetros de encriptación para la interfaz de aire.

Función de Activación Sobre Aire/Servidor de Teleservicio[2] (OTAF – Over the air Activation Function/ Teleservice Server): Como su nombre lo indica, es el nodo encargado de brindar soporte a los teleservicios. También se le conoce como centro de mensajería, es decir que se encarga de la entrega de mensaje cortos a las estaciones móviles, y para lograrlo, debe comunicarse con otras entidades de red a través de señalización SS7 o IP, en particular utiliza el protocolo IS-41 para comunicarse con el HLR y el MSC.

Estación Base Transceptora (BTS – Base Transceiver Station): Proporciona la interfaz TIA/EIA/IS-95 entre las Estación Móvil y el Subsistema de Estaciones Base haciéndose responsable de la codificación y decodificación de las tramas que viajan por el aire. Adicionalmente se encarga de ciertas funciones relacionadas con el control de potencia de los canales de radio.

Controlador de Estación Base (BSC – Base Station Controller): Se encarga de controlar un juego de BTSs proporcionando funciones celulares específicas, como la gestión de los recursos de radio y el control de potencia durante el *handover*. En IS-136 la interfaz que conecta la BTS al BSC no constituye un estándar abierto, lo que significa que los fabricantes tienen libertad en la implementación de la misma.

Función de Interoperabilidad (IWF – Interworking Function): Proporciona un mecanismo para la transferencia de señales digitales de datos y la conversión de

[1] PLMN es el nombre genérico de las redes móviles inalámbricas que utilizan transmisores terrestres basados en radiofrecuencia o estaciones base como hubs de red**.**

[2] En IS-136 se refiere a una aplicación que utiliza la red y la interfaz de aire como portadora de cantidades relativamente pequeñas de información empaquetada (por ejemplo mensajes cortos) entre el servidor y la estación móvil.

protocolos que se manejan en otras redes como una PLMN GSM u otros tipos de redes como una PSTN o ISDN.

Centro de Servicio de Mensajería Corta (SMSC – Short Message Service Center): Es responsable por el almacenamiento y reenvío de los mensajes cortos entre MSs o entre un nodo fijo y una estación.

SMS-GMSC: Básicamente es un MSC capaz de recibir un mensaje corto desde un SMC de la red local y entregar el mensaje corto al MSC externo que puede enviar la información a la MS destino.

Sistema de Intermediación de Datos Móviles (MD-IS – Mobile Data Intermediate System): Es un nodo CDPD que se encarga de gestionar la movilidad de la MS a través del enrutamiento de los paquetes de datos soportando una base de datos de usuarios de su área.

Estación Base para Datos Móviles (MD-BS – Mobile Data Base Station): Es un nodo CDPD que se instala en el BSC y se encarga de recibir paquetes de la MS para luego enviarlos al MD-IS. Cada MD-BS puede manejar de 1-3 canales CDPD, si esto no es suficiente, existe la posibilidad de incrementar la capacidad añadiendo otro MD-BS en el BSC.

Sistema de Intermediación (IS – Intermediate System): Realiza la función de *internetworking* necesaria para realizar la interconexión con la red de paquetes de datos externa.

1.2 GSM

Entre las características principales de GSM se encuentran:

- Digitalización y compresión de voz y datos.
- Se basa en la tecnología de acceso TDMA.
- Utiliza canales duplex de radio frecuencia que constan de dos frecuencias, una de transmisión y otra de recepción.
- La velocidad de transmisión es de 9,6 Kbps por canal.
- Utiliza modulación GMSK.
- Soporta estructura jerárquica de celdas.
- La multitrama de tráfico está formada por 26 tramas y la multitrama de control por 52 tramas.
- Provee algoritmos de encripción para autenticar al usuario y cifrar las conversaciones.
- Utiliza
- Brinda soporte a poblemas de propagación como desvanecimiento (fading), interferencia multitrayectoria y de canal adyacente mediante ecualización, codificación del canal, intercalado (interleaving), diversidad en recepción y saltos lentos de frecuencia.

- Control de potencia opcional, lo que permite la adecuada operación del sistema con o sin él. En caso de que ocurra una falla en el control de potencia no hay degradación del servicio.
- Ofrece *roaming* global.

Arquitectura de red GSM:

La arquitectura completa de la red se muestra en la figura A.2. Ésta permite la prestación de servicios de transmisión de voz y datos utilizando conmutación de circuitos a los usuarios móviles que cuentan con terminales GSM.

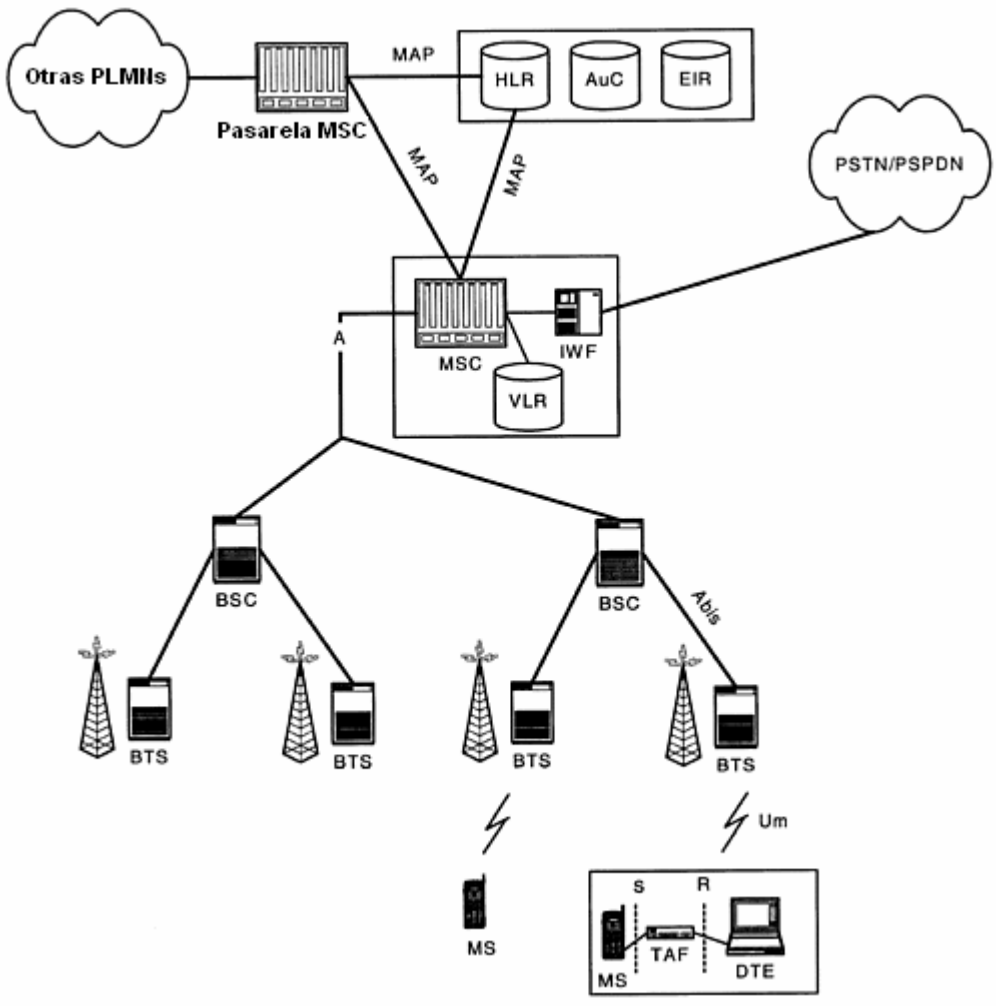

Figura A.2. Arquitectura de red GSM.

Los elementos de la red GSM asociados al manejo del tráfico de datos y que se encuentran en la figura A.2 son:

Centro de Conmutación Móvil (MSC – Mobile Switching Center): es el nodo principal de GSM, realiza funciones de establecimiento, enrutamiento, control y

terminación de llamadas de voz y/o datos. Además, provee interfaces de red, señalización de canal común, gestión de *handover* entre MSCs, facturación y estadísticas.

Registro de Localización de residentes (HLR – Home Location Register): es una base de datos permanente y centralizada para el almacenamiento y administración de subscriptores de un operador específico. El HLR se considera como la base de datos más importante de la red y almacena datos como clase de servicio, información de localización y estado de actividad del subscriptor.

Registro de Localización de Visitantes (VLR – Visitor Location Register): es una base de datos que se encuentra dentro del MSC y que contiene información temporal acerca de los subscriptores que se encuentran en *roaming.* Cuando un terminal se mueve al área de cobertura de un nuevo MSC, el nuevo VLR solicita información al HLR del subscriptor, este provee una copia de los detalles del subscriptor y actualiza la información de localización del terminal.

Centro de Autenticación (AUC – Authentication Center): proporciona parámetros de autenticación y encriptación que verifican la identidad de los usuarios y aseguran la confidencialidad del servicio, además protege a los operadores de la red de diferentes tipos de fraude y brinda parámetros de autenticación al HLR antes de que se realice cualquier actividad de cambio o uso de la información del subscriptor.

Registro de identificación de equipos (EIR – Equipment Identity Register): es una base de datos que tiene la función de validar los terminales utilizados por los subscriptores. Este procedimiento se lleva a cabo con ayuda de la Identificación Internacional del Equipo Móvil (IMEI – International Mobile Equipment Identity) para asegurar que el terminal sea un equipo válido.

Gateway MSC: proporciona las interfaces necesarias para conectar el MSC con otros MSC y redes PSTN, ISDN y PLMN. Durante el establecimiento de las llamadas a los terminales, el GMSC solicita información acerca de la localización del terminal al HLR con el fin de proveer enrutamiento de llamadas.

Función de Interoperabilidad (IWF – Interworking Function): consta del *hardware* y *software* necesario para proporcionar una interfaz hacia otras redes de datos o telefónicas realizando las conversiones de protocolo necesarias.

Equipo Terminal de Datos (DTE – Data Terminal Equipment): es el equipo terminal de datos que normalmente se utiliza en redes cableadas (PC).

Función de Adaptación de Terminal (TAF – Terminal Adaptation Function): como su nombre lo indica, se encarga de adaptar un DTE para que se pueda conectar a una MS, como se observa en la figura maneja las interfaces R y S.

1.3 GPRS

Entre las principales características de GPRS se encuentran:

- Esta en la capacidad de operar en las mismas bandas de frecuencia que GSM.
- Empleo de Modulación Gaussiana GMSK
- Utiliza el mismo canal de radio de 200Khz de GSM
- Introduce conmutación de paquetes a las redes GSM y TDMA/IS-136, además de esquemas adicionales de codificación en la interfaz de radio necesarios para aumentar la velocidad de transmisión de datos.
- No requiere conexión física extremo a extremo y brinda alta eficiencia espectral debido a que los recursos de red y ancho de banda son asignados dinámicamente, es decir, se utilizan solamente cuando hay flujo efectivo de datos.
- La conexión se realiza en el momento en que se utiliza el canal por lo que no es necesario establecer un canal dedicado para cada usuario.
- Proporciona una conexión instantánea y continua a redes de datos externas brindando una experiencia *"always on"*[3] al usuario.
- Emplea nuevos esquemas de tarificación basados en la cantidad de datos transmitidos y no en el tiempo de conexión.
- Soporta comunicaciones simultáneas de voz y datos en la MS.
- No emplea almacenamiento y reenvío al manejar el tráfico de datos independientemente del de voz.
- Incluye los protocolos principales para transmisión de paquetes de datos utilizados en Internet (IP, PPP, X.25), lo que permite que aplicaciones que utilicen estos protocolos puedan operar sobre una conexión móvil celular.
- Velocidades de bit en el rango de 14,4Kbps a 171,2Kbps.
- Opera con mayor eficiencia en la gestión de los recursos de radio debido a que una cantidad reducida de usuarios activos implica que cada usuario tiene acceso a más ancho de banda.
- Incrementa los ingresos y ganancias de los operadores celulares por concepto de servicios de datos.

Se pueden diferenciar cuatro esquemas de codificación (CS) que incorporan diferentes niveles de chequeo de integridad de la información a través de la corrección de errores de encabezado de los datos transmitidos. En buenas condiciones, en un canal con alta Relación Señal a Ruido (SNR – Signal to Noise Ratio), puede usarse cualquiera de los cuatro esquemas de codificación, en éste caso, el CS-4 que ofrece la menor protección del canal, proporcionará el *throughput* más alto en transmisión de datos. Por otro lado, si las condiciones del canal no son buenas, se utiliza el esquema de codificación CS-1, que proporciona mayor cantidad de protección del canal a través de los códigos de corrección de error de encabezado, lo que reduce el *throughput,* pero evita una gran cantidad de retransmisiones.

[3] Siempre en línea.

La tabla A.1 muestra los cuatro esquemas de codificación en mención. Como se observa, el número de bits de datos en el paquete de radio aumenta a medida que se reducen los bits de protección en el encabezado, resultando en un aumento de la velocidad o tasa de transmisión de datos por *time-slot.*

ESQUEMA DE CODIFICACIÓN DEL CANAL	BITS DE DATOS EN EL PAQUETE DE RADIO	TASA DE DATOS POR TS [KBPS]	MÁXIMA TASA DE DATOS POR 8 TS [Kbps]
CS-1	181	9.05	72.4
CS-2	268	13.4	107.2
CS-3	312	15.6	124.8
CS-4	428	21.4	171.2

Tabla A.1. Esquemas de codificación GPRS. [2]

Se debe tener en cuenta que en realidad las tasas de transmisión de datos sobre la interfaz de radio resultan inferiores a las presentadas en la tabla A.1, ya que el canal se ve afectado por factores como la ubicación geográfica del usuario, las condiciones atmosféricas y el número total de usuarios que demandan el servicio a determinada hora del día.

Arquitectura de red GPRS:

La infraestructura GPRS complementa la infraestructura GSM existente, por lo tanto para habilitar los servicios que soporta GPRS, los operadores necesitan renovar su infraestructura GSM a través de la introducción de los nuevos elementos de red GPRS, así como actualizar ciertos nodos GSM ya existentes.

Entre los nuevos elementos introducidos por GPRS se encuentran los Nodos de Soporte de GPRS (GSNs – GPRS Support Nodes), específicamente el Nodo de Soporte de Servicio GPRS (SGSN – Service GPRS Support Node) y el Nodo de Soporte de Pasarela GPRS (GGSN *Gateway* GPRS Support Node), además de la *Gateway* de Frontera (BG – Border Gateway) y la *Gateway* de Función de Cobro (CGF – Charging Gateway Function). Adicionalmente, el sistema GPRS requiere de actualizaciones software en algunos de los nodos GSM existentes como por ejemplo en la MSC, el Registro de Localización de Visitantes (VLR - Visitor Location Register), el Registro de Localización Local (HLR - Home Location Register), así como cambios menores en la Estación Base Tranceptora (BTS - Base Transceiver Station). Finalmente, tanto cambios software como hardware se requieren en el Controlador de Estaciones Base (BSC – Base Station Controller).

La arquitectura completa de la red GPRS se muestra en la figura A.3. Ésta permite la prestación de servicios de transmisión de voz y datos a los usuarios móviles.

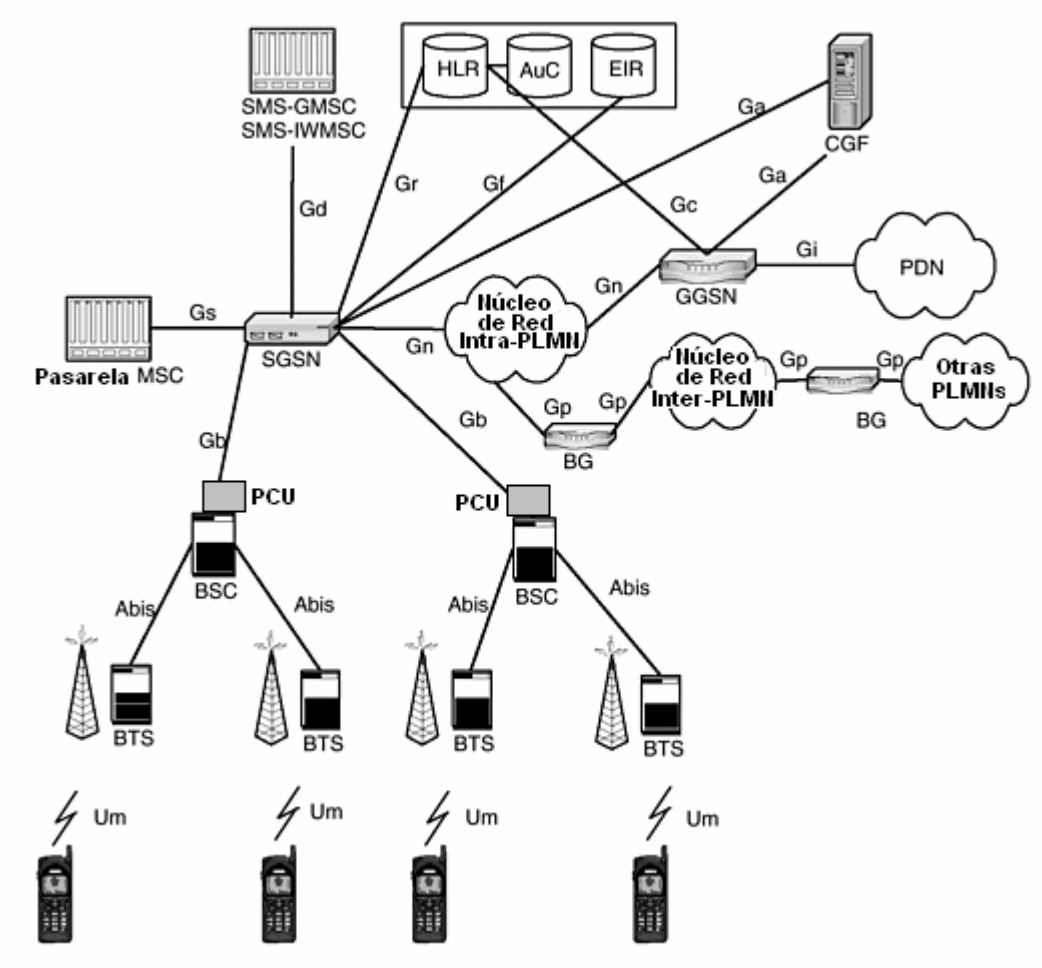

Figura A.3. Arquitectura de red GPRS.

Los nuevos elementos de red asociados al manejo del tráfico de paquetes de datos introducidos por la red GPRS y que se encuentran la figura A.3 son:

Unidad de Control de Paquetes (PCU - Packet Control Unit): es la unidad encargada de la funcionalidad de capacidad por demanda, estableciendo cuales recursos de radio se asignan para la utilización de la conmutación de paquetes y cuales para la conmutación de circuitos. De ésta manera, el BSC maneja los recursos de radio asignados a la conmutación de circuitos, mientras la PCU maneja los recursos de radio asignados al tráfico GPRS, esto incluye el control de acceso al canal, asignación de canal, además de la segmentación y el reensamblado de paquetes de datos.

Nodo de Soporte de Servicio GPRS (SGSN – Service GPRS Support Node): está conectado al BSC por medio de la interfaz Gb y tiene el mismo nivel jerárquico que el MSC. Es el nodo encargado de enviar y recibir paquetes de datos hacia y desde la MS, realiza la gestión de movilidad al almacenar la trayectoria de las MSs dentro del área de servicio, envía consultas a los HLR para obtener los datos de

perfil del subscriptor GPRS, valida usuarios, detecta nuevas MSs GPRS en un área de servicio dada, realiza recolección de datos de facturación, funciones de seguridad y gestiona el control de acceso. En gran medida tiene la misma función que el MSC para el servicio de conmutación de circuitos.

Nodo de Soporte de Pasarela GPRS (GGSN – Gateway GPRS Support Node): provee la interfaz hacia las redes de paquetes IP externas. Desde el punto de vista de éstas redes, el GGSN actúa como un enrutador para todas las direcciones IP de los suscriptores que reciben el servicio de la red GPRS, es por esto que participa en la gestión de sesión al asociar a los suscriptores con el SGSN mas adecuado y así permitir una transmisión eficiente de datos.

Gateway de Frontera (BG – Border Gateway): es el nodo de red encargado de permitir la interconexión de *backbones* intra – PLMN. Aunque las funciones de la BG no están totalmente especificadas por el Instituto Europeo de Estándares de Telecomunicaciones (ETSI - European Telecomunicaciones Standards Institute), como mínimo, debe proporcionar la seguridad suficiente para proteger la intra – PLMN contra ataques externos.

Gateway de Función de Cobro (CGF – Charging Gateway Function): este nodo que puede encontrarse implementado en forma independiente o integrado en el SGSN o GGSN, proporciona un mecanismo de transferencia de información desde el SGSN y el GGSN hacia los sistemas de tarificación y facturación.

Gateway MSC para Servicio de Mensajería Corta / Función de Interoperabilidad del MSC para Servicio de Mensajería Corta (SMS-GMSC / SMS-IWMSC – Short Message Service-Gateway for Mobile Switching Center / Short Message Service-Interworking Function for Mobile Switching Center): es un nodo que permite enviar y recibir Mensajes Cortos (SM – Short Messages) desde y hacia la Estación Móvil sobre los canales de radio GPRS, encargándose de la entrega de los mensajes a los usuarios locales de la red.

1.4 EDGE

Entre las características principales de EDGE se encuentran:

- La interfaz de aire EDGE introduce modulación de alto nivel y nuevos esquemas de codificación para comunicación de datos por conmutación de circuitos y paquetes, logrando de esta manera velocidades de bit más altas que las obtenidas en los sistemas celulares de 2G o 2.5G.
- EDGE se emplea para la transmisión de datos por conmutación de paquetes y realiza corrección de errores hacia atrás, lo que significa que se solicita la retransmisión de paquetes recibidos con errores.
- Permite una integración gradual a la red GSM/GPRS.

Las nuevas técnicas introducidas por EDGE optimizan el caudal de datos para cada enlace de radio. El Control de Enlace de Radio (RLC – Radio Link Control) de EDGE ha cambiado con respecto al protocolo correspondiente a GPRS, debido al incremento de velocidad de bit y a la necesidad de adaptar la protección de datos a la calidad del canal. Los cambios principales implican un mejoramiento del sistema de Control de Calidad del Enlace (LQC - Link Quality Control), el cual incluye el sistema de Adaptación del Enlace (LA – Link Adaptation) y de Redundancia Incremental (IR – Incremental Redundancy).

La funcionalidad de LA adapta dinámicamente la codificación y la modulación con relación a la calidad de la señal. En malas condiciones de radio, se seleccionan codificación robusta y modulación GMSK, en tanto que en buenas condiciones de radio, se emplea una codificación menos robusta y modulación 8PSK.

EDGE emplea el esquema de Redundancia Incremental (IR – Incremental Redundancy) para la correción de errores, el cual consiste en enviar información inicialmente con muy poca codificación; si la decodificación tiene éxito, se obtiene una alta velocidad de bit en forma inmediata, pero si falla se realiza una retransmisión enviando bits codificados adicionales (redundancia) hasta que la decodificación tenga éxito. Una codificación más compleja significa una velocidad de bit más baja y por lo tanto un mayor retardo.

La tabla A.2 muestra los esquemas de codificación que se pueden utilizar para la retransmisión. Por ejemplo, si falla la transmisión inicial con el Esquema de Modulación y Codificación 9 (MCS-9 - Modulation and Coding Scheme 9) y la calidad del canal de radio disminuye, en la retransmisión se utiliza un esquema más robusto de la misma familia.

ESQUEMA	MODULACIÓN	VEL. MAX [Kbps]	FAMILIA
MCS-9	8PSK	59,2	A
MCS-8	8PSK	54,4	A
MCS-7	8PSK	44,8	B
MCS-6	8PSK	29,6	A
MCS-5	8PSK	22,4	B
MCS-4	GMSK	17,6	C
MCS-3	GMSK	14,8	A
MCS-2	GMSK	11,2	B
MCS-1	GMSK	8,8	C

Tabla A.2. Esquemas de codificación EDGE. [3]

1.5 CDMA2000 1X

Entre las características principales de CDMA2000 1X se encuentran:

- Esta en la capacidad de operar en las bandas de frecuencia que utiliza CDMA/IS-95 o cdmaOne, es decir 800Mhz y 1900Mhz.
- Utiliza el mismo espectro que CDMA/IS-95, por lo que reutiliza varios niveles bajos del conjunto de protocolos IS-95.
- Es complatible con implementaciones cdmaOne
- Utiliza modulación QPSK y BPSK.
- Protege la inversión de los operadores en redes cdmaOne existentes y provee migración simple hacia servicios 3G.
- Mejora la calidad y capacidad de la voz comparada con sistemas CDMA anteriores.
- Capacidad y cobertura mejorada en comparación con cdmaOne.
- Soporta tráfico simultáneo de voz y datos, además de servicios multimedia.
- Permite asignación dinámica de ancho de banda por demanda.
- Gestión eficiente de la vida útil de la batería de la MS.
- Proporciona servicios 3G a redes móviles con núcleo IS-41, lo cual incluye las redes existentes de 2G, CDMA/IS-95 y TDMA/IS136.

Arquitectura de red CDMA2000 1X

CDMA2000 1X introduce Núcleo de Red de Paquetes (PCN – Packet Core Network) que es el responsable de brindar soporte a la comunicación de datos por conmutación de paquetes de alta velocidad para las redes CDMA2000, además de permitir a los subscriptores de la red CDMA2000 1X conectarse a Internet o intranets privadas.

La arquitectura de la red CDMA2000 1X se muestra en la figura A.4. Ésta permite la prestación de servicios de transmisión de voz y datos a los usuarios móviles.

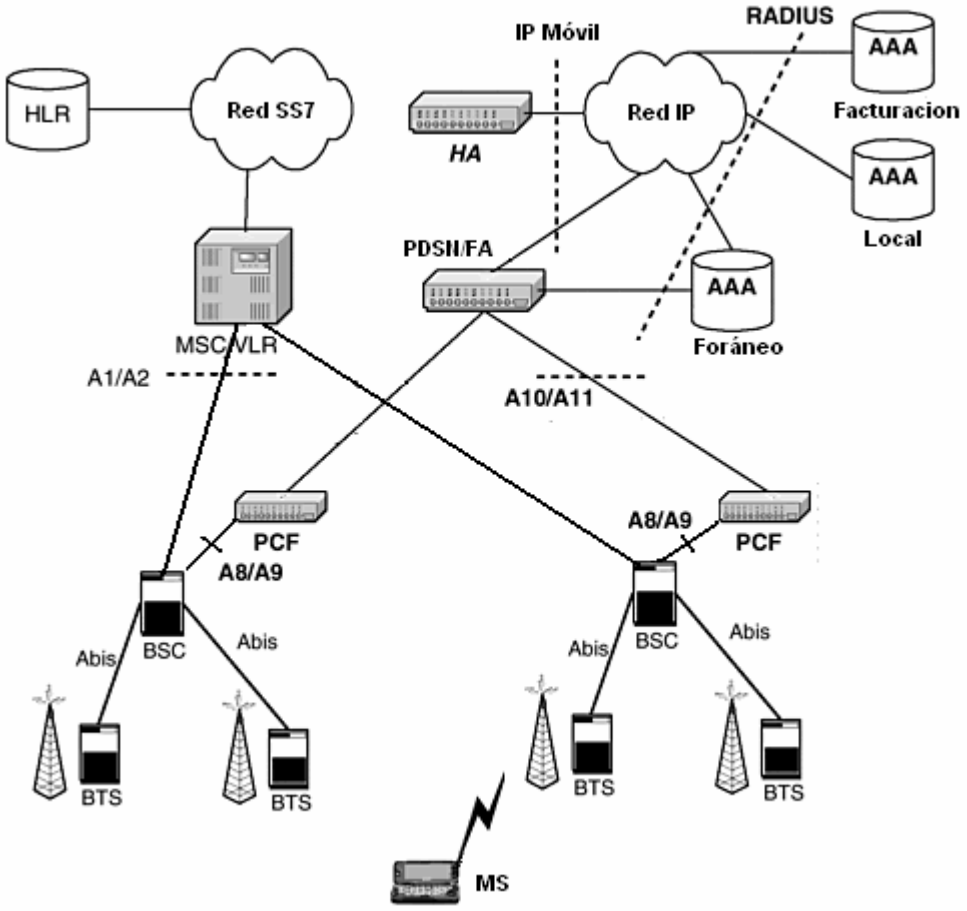

Figura A.4. Arquitectura de red CDMA2000 1X.

Función de Control de Paquetes (PCF – Packet Control Function): enruta los paquetes de datos IP entre la estación móvil y el PDSN. Durante las sesiones de paquetes de datos, asigna SCHs disponibles con el fin de proporcionar los servicios requeridos por el móvil. La PCF mantiene un estado de "alcanzable" entre la Red de Acceso Radio (RAN – Radio Access Network) y la estación móvil, asegurando un enlace consistente para los paquetes. Almacena los paquetes que llegan del PDSN cuando los recursos de radio no son suficientes para soportar el flujo hacia la Estación Móvil (MS – Mobile Station), y se encarga de reenviar los paquetes entre el PDSN y la MS. La PCF es generalmente parte del BSC, y puede ser HW o SW.

Agente Local (HA – Home Agent): es un enrutador ubicado el la red local a la que pertenece la MS y utiliza un mecanismo de entunelamiento para redirigir el tráfico de Internet, de manera que la dirección IP de la MS no tiene que ser cambiada cada vez que ésta se conecta a la red desde un segmento de red diferente.

Servidor de Autenticación, Autorización y Tarificación (AAA - Authentication, Authorization, and Accounting): se utiliza para gestionar el acceso a servicios de datos proporcionados por la red y para almacenar las estadísticas de utilización de

los mismos por parte de los usuarios. Por lo general utiliza el protocolo de Servicio de Marcado de Usuario para Acceso Remoto (RADIUS - Remote Access Dial-In User Service), aunque brinda la posibilidad de utilizar Diameter.

Nodo de Servicio de Paquetes de Datos / Agente Foráneo (PDSN/FA - Packet Data Serving Node / Foreign Agent): es la *gateway* que permite la comunicación entre la RAN y las redes de paquetes públicas y/o privadas de paquetes de datos, realizando el enrutamiento de paquetes hacia las redes de paquetes externas o hacia el HA, lo cual puede ser realizado a través de túneles seguros. Gestiona activamente los servicios de suscriptores basado en el perfil de información recibido desde el servidor AAA y proporciona una dirección IP a la MS, ya sea a través de un recurso interno, un servidor DHCP o a través de un servidor AAA. En una red con servicio de IP simple, el PDSN actúa únicamente como Servidor de Acceso a la Red, mientras que en una red con servicio de IP móvil, también cumple la función de un FA. El Agente Foráneo (FA – Foreing Agent) trabaja en conjunto con el HA con el fin de realizar el reenvío del tráfico de Internet a la MS conectada desde cualquier ubicación diferente a su red local.

1.6 CDMA2000 1xEV-DO

Entre las características principales de CDMA2000 1X se encuentran:

- Esta en la capacidad de operar en las bandas de frecuencia de 800Mhz y 1900Mhz.
- No requiere de recursos proporcionados por el MSC.
- Puede brindar a los subscriptores velocidades de hasta 2,4Mbps en el enlace de bajada y 153,6Kbps en el enlace de subida
- Mejora 3.5 a 4 veces el *throughput* de datos en comparación con sistemas 1X en el enlace de bajada.
- *Handoff* entre portadoras 1xEV-DO y 1X para dispositivos de usuarios duales, lo que permite que los usuarios reciban servicios de voz u otros servicios 1X de la portadora 1X.

La arquitectura de la red CDMA2000 1xEV-DO es prácticamente idéntica a la de la red CDMA2000 1X, ya que reutiliza todos sus elementos de red; la diferencia radica en las siguientes actualizaciones que se realizan a la infraestuctura existente:

- Actualización hardware en el BSC, llamada Controlador de Acceso a la Red (ANC – Access Network Controller) que en ocasiones ya incluye la funcionalidad del PCF (es por eso que en CDMA2000 1xEV-DO el BSC se llama en ocasiones ANC/PCF).
- Actulización hardware en el BTS con la adición de un Módulo de Canal de o Datos (DCM – Data Channel Module).
- Actualización software en el PDSN.

2. REDES WLAN

Con el fin de lograr las velocidades nombradas en el capitulo 1.2.1 – 1.2.3, cada uno de los estándares maneja variados mecanismos de modulación. 802.11b emplea la técnica de Ensanchamiento de Espectro por Secuencia Directa (DSSS - Direct Secuence Spread Spectrum) y técnicas como la Modulación por Desplazamiento de Fase Bivalente Diferencial (DBPSK – Differential Binary Phase Shift Keying) para velocidades de 1Mbps, la Modulación por Desplazamiento de Fase Cuadrivalente Diferencial (DQPSK - Differential Quadrature Phase Shift Keying) para velocidades de 2Mbps y la Modulación de Código Complementario (CCK - Complementary Code Keying) para velocidades de 5.5 y 10 Mbps. 802.11a utiliza una técnica de modulación de frecuencia llamada Multiplexación por División de Frecuencia Ortogonal (OFDM – Orthogonal Frecuency Division Multiplexing), la cual le permite alcanzar altas velocidades como 54 Mbps. De igual forma que la tecnología 802.11a, la tecnología 802.11g se basa en una técnica de modulación OFDM que proporciona una velocidad máxima de 54 Mbps en la transmisión de datos.

Arquitectura de red WLAN

Entre los elementos que forman parte de una red WLAN se incluyen APs inalámbricos y otros componentes escalables como *gateways* y *switches* WLAN. La figura A.5 muestra la arquitectura típica de una WLAN.

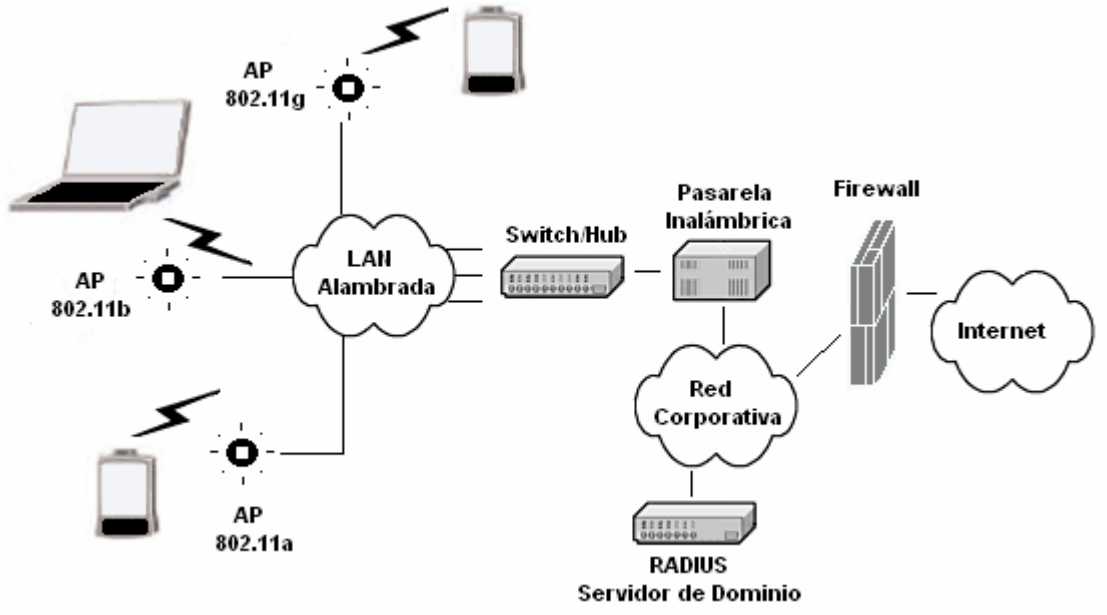

Figura A.5. Arquitectura típica de una WLAN. [4]

Punto de Acceso (AP – Acces Point): es el dispositivo de red encargado de brindar el acceso inalámbrico a los equipos WLAN transformando las señales de radio

analógicas en señales digitales que se pueden enviar por la red cableada. Entre las funciones principales del AP se encuentran:

- Autenticación de equipo de usuario: Cada AP tiene un número de Identificación del Juego del Servicio de una WLAN (SSID – Service Set Identification), el cual define la subred que éste controla. El SSID es un mecanismo simple de *password,* por lo tanto, cualquier equipo que intente conectarse con el AP debe tener el mismo SSID. Debido a que el AP - por defecto - periódicamente difunde su SSID (típicamente cada 10 ms), cualquier equipo puede eventualmente adquirir el SSID a través de técnicas de *sniffing* de datos sobre la interfaz de aire y conectarse al AP. Esta característica, en la mayoría de los casos, está deshabilitada por razones de seguridad.

- Encriptación de los datos: La mayoría de los APs están dotados con WEP como característica de seguridad básica para realizar encripción de datos y autenticación de equipos. Desafortunadamente WEP presenta inherentes debilidades relacionadas con la seguridad, lo cual ha retardado la adopción de WLANs en las empresas. A pesar de esto, WEP aun es habilitado como un nivel de seguridad de datos mínimo, y en su lugar ya existen equipos con otros estándares de seguridad, como lo son WPA y 802.11i.

- Asignación de Recursos: El AP utiliza, por defecto, el Protocolo de Configuración Dinámica de Host (DHCP – Dynamic Host Configuration Protocol) para asignar dinámicamente direcciones IP a los equipos asociados en la subred. Sin embargo, equipos no autorizados que han *sniffed* el SSID difundido por el AP, pueden recibir una dirección IP y obtener acceso a la red a través de dicho AP. Por ésta razón, DHCP debe ser deshabilitado si no se cuenta con un estándar de seguridad confiable que impida o minimice las posibilidades de que un usuario no autorizado acceda a la red, teniendo que utilizarse direcciones IP estáticas.

Tarjetas de Interfaz de Red (NICs – Network Interface Cards)*:* también denominadas como adaptadores de equipos o tarjetas WLAN. Sirven como *transceivers,* y son los encargados de establecer la conexión con el AP al cual se encuentran asociados. Similar a la funcionalidad del AP, los adaptadores realizan conversión de señal analógica a digital, autenticación del usuario y del equipo y manejo de potencia, así como otras funciones esenciales para el establecimiento de la comunicación. Las NICs por lo general se insertan el los portátiles y PCs de escritorio a través de un *slot* o ranura de expansión PCMCIA o USB. Tarjetas flash compactas (CF – Compact Flash) y tarjetas conectores de red incrustadas (es decir, tarjetas mini PCI) se utilizan en PDAs, PCs de bolsillo y otros equipos móviles similares.

Gateway Inalámbrica: La *gateway* Inalámbrica es un dispositivo de interconexión de redes que realiza funciones de enrutamiento de tramas de una WLAN a otra red, típicamente una Red de Área Amplia (WAN – Wide Area Network), operando

en los niveles 2 y 3 del modelo OSI y combinando las funciones de un AP, un enrutador, y a menudo proporcionando funciones de *firewall.* Frecuentemente incluyen enrutamiento NAT y servicios DHCP, a la vez que pueden incluir seguridad, encripción, VPN y VoIP. Por lo general desempeña el papel de intermediación en el proceso de autenticación de usuarios.

Servidor RADIUS: Este elemento de red desempeña el papel de servidor AAA para los usuarios locales y como un Proxy AAA para usuarios visitantes. En algunos casos, estos dos roles (proxy y servidor) se encuentran implementados utilizando servidores RADIUS independientes. El papel del servidor AAA resulta fundamental en redes públicas que prestan un servicio de telecomunicaciones a los usuarios, ya que se encarga de procesar los registros de sesión de los usuarios para que sea posible generar la tarificación del servicio que se les presta. En los casos en los cuales se ofrece un servicio en prepago, la autenticación RADIUS soporta la transferencia del atributo *timeout* dentro de los atributos de sesión y su valor se establece de acuerdo con el tiempo de vencimiento de la cuenta prepago.

ANEXO B. SEGURIDAD EN WLANS Y PROTOCOLOS DE AAA PARA SOLUCIONES RÍGIDA Y LIGERAMENTE ACOPLADAS

1. PROTOCOLOS Y MECANISMOS DE SEGURIDAD EN REDES WLAN

1.1 FILTRADO DE DIRECCIONES MAC

Este método para proveer seguridad en redes WLAN, consiste en la creación de una tabla de datos en cada uno de los puntos de acceso a la red inalámbrica. Dicha tabla contiene las direcciones MAC (Media Access Control) de las tarjetas de red inalámbricas que se pueden conectar al punto de acceso. Como toda tarjeta de red posee una dirección MAC única, se logra autenticar el equipo.

1.2 WEP

El algoritmo WEP forma parte de la especificación 802.11, y se diseñó con el fin de proteger los datos que se transmiten en una conexión inalámbrica mediante encripción. WEP opera a nivel 2 del modelo OSI, siendo soportado por los equipos de la gran mayoría de fabricantes de soluciones inalámbricas. Básicamente consiste en la combinación de la información transmitida con una clave estática de 40 o 128 bits conocida tanto por el receptor como por el transmisor.

1.3 IEEE 802.1X

802.1X es un protocolo de control de acceso y autenticación basado en la arquitectura cliente/servidor que restringe la conexión de equipos no autorizados a una red. El protocolo fue creado inicialmente por la IEEE para uso en redes de área local alambradas, pero se ha extendido también a las redes inalámbricas, así que muchos de los puntos de acceso que se fabrican en la actualidad ya son compatibles con 802.1x. La arquitectura de 802.1x consta tres participantes: el suplicante o equipo del cliente, que desea conectarse con la red, el servidor de autorización/autenticación, que contiene toda la información necesaria para saber cuáles equipos y/o usuarios están autorizados para acceder a la red (802.1x fue diseñado para emplear RADIUS[4]) y el autenticador, que es el equipo de red (switch, enrutador, AP, servidor de acceso remoto...) que recibe la conexión del suplicante, es decir, que el autenticador actúa como intermediario entre el

[4] Protocolo de autenticación explicado en éste mismo anexo en la sección 2.1

suplicante y el servidor de autenticación, y solamente permite el acceso del suplicante a la red cuando el servidor de autenticación así lo autoriza.

La figura B.1 muestra los diferentes niveles de protocolos de red que intervienen en el proceso de autenticación de un usuario en una red WLAN. Es de resaltar que el protocolo EAP[5] y sus diferentes métodos son llevados desde el suplicante hacia el servidor de autenticación sin variación alguna. Por el contrario, los protocolos de bajo nivel cambian en el punto de acceso (EAP cambia a RADIUS). 802.1X define EAPOL así como la conversión de EAPOL a RADIUS, definiendo también el bloqueo de tráfico hasta la autenticación del usuario.

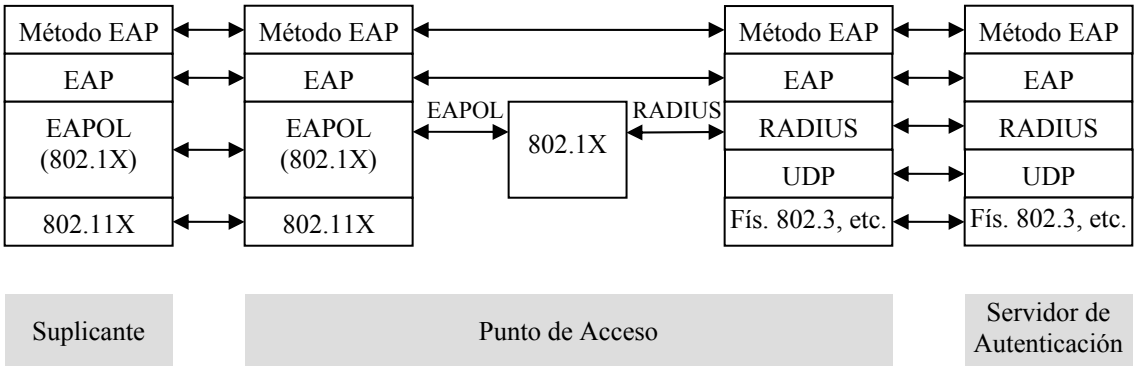

Figura B.1. Stack de Protocolos para autenticación RADIUS sobre un AP con capacidad 802.1X. [5]

802.1X busca superar la debilidad del estático WEP introduciendo diferentes métodos EAP dentro de la seguridad WLAN. La introducción de un servidor de autenticación dentro de configuraciones WLAN habilita escalabilidad en la empresa.

La seguridad en WLANs se divide en dos áreas básicas: privacidad de datos (encripción) y autenticación. Cuando 802.11 se introdujo como un estándar, intentaba apuntar a la necesidad de privacidad de datos (aunque bastante in satisfactoriamente) con WEP. La autenticación se limitaba a claves secretas compartidas, lo cual también significaba la utilización de claves estáticas, incambiables en la práctica. Los proveedores de la industria direccionaron este descuido para traer al mercado productos que soportaban el estándar IEEE 802.1X.

802.1X proporciona capacidad de control de acceso a la red por autenticación de usuarios utilizando un método de autenticación configurable a través de una autoridad central. Éste proporciona autenticación especificando cómo transportar información entre el suplicante y el autenticador, cómo ésta identidad puede verificarse con un servidor AAA/RADIUS y cómo el autenticador evita el acceso

[5] Protocolo de autenticación explicado en éste mismo anexo en la sección 2.2

del suplicante a la red hasta que el servidor AAA/RADIUS verifica la identidad. Cuando un suplicante intenta obtener acceso a una red habilitada 802.1X, se le impedirá la obtención del acceso a la red y se le solicitará que compruebe su identidad. La solicitud/respuesta se lleva a cabo entre el suplicante y el servidor de autenticación con el punto de acceso actuando como un proxy para esos intercambios. El servidor AAA/RADIUS compara la identidad con una base de datos de autenticación para la validación, si se encuentra que es una identidad de usuario válida, el autenticador permite el acceso a la red, si no, el acceso es denegado. Mientras 802.1X habilita la autenticación, no define el método específico de solicitud/respuesta utilizado para probar la identidad del usuario, con el fin de proveer adaptación de autenticación a necesidades particulares. 802.1X define como transportar EAP, un estándar de autenticación bien fundamentado por la IETF (RFC 2284), el cual es un protocolo general que permite uno de una lista de métodos emergentes EAP para utilizarse realmente en el proceso de solicitar al suplicante que pruebe su identidad. EAP (y el método EAP escogido) se encapsulan por 802.1X en EAPOL para el dialogo entre el suplicante y el autenticador. El dialogo entre el autenticador y el servidor AAA/RADIUS se conduce a través del protocolo RADIUS.

1.4 WPA

WPA es un estándar propuesto por los miembros de la Wi-Fi Alliance (que reúne a los grandes fabricantes de dispositivos para WLAN) en colaboración con la IEEE. Este estándar busca subsanar los problemas de WEP, mejorando la encripción de los datos y ofreciendo un mecanismo de autenticación. Para solucionar el problema de encripción de los datos, WPA propone un nuevo protocolo de encripción conocido como Protocolo de Integridad de Clave Temporal (TKIP - Temporary Key Integrity Protocol). Este protocolo se encarga de cambiar la clave compartida entre el punto de acceso y el cliente cada cierto tiempo para evitar ataques que permitan revelar la clave, además de mejorar los algoritmos de encripción de trama y de generación de vectores aleatorios con respecto a WEP. La norma WPA data de abril de 2003, y es de obligatorio cumplimiento para todos los miembros de la Wi-Fi Alliance a partir de finales de 2003. Según la Wi-Fi Alliance, todo equipo de red inalámbrica que posea el sello “Wi- Fi Certified” podrá ser actualizado por software para que cumpla con la especificación WPA.

WPA incorpora la estructura 802.1X/EAP, adicionando un sistema de manejo de claves sofisticado. Se destaca en WPA un robusto sistema de intercambio de claves que une funciones de autenticación y privacidad de datos. Las claves se generan después de una autenticación exitosa y a través de un posterior “saludo” de 4 formas entre la estación móvil y el punto de acceso.

WPA trata la mayoría de las vulnerabilidades conocidas de WEP y se dirige principalmente a WLANs como las encontradas en las empresas; aunque puede desplegarse en hogares y pequeñas oficinas de manera muy simple. WPA es más potente cuando se despliega con la configuración empresarial puesta por el

estándar IEEE 802.1X que incluye estaciones móviles, puntos de acceso y servidores de autenticación, típicamente servidores RADIUS.

La solidez de WPA viene de una secuencia de operaciones integradas que incluyen autenticación 802.1X/EAP y un manejo de claves sofisticado y técnicas de encripción. Entre las principales funciones se encuentran:

- Determinación de las capacidades de seguridad de red. Esto ocurre en el nivel 802.11 y se comunica a través de los elementos de información WPA en Soporte, Respuesta de Sondeo, y Peticiones de Asociación y Reasociación. La información en esos elementos incluyen el método de autenticación (802.1X o la clave pre-compartida) y el método de cifrado preferido (WEP, TKIP o AES (Advanced Encryption Standard)).

- Autenticación. Se utiliza EAP sobre 802.1X para la autenticación. Se obtiene autenticación mutua escogiendo un tipo de EAP que soporte esta característica que se requiere en WPA. El control de acceso al puerto 802.1X impide el acceso completo a la red hasta que la autenticación se complete. Los paquetes de claves EAPOL 802.1X se utilizan por WPA para distribuir las claves por sesión a aquellas estaciones autenticadas exitosamente.

- Manejo de claves. Se destaca en WPA un robusto sistema de generación/manejo de claves que reúne las funciones de autenticación y privacidad de datos, generando las claves después de un proceso de autenticación exitoso.

- Privacidad de datos (encripción). Se utiliza TKIP para envolver a WEP en una criptografía sofisticada y en técnicas de seguridad con el fin de superar la mayoría de sus falencias.

- Integridad de datos. WPA utiliza TKIP que incluye un Código de Integridad de Mensaje (MIC - Message Integrity Code) al final de cada mensaje de texto plano para asegurar que los mensajes no sean *spoofed* [6], repetidos o modificados en la transmisión.

1.5 IEEE 802.11i, WPA2

802.11i entrega mejoras en la integridad de los mensajes, los primeros pasos hacia un *roaming* basado en estándares e introduce encripción CCMP, que es un protocolo basado en el algoritmo de encripción AES utilizando el Counter Mode con el modo de operación CBC-MAC (CCM). El modo CCM combina el modo de privacidad Counter (CTR) y el código de autenticación Cipher Block Chaining Message Authentication Code (CBC-MAC). Estos modos se han utilizado y

[6] Cuando un intruso logra interceptar los datos o mensajes en una red asumiendo la identidad de otro usuario. En un *spoofing* el atacante falsifica el origen y/o destino de un paquete con el fin de alcanzar algún objetivo restringido. Éste puede asumir una identidad diferente cambiando su dirección MAC.

estudiado por largo tiempo y poseen unas propiedades criptográficas bien entendidas que proveen seguridad y rendimiento en hardware o software. CCM está únicamente definido para el uso con códigos de paquetes de 128 bits, como AES.

CCMP requiere de una clave temporal nueva para cada sesión y también un *nonce* particular para cada trama protegida por una clave temporal dada. Esto provee protección repetida, siendo el *nonce* un número de paquete de 48 bits. Para proteger la dirección MAC (la cual se ha enviado en texto plano) del *spoofing,* CCMP proporciona autenticación de origen a través de un método llamado AAD (Additional Authenticated Data), el cual incorpora los datos de encabezado dentro del MIC (Message Integrity Check) tal que también esté seguro de intromisiones. [6]

WPA2 (Wi-Fi Protected Access v2) es el estándar relacionado de la Alianza WiFi que mejora las capacidades del estándar WPA existente, y son virtualmente lo mismo con 802.11i. Con WPA, WiFi se sintió obligado a crear una división de 802.11i con el fin de suministrar rápidamente al mercado una de las medidas de seguridad más fuertes cubierta por 802.11i, la cual tenía aún que ser ratificada, además que tenia la necesidad de contrarrestar la mala imagen obtenida por las WLANs 802.11 como resultado de su débil método de privacidad de datos WEP.

Roaming rápido a través de la pre-autenticación de clientes por los puntos de acceso retuvo la ratificación sobre 802.11i, y esto aún no está completamente resuelto. La coordinación de los puntos de acceso no es una propuesta simple, e involucra la evaluación de métodos de competencia entre los mayores actores en la industria. El estándar 802.11i realizó algunos pasos iniciales en esta área, pero no entregó especificaciones detalladas para la pre-autenticación/*roaming* rápido. El *roaming* rápido puede incrementar en importancia cuando las WLANs empiecen a utilizar VoIP.

2. PROTOCOLOS DE AAA PARA SOLUCIONES RÍGIDA Y LIGERAMENTE ACOPLADAS

2.1 RADIUS

RADIUS es un protocolo que permite autenticación centralizada de usuarios con el fin de mantener un acceso a la red seguro. RADIUS se utiliza por los puntos de acceso a la red para comunicarse con el servidor de credenciales de usuario central que provee Autenticación, Autorización y Registro de Datos de Tarificación.

El servidor RADIUS es un tipo de servidor AAA muy popular debido a que utiliza comunicaciones encriptadas con otros equipos de red en el intercambio de la información de identificación de usuarios. Éstos se encuentran típicamente en

empresas o ISPs que necesitan mantener grandes bases de datos de usuarios, en las cuales son necesarios sistemas de seguridad escalables con la habilidad de administrar centralmente sus políticas de seguridad. En la figura B.2 se ilustra el proceso para permitirle a un usuario el acceso a una red WLAN a través del servidor RADIUS utilizando EAP.

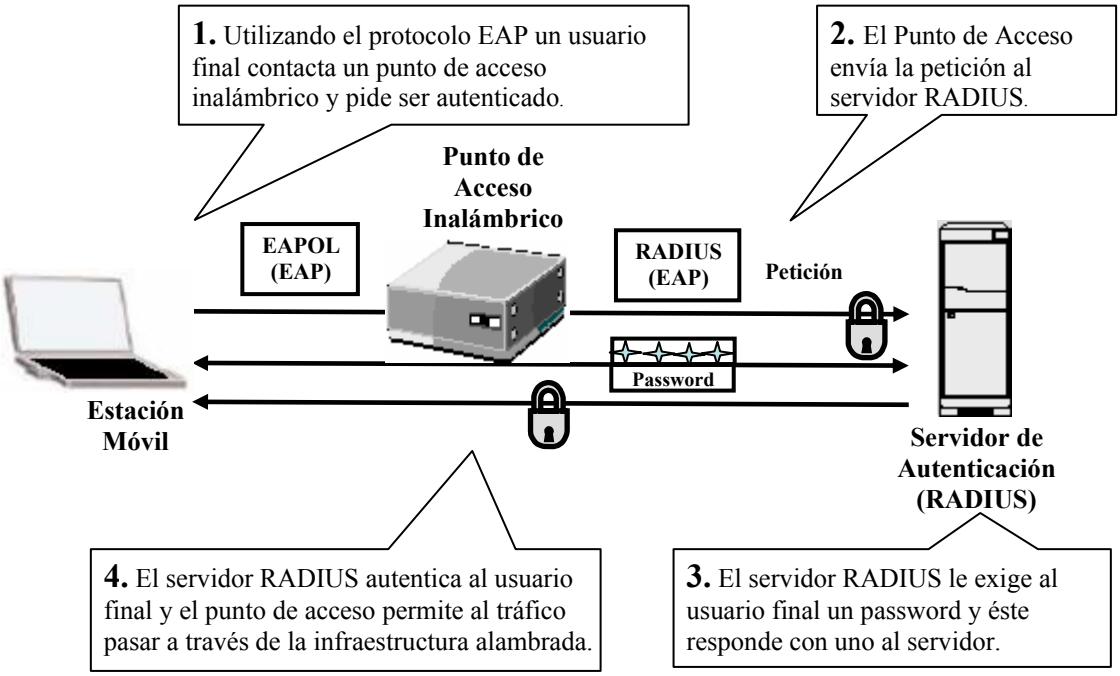

Figura B.2. Autenticación de un usuario a través de RADIUS [5]

El servidor RADIUS autentica usuarios finales que intentan obtener acceso a la red. En WLANs con capacidad 802.1X como la mostrada en la figura B.2, la comunicación EAPOL (EAP Over LAN) ocurre entre el usuario final (suplicante) y el punto de acceso (auntenticador), mientras que RADIUS se utiliza para comunicaciones encriptadas entre el autenticador y el servidor RADIUS.

2.2 EAP

El EAP es un protocolo de autenticación peer-to-peer usado entre un cliente y un servidor de autenticación final. El autenticador es la parte de autenticación del cliente y usa el servidor de autenticación final para realizar ésta. EAP ha sido definido como un protocolo de autenticación genérico, el cual por ejemplo puede ser ejecutado sobre el protocolo RADIUS, por lo que el autenticador puede entender únicamente comandos específicos del protocolo RADIUS. Para implementaciones futuras, el protocolo EAP se usará con el fin de autenticar una variedad de clientes móviles a través de diferentes tipos de autenticación soportados por el EAP. En el presente hay definidos, por ejemplo, EAP-SIM, EAP-

GPRS, EAP-AKA, entre otros. En la tabla B.1 se muestran algunos de los métodos EAP más utilizados actualmente.

TIPO DE EAP	REASIGNACIÓN DE CLAVES DINÁMICA	AUTENTICACIÓN MUTUA	LOGIN Y PASSWORD	COMENTARIOS
EAP-MD5	No	No	Si	♦ Inseguro ♦ Fácil de implementar ♦ Soportado en muchos servidores
EAP-TLS	Si	Si	No	♦ Requiere certificados de clientes ♦ Incremento en el mantenimiento y los costos
EAP-SRP	Si	Si	Si	♦ Sin certificados (el servidor verifica las claves secretas) ♦ Ataque diccionario sobre las credenciales almacenadas ♦ Debate sobre propiedad intelectual
EAP-LEAP	Si	Si	Si	♦ Solución propietaria de Cisco ♦ AP debe soportar LEAP
EAP-SIM	Si	Si	No	♦ Apalancamiento con la infraestructura de *roaming* GSM ♦ Autenticación mutua (únicamente UMTS)
EAP-AKA	Si	Si	No	♦ Apalancamiento con la infraestructura de *roaming* GSM
EAP-SecureID	No	No	No	♦ Password de usuarios PIN/*One-time* ♦ Requiere autenticación entunelada
EAP-TTLS	Si	Si	Si	♦ Creación de un túnel TLS (SSL) seguro ♦ Soporta métodos de autenticación de herencia: PAP, CHAP, MS-CHAP, MS-CHAP V2 ♦ La identidad de usuario es protegida (encriptada)
EAP-PEAP	Si	Si	Si	♦ Similar a EAP-TTLS ♦ Creación de un túnel TLS (SSL) seguro ♦ La identidad de usuario es protegida (encriptada)

Tabla B.1. Métodos EAP comúnmente utilizados. [5]

EAP no está definido en algún nivel OSI, es un protocolo “layer-less” o sin nivel, pero actualmente corre a nivel 2 sobre EAPOL/PPP y a nivel 3 sobre RADIUS/IKE2.

EAP es transportado por EAPOL, lo cual está definido en el estándar 802.1X, y los métodos EAP, que son transportados vía EAP, se han ideado para proveer una mayor seguridad de red y para trabajar en ambientes específicos, como es el caso de EAP-SIM (para convergencia de voz y datos). Debido a la flexibilidad de EAP para satisfacer las necesidades cambiantes, los métodos EAP pueden introducirse continuamente.

Los métodos EAP de mayor importancia en ambientes WLAN son: TLS, TTLS, LEAP y PEAP, los cuales soportan autenticación mutua, es decir, cuando un usuario autentica a la red y la red autentica al usuario, evitando así la asociación con falsos usuarios y redes no autorizadas.

Para sistemas ligeramente acoplados se consideran principalmente EAP-SIM, EAP-AKA y EAP-SIM-GMM, debido a que proporcionan apalancamiento con la infraestructura de *roaming* GSM/GPRS, y para las soluciones rígidamente acopladas existe un método emergente denominado EAP-GPRS que utiliza de igual forma que EAP-SIM, EAP-AKA y EAP-SIM-GMM información SIM para la autenticación del usuario. En las secciones 2.2.1 a 2.2.4 se describen estos métodos debido a su importancia y utilización en las soluciones de *roaming* entre las redes móviles celulares y las WLANs.

2.2.1 EAP-SIM

EAP-SIM define la utilización de la autenticación GSM con una estructura EAP. En una autenticación GSM normal, una sesión de solicitud-repuesta se mantiene entre la SIM y la infraestructura de autenticación del operador (HLR/AuC). La red autentica la SIM a través del uso de algoritmos y claves secretas ubicadas únicamente en la SIM y en el HLR/AuC. Un efecto secundario del mecanismo es la generación de claves de encripción para el enlace radio. Este es un método de autenticación de tarjeta inteligente, las cuales pueden almacenar pequeños programas e información acerca de la historia del equipo, su utilización y su dueño. Los clientes utilizan estas pequeñas tarjetas que contienen sus credenciales para autenticar y ser autenticados por la red.

EAP-SIM se constituye sobre este fundamento y utiliza métodos criptográficos conocidos y probados que incrementan la entropía del material de autenticación original los que dificulta su reconocimiento por parte de agentes externos. El proceso real se describe a continuación:

- Una comunicación 802.11 inicial utilizando 802.1X (EAP) empieza con una estación móvil no autenticada intentando conectarse con un punto se acceso que sirve de intermediario con el servidor de autenticación. El AP 802.1X tiene dos

puertos lógicos: un puerto no controlado que permite tráfico EAP y un puerto controlado, que se abre solo cuando la autorización 802.1x es exitosa. El punto de acceso se conecta a un servidor de autenticación.

- La presencia de la estación móvil dispara el protocolo EAP en el servidor de autenticación.
- La autenticación solicita la identidad de la estación móvil, la cual es obtenida de su tarjeta SIM.
- Utilizando esta información, el servidor de autenticación solicita el material de autenticación del operador de red móvil de la misma forma que un flujo GSM normal (desde el HLR/AuC). Sin embargo, utilizando funciones criptográficas de una vía, el material de autenticación no solo es simplemente comparado, si no que se utiliza para obtener varias claves secretas compartidas: una clave de autenticación de cliente, una clave de autenticación de red y una clave de sesión master. (Estas claves son mucho más largas que el material de autenticación original). La estación móvil depende de la tarjeta SIM para realizar los mismos cálculos. Se realiza autenticación mutua utilizando un protocolo de solicitud/respuesta clásico.
- La red autentica el cliente y el cliente autentica la red utilizando diferentes claves.
- Cuando ésta se realiza exitosamente, el puerto controlado en el punto de acceso se abre a la estación móvil, utilizando la clave de sesión master para proteger todos los datos del *payload* entre el punto de acceso y la estación móvil.

La principal ventaja de tal estructura es que no se requieren modificaciones en el núcleo de red GSM. Lo que se necesita es comunicación entre el servidor de autenticación y el HLR/AuC, y entre el software cliente EAP-SIM y la tarjeta SIM en el equipo del cliente. [7]

2.2.2 EAP-AKA

Este EAP permite que el cliente móvil GSM/UMTS sea autenticado en redes WLAN. Al igual que en EAP-SIM, se utilizan mecanismos similares que se basan en la funcionalidad de la SIM del cliente. El protocolo tiene soporte para autenticación mutua en modo UMTS mientras que soporta únicamente autenticación en un sentido para clientes GSM.

2.2.3 EAP-SIM-GMM

Este es un método de autenticación basado en SIM para la estructura de autenticación EAP. Similar a EAP-SIM y EAP-AKA, este método utiliza la SIM para propósitos de autenticación sobre una red GPRS, este lo hace utilizando el protocolo de Gestión de Movilidad y Seguridad GPRS (GMM) con el fin de realizar Attach/Detach GPRS y operaciones de autenticación. Como el protocolo cuenta con una más baja seguridad de transporte de nivel de red, recomienda el uso de encripción proporcionada por la red en lugar del uso, por ejemplo, de claves Kc, con el fin de mantener la confidencialidad de las claves secretas de los clientes

móviles y de los algoritmos utilizados para la autenticación y encripción de datos. [8]

2.2.4 EAP-GPRS

EAP-GPRS provee una extensión al protocolo EAP para soluciones de integración WLAN/GPRS rígidamente acopladas cuando usa el *backbone* de la red GPRS como la red de transporte para todo el tráfico de origen WLAN. El estándar especifica como el cliente móvil podría usar la tarjeta WLAN en vez de su modulo GPRS como la Tecnología de Radio Acceso (RAT-Radio Access Technology).

Este estándar usa en similitud con el EAP-SIM o EAP-AKA los mecanismos de autenticación proporcionados por la SIM card. Estos protocolos serán explicados más adelante ya que se usan en las soluciones ligeramente acopladas.

EAP-GPRS permite a los clientes GPRS asociarse y/o hacer *roaming* a un núcleo de red GPRS a través de equipos que cumplen con control de acceso basado en EAP (como los puntos de acceso 802.1x). Un escenario típico donde EAP-GPRS es ampliamente aplicable es cuando una WLAN se encuentra rígidamente acoplada con un núcleo de red GPRS y sirve como una tecnología de radio acceso complementaria, por ejemplo, cuando la WLAN se encuentra conectada al núcleo de red GPRS en la interfaz Gb o Gn con control de acceso 802.1x. Cuando un cliente GPRS entra a la WLAN necesita negociar con dos procedimientos de control de acceso independientes: primero el 802.1x debido a los puntos de acceso WLAN y segundo el control de acceso específico GPRS debido a su propio núcleo de red GPRS. Con la ayuda de EAP-GPRS, la señalización de control de acceso (o gestión de movilidad) toma lugar en el contexto de la señalización de control de acceso 802.1x como un procedimiento dentro de este. Esto es, si el control de acceso es exitoso (o no), entonces el procedimiento 802.1x es también exitoso (o no). Con estas propiedades, EAP-GPRS llega a ser un mecanismo que correlaciona los dos esquemas de control de acceso y permite a los clientes GPRS usar los mismos mecanismos de Gestión de Movilidad GPRS (GMM) independientemente de la tecnología de radio de bajo nivel, es decir GPRS o WLAN. Esto permite implementaciones de clientes GPRS más simples y una gestión del suscriptor más simple, requiriendo una suscripción GPRS única para controlar tanto el acceso WLAN como el acceso de núcleo de red GPRS.

Permitiendo que la señalización GMM sea transportada en el contexto del procedimiento 802.1x, EAP-GPRS puede facilitar *roaming* inter-RAT (es decir entre la red GPRS y la WLAN) con el uso de un único protocolo de gestión de movilidad. Por ejemplo, cuando el cliente pasa de una red de radio acceso GSM a una red de radio acceso WLAN, el típico procedimiento GPRS de Actualización de Área de Enrutamiento (RAU-Routing Area Update) puede ser llevado en el contexto del procedimiento 802.1x. De esta manera, se le debería permitir al

cliente hacer el *roaming* a la nueva área WLAN, terminando exitosamente el procedimiento de RAU y el procedimiento 802.1x.

EAP-GPRS no es un nuevo mecanismo de autenticación, más exactamente sería un nuevo mecanismo de transporte para protocolos de más alto nivel. Esos protocolos de más alto nivel son referidos como Aplicaciones de Usuario EAP-GPRS (UAs). EAP-GPRS depende de las UAs para autenticar un cliente GPRS y proveer un grado particular de servicio de transporte (es decir detección de error, control de secuencia, control de flujo, etc.). EAP-GPRS puede en general también soportar UAs no específicas de GPRS, por lo tanto, EAP-GPRS puede soportar tanto clientes GPRS como clientes no GPRS.

En general, la ventaja de usar EAP-GPRS es primero que los procedimientos GMM pueden llevarse en el contexto de un procedimiento de bajo nivel 802.1x, y segundo que se crea un mecanismo de correlación entre esos procedimientos. Con tal mecanismo de correlación teniendo lugar, el procedimiento 802.1x termina exitosamente o no, basado en el resultado del procedimiento GMM implicado, en otras palabras, cuando un cliente GPRS gestiona una asociación o un *roaming* exitosamente al núcleo de red GPRS, entonces el procedimiento 802.1x termina exitosamente y el cliente GPRS es autorizado para usar un puerto en la red de acceso para la subsiguiente transferencia de datos. De lo contrario, si al cliente GPRS se le rechaza el acceso al núcleo de red GPRS (debido a falla en la autenticación o limitaciones de suscripción), entonces el procedimiento de bajo nivel 802.1x termina no exitosamente y el cliente no puede usar la red de acceso para ninguna transferencia de datos.

Otra ventaja de usar EAP-GPRS es que los móviles multi-RAT, por ejemplo que soporten dos o más tecnologías de radio acceso como GSM/GPRS, IEEE 802.11, etc., pueden implementar un único juego de procedimientos de gestión de movilidad a través de todas las RATs soportadas. Con EAP-GPRS los procedimientos de gestión de movilidad GPRS pueden también ser aplicados sobre redes que impliquen control de acceso 802.1x.

EAP-GPRS provee los siguientes servicios:

- Iniciación y terminación de un dialogo GPRS que toma lugar en el contexto de un procedimiento de control de acceso 802.1x.
- Negociación del modo de transferencia (o aplicación de usuario) que será usado por el dialogo GPRS.
- Encapsulamiento de mensajes de aplicación de usuario en paquetes que pueden pasar a través de elementos de red, lo cual obliga el control de acceso 802.1x.
- Transferencia punto a punto de mensajes de aplicación de usuario entre dos pares EAP-GPRS. Este servicio de transferencia no provee ninguna clase de detección de error, corrección de error, control de flujo, identificación de mensajes

perdidos y duplicados, etc. Esos servicios son asumidos para ser proveídos por la aplicación de usuario.

En un escenario de uso típico, los mensajes de aplicación de usuario pueden ser tramas LLC GPRS, las cuales incluyen mensajes de gestión de movilidad GPRS. [9]

2.3 TARIFICACIÓN EN SOLUCIONES LIGERAMENTE ACOPLADAS

2.3.1 Creación de CDRs en la WLAN

Cuando los clientes GPRS entran y salen de las redes WLAN, generan registros tarificables de inicio y fin de sesión, que son enviados a un servidor AAA que maneja un protocolo como RADIUS. La información de tarificación es almacenada por ejemplo en una base de datos SQL que contendrá toda la información necesaria para que el servidor genere los CDRs adecuados que puedan ser transferidos al sistema de facturación. La generación de CDRs no necesita realizarse en tiempo real, así que puede programarse para realizarse durante las horas que el servidor AAA no se encuentra sobrecargado.

El formato para los CDRs ha sido especificado para seguir las normas de ASN.1. Este es el formato de registro que se utiliza más comúnmente para información de cobro en redes GPRS. La estructura exacta de los CDRs ASN.1 se resume en el RFC 3332 [10]. El formato CDR se usa durante las transmisiones a los sistemas de facturación.

Entre los parámetros más relevantes para la autenticación de usuarios GPRS que desean utilizar servicios WLAN son:

- MSISDN/IMSI del cliente
- Password estático
- Especificaciones del perfil de producto para todos los usuarios basados en SIM

Los parámetros relevantes que deben reunirse para la Autenticación y la generación de información CDR son:

- Número MSISDN/IMSI del cliente
- Dirección IP del cliente
- Punto de acceso / Dirección IP del NAS
- Volumen de datos enviados/recibidos en bytes
- Tiempo de sesión
- Id de la sesión
- Marca de tiempo / registro de tiempo de Record comienzo
- Perfil del producto de usuario
- Método de autenticación
- Nivel de servicio QoS

2.3.2 Métodos de cobro WLAN-GPRS

2.3.2.1 Usuarios GPRS post-pago

La gestión de contabilidad para este tipo de clientes no necesita ninguna clase de acción acerca de los “créditos perdidos” en los clientes de suscripción GPRS. Al cliente se le cobra por todos los servicios usados a través de una factura mensual por parte del operador GPRS del cliente.

2.3.2.2 Usuarios GPRS pre-pago/cash card

Clientes GPRS prepago que hacen *roaming* en redes WLAN pueden tener un problema cuando sus tarjetas pre-pago se quedan sin créditos, ya que se debe mantener un control activo de la cantidad de créditos utilizados por el cliente. Puede existir una situación en la que el cliente GPRS se queda sin créditos en el momento que esta utilizando la WLAN, esto requiere una solución de tiempo real donde la cantidad de créditos restantes en la tarjeta pre-pago son monitoreados activamente a través de la red GPRS.

Tal solución está directamente relacionada con como es manejada la tarificación. Si el cobro por el uso de la red puede ser realizado en tiempo real, entonces la cuenta de los créditos restantes es más fácil. En una implementación real en redes WLAN, es más probable que el cobro y facturación se manejen en tiempo no real.

Una solución a esto es que el cliente esté capacitado para usar los recursos de la actual red para un tiempo limitado previamente autorizado por el servidor RADIUS, basándose en la cantidad de créditos que quedan en la tarjeta prepago del cliente. Este también puede seleccionar cuanto tiempo o cuantos datos va a usar durante su sesión con el fin de autorizar la tarjeta prepago para un tiempo específico. Después de la autorización por una cantidad limitada de tiempo/datos, los créditos se cierran hasta que el cliente ha terminado la sesión y la información de cobro final puede agregarse al usuario.

ANEXO C. CONCEPTOS FUNDAMENTALES DE LOS PROTOCOLOS IP MÓVIL Y SCTP

1. IP MÓVIL

IP Móvil es un estándar abierto definido por la IETF que permite al usuario mantener la misma dirección IP, permanecer conectado, y mantener aplicaciones en curso mientras se mueve de una subred IP a otra. Este protocolo incluye los recursos adecuados para proveer movilidad a través de redes homogéneas y heterogéneas. El estándar IP Móvil se basa en unos pocos componentes que se describen a continuación.

1.1 ENTIDADES DE LA ARQUITECTURA IP MÓVIL

El estándar IP Móvil introduce las siguientes entidades funcionales:

Nodo Móvil:

Un host que cambia su punto de conexión de una red o subred a otra. Éste puede cambiar su ubicación sin cambiar su dirección IP, continuando la comunicación con otros nodos de Internet en cualquier ubicación utilizando su dirección IP (constante o local), asumiendo conectividad de nivel de enlace (a través de direcciones MAC) hacia un punto de conexión disponible.

Agente Local:

Un router en una red local del nodo móvil, el cual entunela los datagramas para su entrega hacia el nodo móvil cuando éste se encuentra fuera de su red local, manteniendo la información de ubicación actual del mismo.

Agente Foráneo:

Un router en una red foránea del nodo móvil, el cual proporciona servicios de enrutamiento hacia el nodo móvil mientras éste se encuentra registrado. El agente foráneo desentunela y entrega los datagramas entunelados y enviados por el agente local hacia el nodo móvil correspondiente.

A un nodo móvil le es dada una dirección IP de largo término en una red local determinada. Esta dirección local se administra de la misma forma como una dirección IP "permanente" es proporcionada a un host fijo. Cuando el usuario se encuentra fuera de su red local, se asocia una dirección "care-of" con el nodo móvil, la cual refleja el punto de conexión actual del mismo. El nodo móvil utiliza su dirección local como dirección fuente para todos los datagramas IP que éste envía, excepto en algunos casos especiales para funciones de gestión de movilidad descritos en el RFC del estándar IP Móvil.

1.2 FUNCIONALIDAD GENERAL DE IP MÓVIL UTILIZANDO DIRECCIONES *CARE-OF Y COLOCATED CARE-OF*

Dependiendo del tipo de direcciones que se utilizan en una configuración IP Móvil, existen diferentes formas de recepción de los paquetes en el nodo móvil. Éstas direcciones son las direcciones *care-of* y las direcciones *colocated care-of*

1.2.1 Funcionalidad utilizando direcciones *care-of*

Un FA posee una o varias direcciones IP que asigna a las MS (TE) visitantes llamadas direcciones *care-of*. Se debe tener en cuenta que una dirección *care-of* puede ser compartida por mas de una MS (TE). El proceso de envío de información desde y hacia una estación móvil que utiliza una dirección *care-of* se ilustra en la figura C.1.

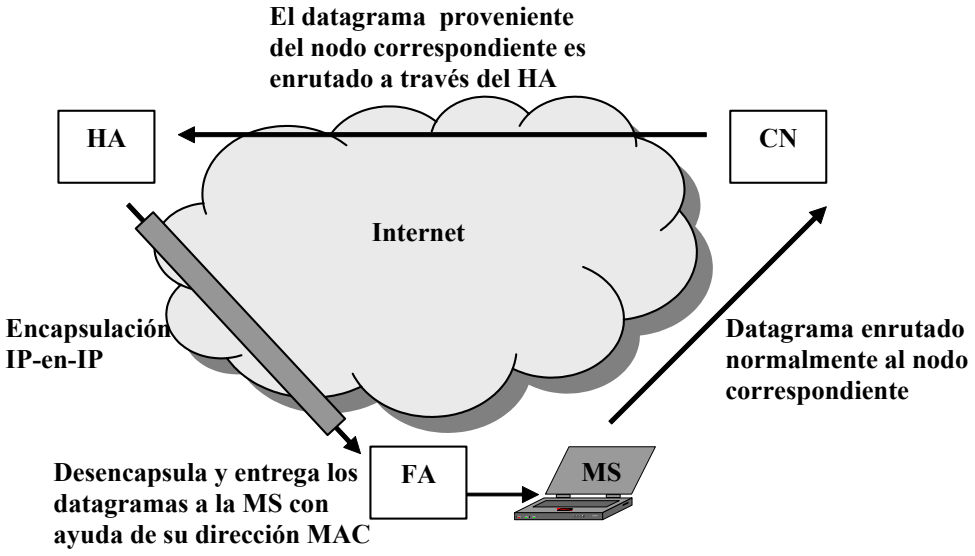

Figura C.1. Dirección *care-of.* [11]

Como se observa en la figura C.1, la dirección IP del FA se utiliza como destino para los paquetes entunelados que se envían a la MS. Para determinar a cual MS el FA debe entregar los paquetes desencapsulados, el FA posee una tabla que

relaciona la dirección *care-of* asignada, con las direccion IP que cada MS (TE) posee en su red local.

1.2.2 Funcionalidad utilizando direcciones *co-located care-of*

En este escenario, el nodo móvil recibe una dirección IP que puede utilizar mientras visita la red, por medio de un protocolo como DHCP o un protocolo similar. El proceso de envío de información desde y hacia una estación móvil que utiliza una dirección *co-located care-of* se ilustra en la figura C.2.

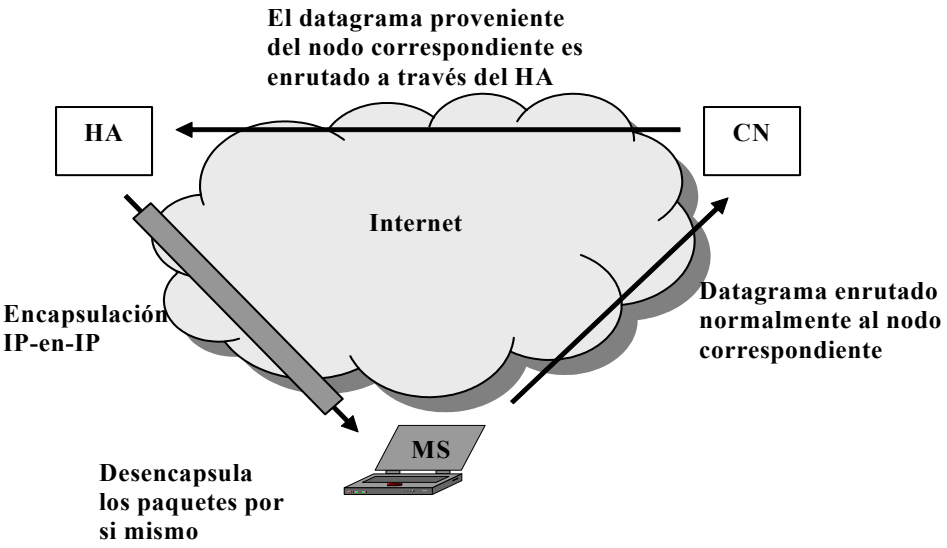

Figura C.2. Dirección *co-located care-of.* [11]

La diferencia primordial entre la dirección *care-of* y *co-located care-of* radica en que el nodo móvil es quien se encarga de desencapsular los paquetes cuando utiliza direcciones *co-located care-of.*

2. SCTP

A continuación se presenta el modelo de manejo de direcciones por parte de SCTP con el esquema de multi-localidad, donde un punto final único soporta múltiples conexiones con diferentes interfaces y direcciones IP simultáneamente, intercambiando listas de direcciones IP durante la iniciación de una conexión o asociación, haciendo posible la movilidad y el *roaming* a través de diferentes redes. [12]

En una asociación SCTP (conexión que SCTP provee a los puntos extremos), hay dos puntos extremos y dos direcciones conocidas por ambos. Esta asociación (A) está dada por:

$$A = [E1 : Addr(E1); E2 : Addr(E2)]$$

Donde *E1* (Endpoint 1) es el punto extremo 1 con dirección *Addr(E1)* (Address(E1)) y *E2* (Endpoint 2) es el punto extremo 2 con dirección *Addr(E2)* (Address(E2)).

En implementaciones IP, la interfaz de un *host con multi-localidad* está determinada por su dirección IP de destino. El mapeo de las direcciones IP fuente y destino se hace a través de un *lookup* en la tabla de enrutamiento (RT-Routing Table) de *hosts* mantenida por el sistema operativo. Se asume que un punto extremo *E* tiene *m* direcciones IP fuente en la asociación: *s_IP1 (source_IP1), ..., s_IPm* y su correspondiente tiene *n* direcciones IP: *d_IP1 (destine_IP1), ...,d_IPn*. El camino principal en la asociación es la conexión entre *s_IP1 y d_IP1.* Por lo tanto, la tabla de enrutamiento de *hosts* del punto extremo *E* puede expresarse como:

$$RT = [(s\_IP1, d\_IP1); (s\_IP2, d\_IP2), ..., (s\_IPm, d\_IPn)]$$

Hay que notar que el par de direcciones IP primarias está separado de los pares de direcciones IP secundarias con un ";". Cuando *m≠n,* el mapeo de direcciones no es de correspondencia uno a uno.

Los procesos necesarios para el manejo de direcciones con la extensión SCTP DAR se describen en las tres siguientes secciones:

2.1 ADICIÓN DE UNA DIRECCIÓN IP

Dada una asociación:

$$A = [MS : Addr(MS); CN : Addr(CN)]$$

Donde:
MS: estación móvil (mobile station)
CN: nodo correspondiente (correspondent node)

Antes del proceso de adición de la dirección IP:

$$Addr_{old}(MS) = \{MS\_IP1\} \text{ y } Addr_{old}(CN) = \{CN\_IP1\}$$
$$RT_{old}(MS) = [(MS\_IP1, CN\_IP1)]$$
$$RT_{old}(CN) = [(CN\_IP1, MS\_IP1)]$$

Después del proceso de adición de la dirección IP (la nueva dirección IP de la MS (*MS_IP2*) es adicionada a la asociación):

$$Addr_{new}(MS) = Addr_{old}(MS) \text{ Y } \{MS\_IP2\} = \{MS\_IP1, MS\_IP2\}$$

$$RT_{new}(MS) = [(MS\_IP1, CN\_IP1)]$$
$$RT_{new}(CN) = [(CN\_IP1, MS\_IP1); (CN\_IP1, MS\_IP2)]$$

2.2 ELIMINACIÓN DE UNA DIRECCIÓN IP

Antes del proceso de eliminación de la dirección IP:

$$Addr_{old}(MS) = \{MS\_IP1, MS\_IP2\} \text{ y } Addr_{old}(CN) = \{CN\_IP1\}$$
$$RT_{old}(MS) = [(MS\_IP1, CN\_IP1)]$$
$$RT_{old}(CN) = [(CN\_IP1, MS\_IP1); (CN\_IP1, MS\_IP2)]$$

Después del proceso de eliminación de la dirección IP (la dirección *MS_IP2* es eliminada de la asociación):

$$Addr_{new}(MS) = Addr_{old}(MS) - \{MS\_IP2\} = \{MS\_IP1\}$$
$$RT_{new}(MS) = [(MS\_IP1, CN\_IP1)]$$
$$RT_{new}(CN) = [(CN\_IP1, MS\_IP1)]$$

2.3 COLOCACIÓN DE UNA DIRECCIÓN IP PRIMARIA

Antes del proceso de colocar una dirección IP primaria:

$$Addr(MS) = \{MS\_IP1, MS\_IP2\} \text{ y } Addr(CN) = \{CN\_IP1, CN\_IP2\}$$
$$RT_{old}(MS) = [(MS\_IP1, CN\_IP1); (MS\_IP2, CN\_IP2)]$$
$$RT_{old}(CN) = [(CN\_IP1, MS\_IP1); (CN\_IP2, MS\_IP2)]$$

Después del proceso de colocar una dirección IP primaria (la MS pide al CN poner la dirección *MS_IP2* como la dirección primaria):

$$RT_{new}(MS) = [(MS\_IP2, CN\_IP2); (MS\_IP1, CN\_IP1)]$$
$$RT_{new}(CN) = [(CN\_IP2, MS\_IP2); (CN\_IP1, MS\_IP1)]$$

ANEXO D. DESCRIPCIÓN DE LOS PROCESOS Y SEÑALES DEL ROAMING PARA LAS SOLUCIONES ESCOGIDAS

En esta sección se realiza una descripción de los procesos y señales involucrados en el *roaming* entre las redes móviles celulares, GPRS y CDMA2000, y la red WLAN para las soluciones IP Móvil seleccionadas como las más óptimas dentro del entorno colombiano, con el fin de brindar un análisis completo de los diferentes recursos y mecanismos utilizados para dar soporte al mismo.

Se describen los procesos llevados a cabo en el registro de los usuarios móviles a la red celular siendo habilitados para la utilización del estándar IP Móvil, la asignación de direcciones IP Móvil y la realización del *roaming* y asociación a la red WLAN.

1. *ROAMING* GPRS – WLAN A TRAVÉS DE IP MÓVIL UTILIZANDO EL NODO GGSN/FA

Para permitir a un usuario utilizar el servicio IP Móvil a través de la red GPRS, por ejemplo con direcciones *care-of* de un Foreing Agent, la MS necesita conectarse con el GGSN, la cual provee funcionalidad de FA IP Móvil.

Con el fin de que el usuario pueda transferir datos a través de la red GPRS, debe activarse un Contexto PDP (Packet Data Protocol) en la MS, el SGSN y el GGSN. El usuario inicia este procedimiento, el cual es similar al logueo en la red de destino requerida. El esquema de señalización en la figura D.1 muestra como la MS puede conectarse al GGSN/FA y registrarse con su HA con un mínimo de mensajes de activación de contexto PDP.

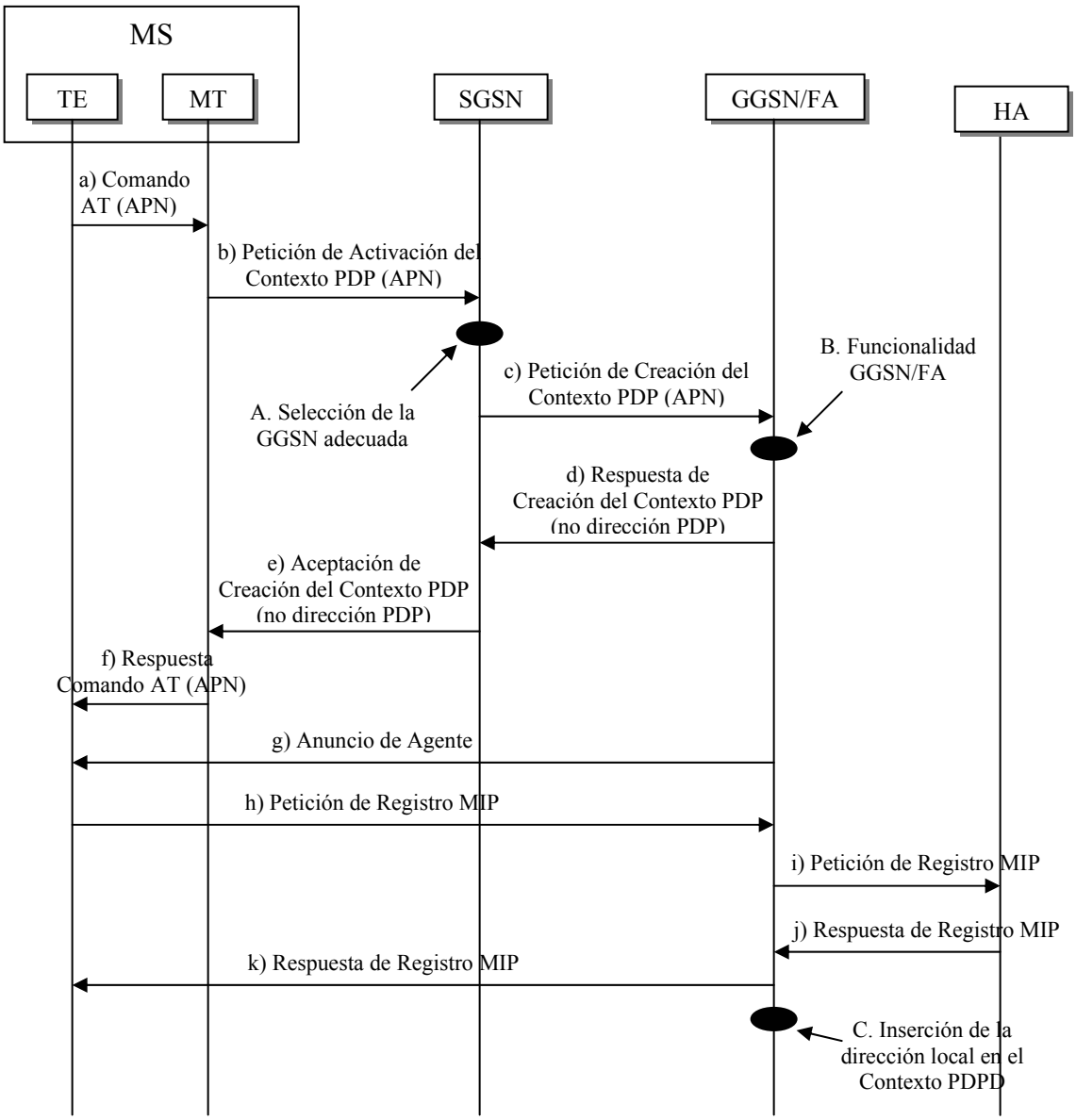

Figura D.1. Activación del contexto PDP con registro IP Móvil. [13]

A continuación se describe la funcionalidad de cada uno de los mensajes que participan en el proceso de activación del contexto PDP y del registro IP Móvil. No se detalla el proceso de iniciación de la conexión PPP entre el TE y el MT ni el de asociación GPRS, ya que este tema se sale del objetivo del trabajo de grado, además que estos procesos no varían con la inclusión de IP Móvil en la red GPRS.

Hay que tener en cuenta que las flechas en la figura D.1 denotan mensajes entre nodos y los círculos funcionalidad en un nodo.

a) El comando AT contiene parámetros que el MT necesita para realizar la petición de Activación del Contexto PDP, el más importante de estos es el Nombre del Punto de Acceso (APN - Access Point Name) ya que especifica

el GGSN o tipo de GGSN (si se requiere algún tipo de servicio y no se especifica el GGSN). El comando AT es seguido por la iniciación de la conexión PPP entre el MT y el TE.

b) El MT envía la Petición de Activación del Contexto PDP al SGSN. El mensaje incluye varios parámetros entre los que se encuentran el APN y la Dirección PDP Requerida. El APN es un nombre lógico referido a la red de paquetes de datos externa o a un servicio que el usuario desea conectarse. La dirección PDP requerida deberá ser omitida (puesta a 0.0.0.0) por todas las MSs que usan IP Móvil (ya que posteriormente se utilizará la dirección local de la MS (TE) la cual es asignada dinámica o estáticamente por su red local). Los motivos por los que se realiza este proceso son que la dirección que se registre en el HLR sea la dirección IP Móvil y que el registro se realice de igual manera para todas las MSs.

De forma alternativa una dirección PDP asignada permanentemente puede incluirse, sin embargo esta dirección PDP debe ser una dirección IP GPRS, ya que es comprobada en el HLR y mapeada a un GGSN específica. Si la MS (MT) inserta la dirección IP Móvil estática del TE (la cual se relaciona con su red local) como dirección fuente en la petición de activación del contexto, el acceso es denegado por la SGSN.

A. El SGSN basará la escogencia del GGSN en el APN que es dado por la MS.

c) El SGSN solicita al GGSN establecer un Contexto PDP para la MS. Los campos de la dirección PDP y el APN son los mismos que en el mensaje de Petición de Activación del Contexto PDP que proviene de la MS.

B. Para anunciar su presencia y sus parámetros, el FA puede difundir mensajes de Anuncio de Agente regularmente, pero para evitar tráfico innecesario sobre la interfaz de radio, el nodo móvil puede pedir la información cuando la necesite, enviando un Mensaje de Solicitud de Agente. Sin embargo, cuando el GGSN/FA se da cuenta de que una nueva MS ha entrado a la red, podría enviar un mensaje de Anuncio de Agente dedicado directamente a la nueva MS. Esto ahorraría un mensaje de Solicitud de Agente vía radio desde la MS y aceleraría un poco el procedimiento de registro.

Se debe tener en cuenta que el GGSN no asignará una dirección IP GPRS temporalmente a la MS (por ejemplo una PDP) ya que se ha solicitado un servicio IP Móvil.

d) Una Respuesta de Creación de Contexto PDP se envía desde el GGSN/FA al SGSN. Si la creación del contexto PDP fue exitosa se devolverán algunos parámetros al SGSN, si no, se devolverá un código de error. Si el GGSN ha sido configurado con funcionalidad de FA para el APN solicitado,

la dirección PDP devuelta por el GGSN será 0.0.0.0 indicando que la dirección PDP será establecida en un proceso posterior entre la MS (TE) y el HA después del procedimiento de activación del Contexto PDP.

e) El mensaje de Aceptación de Activación del Contexto PDP se reenvía por la SGSN a la MS.

f) El MT envía una respuesta AT al TE para confirmar que la activación del contexto PDP ha sido realizada.

g) El Anuncio de Agente es un mensaje de Anuncio de Enrutador ICMP (Internet Control Message Protocol) con una extensión de anuncio de agente de movilidad. La última parte contiene parámetros del FA que la MS necesita, entre los cuales están una o más direcciones *care-of* que el FA ofrece. Este mensaje se envía en el plano de usuario GPRS, como un mensaje de difusión IP dirigido, por ejemplo con dirección de destino 255.255.255.255, sobre el TID para la MS específica con el fin de evitar una difusión sobre la interfaz de radio.

h) La Petición de Registro IP Móvil se envía desde la MS al GGSN/FA a través del *backbone* GPRS como tráfico de usuario.

La MS incluye parámetros como la dirección de su HA y su dirección local (estática). De manera alternativa, este puede solicitar una dirección temporal asignada por la red local enviando 0.0.0.0 como su dirección local, en cuyo caso se envía un Identificador de Acceso a la Red (NAI - Network Access Identifier) en la Extensión NAI-Nodo-Móvil (que se ha propuesto con el fin de manejar asignación temporal de direcciones). Este identificador tiene un formato similar a una dirección e-mail y únicamente identifica al usuario y a la red local del usuario.

Para mantener el enlace desde la red local con la MS correcta, el GGSN/FA almacena la dirección local de la MS o el NAI (si aún no le ha sido asignada esta dirección) y la dirección del enlace local de la MS, es decir, el TID. El GGSN/FA debe tener una dirección IP a la cual el nodo móvil pueda enviar la petición de registro, sin embargo esta no necesita ser conocida fuera de la PLMN.

i) El GGSN/FA reenvía la Petición de Registro IP Móvil a la red local del nodo móvil, donde un HA la procesa.

j) **k)** La Respuesta de Registro se envía desde la red local al GGSN/FA, el cual extrae la información que necesita (por ejemplo, la dirección local del nodo móvil asignada por la red local) y redirige el mensaje al nodo móvil en el plano de usuario GPRS. Como el GGSN/FA conoce el TID y el NAI o la dirección local, reenvía el mensaje a la MS correcta. Cuando una dirección

local ha sido asignada por la red local, el MS (TE) no conoce todavía su dirección IP, por lo tanto, análogamente con el Anuncio FA, se usa una dirección de difusión local como dirección de destino.

C. El GGSN realiza un procedimiento de modificación del Contexto PDP GGSN inicial, con el fin de actualizar la dirección PDP en el GGSN, por ejemplo, sustituir la dirección 0.0.0.0 (insertada inicialmente en la activación de contexto PDP) por la dirección asignada por el HA a la MS.

Después de haberse realizado este procedimiento, la MS queda registrada en el GGSN/FA y los paquetes dirigidos a ésta son encaminados desde el nodo correspondiente a través del HA y la GGSN/FA.

Debido a la movilidad del usuario a través de diferentes áreas, se pueden presentar varios procesos después de haberse realizado el registro IP Móvil en la red GPRS. A continuación se describen estos procesos, que incluyen el cambio de GGSN o *handover* entre GGSN/FAs y el *roaming* con la red WLAN.

1.1 *HANDOVER* ENTRE GGSN/FAs

Con la realización de este proceso se pretende cambiar de GGSN/FA durante la sesión en la red GPRS con el fin de optimizar la ruta a través de la cual se está prestando un servicio o sobre la cual se está realizando la conexión con la red de paquetes externa.

El SGSN tiene el control para realizar el cambio de GGSN/FA, por ejemplo, después de haber efectuado un *handover* inter-SGSN para optimizar la ruta desde el nuevo SGSN al GGSN/FA más adecuado. Si no existe un GGSN/FA más óptimo disponible, el SGSN no cambiará el GGSN/FA. El SGSN tiene la información acerca de los GGSN/FAs que están en su dominio, evitando de esta manera el cambio a un GGSN que no tenga un FA.

En la figura D.2 se ilustra el proceso de cambio de GGSN/FA. El cambio de GGSN/FA normalmente sería realizado después de un *handover* SGSN, pero podría utilizarse para balanceo de carga entre dos GGSN/FAs.

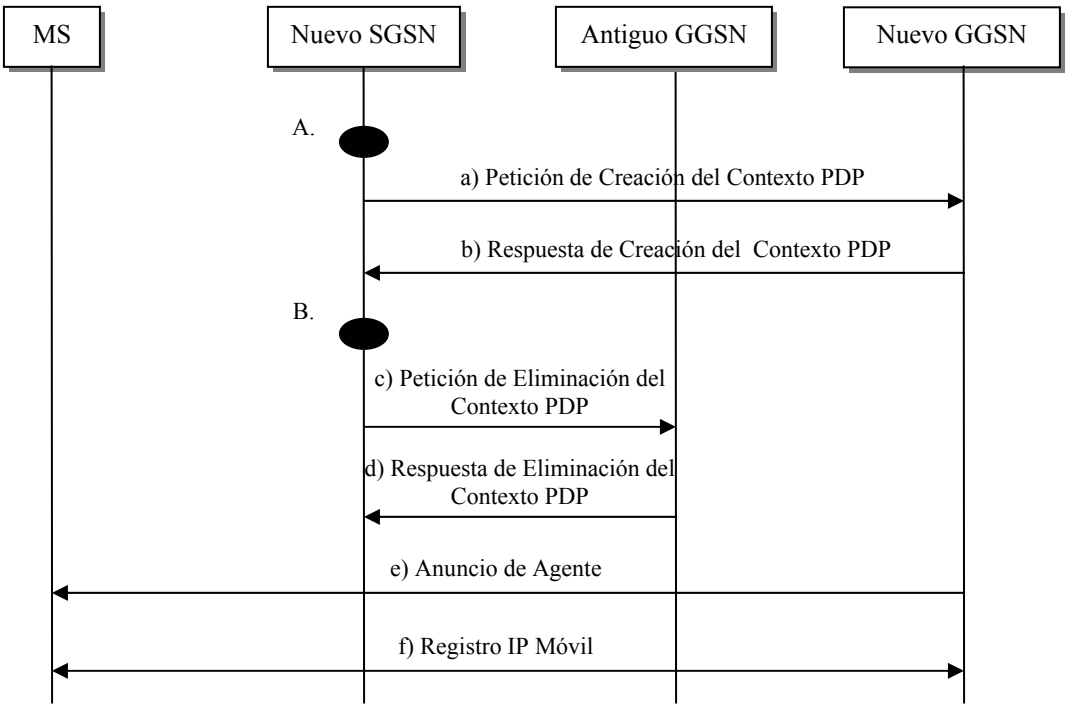

Figura D.2. *Handover* entre GGSN/FAs. [13]

El proceso de *handover* entre GGSN/FAs se describe a continuación, suponiendo que se realiza después del *handover* entre dos SGSNs:

A. Después de haberse efectuado un *handover* SGSN, el SGSN tiene la posibilidad de cambiar el GGSN/FA basándose en el conocimiento de los GGSN/FAs que se encuentran en su dominio. Si decide no cambiar de GGSN/FA, el contexto PDP y el GGSN/FA original son mantenidos de manera normal, de otra manera, si decide realizar el *handover,* el proceso que se realiza es el siguiente:

a) El nuevo SGSN envía una Petición de Creación del Contexto PDP al nuevo GGSN/FA con la información que el Contexto PDP es un Contexto IP Móvil. La información del tipo de contexto es puesta en el campo APN como se describió anteriormente en el Proceso de Activación del Contexto PDP, en los pasos 2 y 3.

b) El nuevo GGSN/FA envía una Respuesta de Creación del Contexto PDP tal como se explica en el paso 4 de la Activación del Contexto PDP.

B. Después de una creación exitosa del nuevo Contexto PDP se puede activar un timer, el cual se encarga de contar el tiempo hasta que el antiguo Contexto PDP se elimina, permitiendo a los datagramas que arriban al antiguo GGSN/FA ser redirigidos al equipo del usuario. El timer puede colocarse en cero para señalar la ausencia de un timer, por lo que el

Contexto PDP del antiguo GGSN/FA es eliminado inmediatamente después de haber sido creado el nuevo Contexto PDP.

c) El nuevo SGSN envía una Petición de Eliminación del Contexto PDP al antiguo GGSN/FA.

d) El antiguo GGSN/FA elimina el Contexto PDP y envía una Respuesta de Eliminación del Contexto PDP al SGSN.

e) El FA envía al equipo de usuario un Anuncio de Agente como se explica en el paso 7 del proceso de Activación del Contexto PDP.

f) Se realiza el registro IP Móvil como se explica en los pasos 8 al 11 del proceso de Activación del Contexto PDP.

Nota:

En el caso de que ocurra una falla en el registro IP Móvil, por ejemplo, que el nuevo FA no soporte un servicio requerido por la MS, o que el HA niegue la petición de registro, el GGSN/FA podrá reaccionar y tomar decisiones. El FA sabe la severidad de la falla y realizará una acción dependiendo de esto. Si la falla no es severa y la MS puede tratar un nuevo registro, el FA podrá decidir esperar. De otra manera, si la falla es severa el GGSN/FA que reporto la falla puede causar la eliminación del Contexto PDP comunicándole la decisión al SGSN. Este responderá al GGSN/FA confirmando la eliminación del contexto y determinará (dependiendo de la información de la falla recibida del GGSN/FA) la posibilidad de registrarse nuevamente con el antiguo GGSN/FA. Si detecta que esto es posible y que el Contexto PDP está aun abierto, éste será reutilizado y el timer que lo borra será parado. Por lo tanto el tráfico se enrutará a través del antiguo contexto PDP al antiguo GGSN/FA. Si no es posible reutilizarlo, se eliminará el Contexto PDP del antiguo GGSN/FA mediante la comunicación entre el SGSN y éste, comunicándoselo posteriormente a la MS.

1.2 *ROAMING* GGSN/FA (RED GPRS) - FA (RED WLAN)

Este proceso es necesario para que la MS mantega una sesión activa mientras realiza un cambio de acceso desde la red GPRS a la red WLAN. En la figura D.3 se ilustra el proceso de *roaming* entre la red GPRS y la red WLAN.

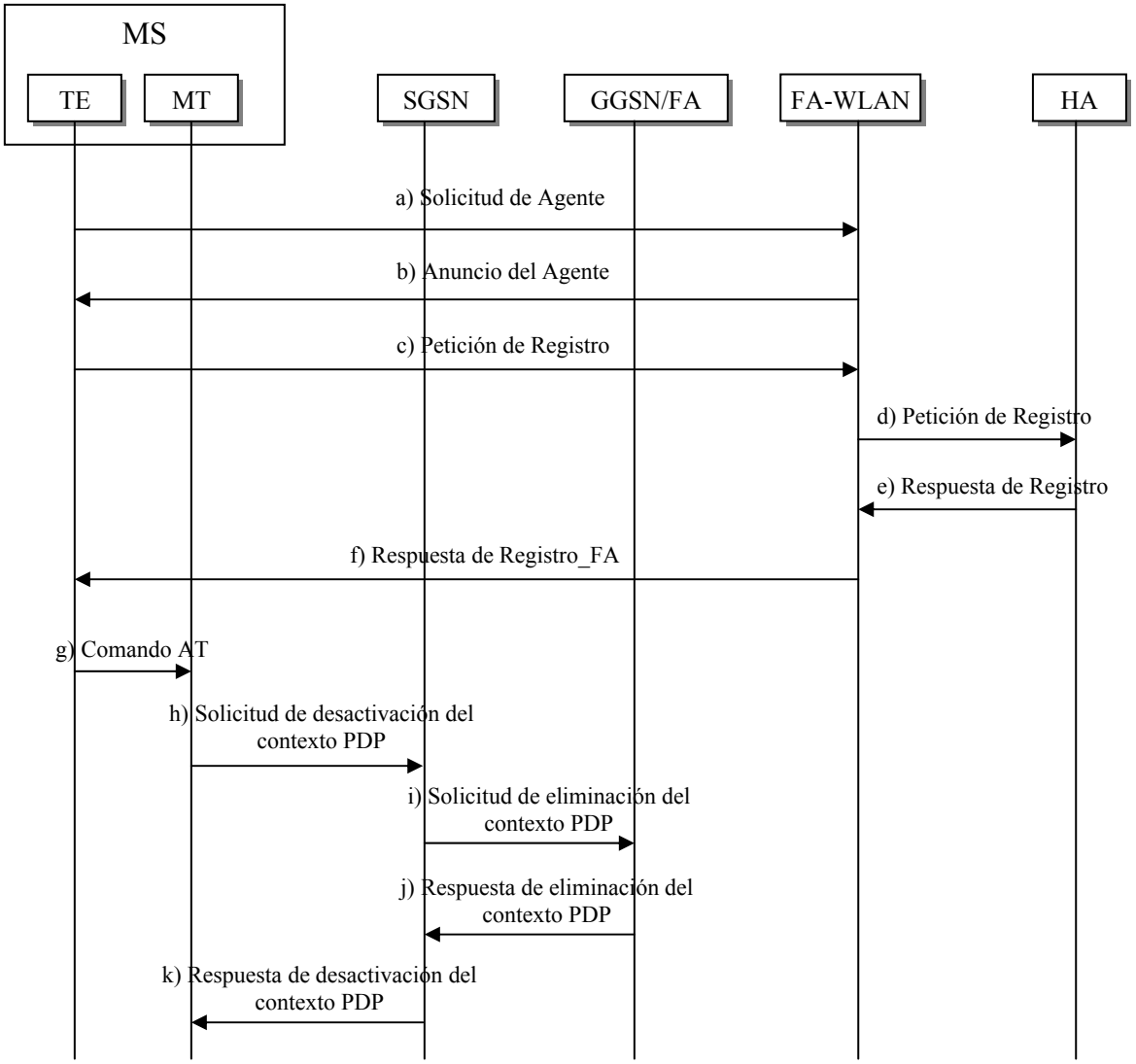

Figura D.3. Proceso de *roaming* red GPRS – WLAN

En este escenario la MS se encuentra asociada a la red GPRS, recibiendo datos a través de ella hasta que entra en el área de cobertura de una red WLAN. En ese momento se origina el procedimiento de *roaming* entre las dos redes.

a) Una vez la MS (TE) detecta un buen nivel de señal proveniente de una WLAN, realiza una solicitud de anuncio de agente de ese segmento de red. Esta es idéntica a una solicitud de enrutador ICMP y evita que la MS (TE) tenga que esperar hasta el próximo anuncio de agente.

b) El FA envía un mensaje de anuncio ICMP, de igual forma a como se describe en el paso 7 del Proceso de Activación del Contexto PDP, pero esta vez a través de un Punto de Acceso WLAN.

c) Las MS (TE) envía una petición de registro, entre cuyos parámetros mas importantes se incluye la dirección *care-of* deseada, la dirección IP de su HA, y la dirección IP que tiene asignada localmente. La petición de registro se hace a través del FA ya que la MS (TE) va a utilizar una de sus direcciones *care-of.*

d) El FA hace un reenvío hacia el HA de la petición de registro proveniente de la MS (TE).

e) El HA actualiza sus tablas de configuración y registro teniendo en cuenta la dirección IP del FA y la dirección *care-of* asignada a la MS. Luego envía una respuesta a la MS (TE) confirmando o rechazando la operación de registro.

f) El FA hace un reenvío de la respuesta de registro proveniente del HA.

g) El TE le indica al MT que se ha asociado al segmento WLAN.

h) La MS (MT) inicia la desactivación del contexto PDP lo que permite que se liberen los recursos utilizados de la red GPRS en esa conexión para que puedan ser reutilizados por otra MS.

i) La GGSN/FA elimina el registro de la MS de su lista de direcciones care-of /TEID correspondiente a la conexión establecida previamente.

j) **k)** Mensajes de confirmación de la eliminación del contexto PDP.

Una vez realizado este proceso, el usuario puede continuar con la sesión recibiendo y transmitiendo datos a través de la WLAN.

Nota:

En caso de que la MS (TE) reciba un anuncio de Agente perteneciente a su HA, no requiere de enviar solicitudes de registro IP Móvil ya que se encuentra en su área local, pero de igual forma, realiza el proceso de eliminación de registro de la red GPRS.

Cuando la MS (TE) detecta un nivel de señal bajo proveniente de la red WLAN, solicita que se active un contexto PDP en la red GPRS para que le sea posible registrarse con la GGSN/FA y pueda continuar con la sesión de transferencia de datos activa.

2. *ROAMING* CDMA2000 – WLAN A TRAVÉS DE IP MÓVIL

Con el fin de iniciar una sesión de paquetes de datos en la red CDMA2000, el usuario necesita autenticarse primero para permitírsele el acceso a la red y luego para que le sean asignados los diferentes recursos y pueda utilizar los servicios de paquetes de datos.

En la figura D.4 se detalla el proceso de registro y autenticación de una estación móvil en la red CDMA2000 iniciando una sesión de paquetes de datos basada en IP Móvil. Se muestra el proceso de autenticación del usuario tanto en el servidor AAA foráneo (perteneciente a la red CDMA2000) como en el servidor AAA local (perteneciente a la red WLAN a la cual pertenece el usuario).

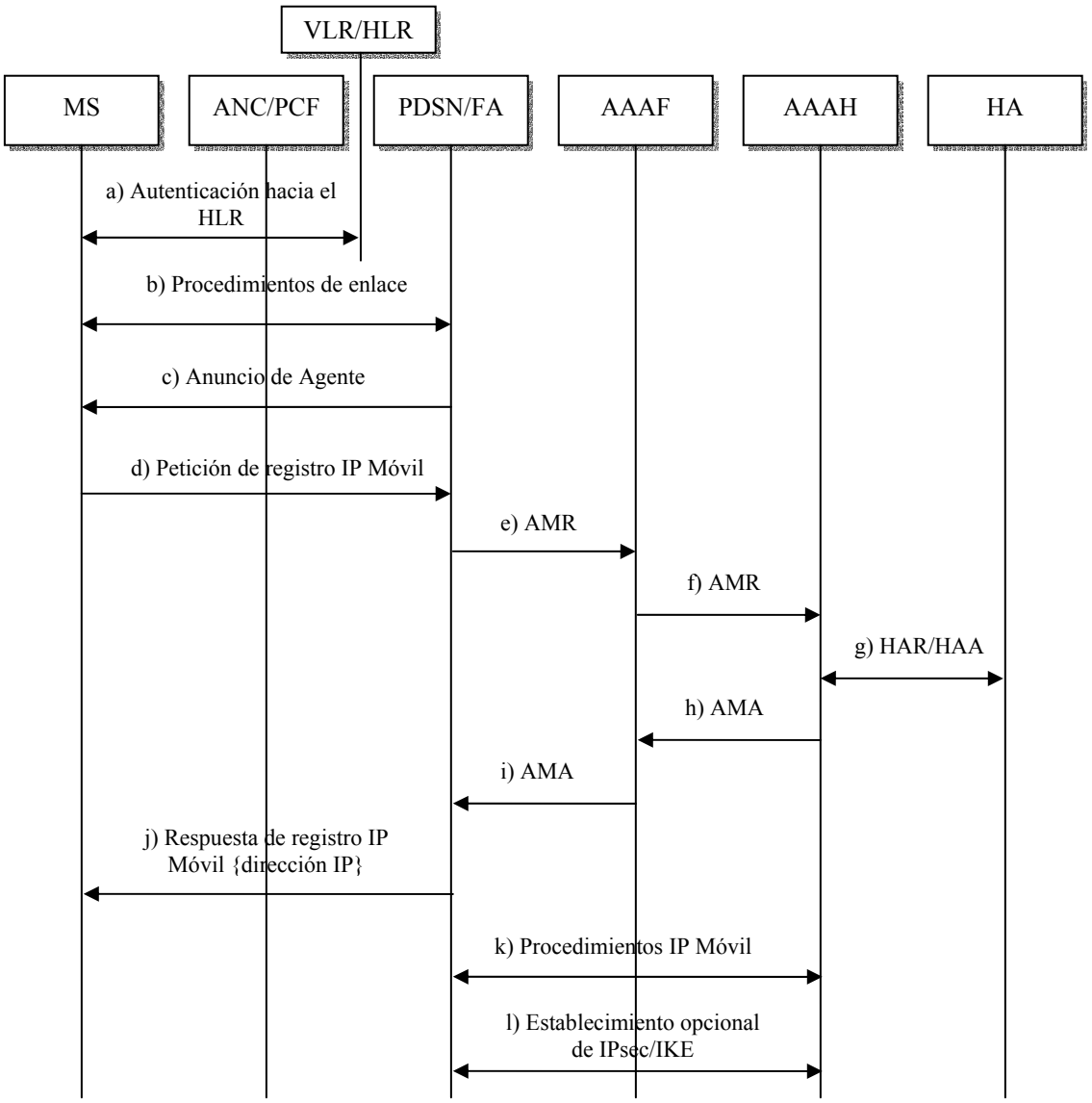

Figura D.4. Proceso de AAA CDMA2000 con registro IP Móvil. [14]

a) La MS entra a la red de acceso y se registra utilizando los procedimientos específicos de esta red. En la red CDMA2000 este procedimiento incluye autenticación con el HLR, siendo independiente de la utilización de IP Simple o IP Móvil. La MS inicia la sesión enviando un mensaje de origen que incluye una indicación de que ésta es una sesión de paquetes de datos. La MS se autentica hacia el HLR comunicándose a través de la red de acceso radio con el MSC, el cual se encarga de realizar un procedimiento de autenticación similar al proceso de autenticación de circuitos conmutados, para luego asignársele a la MS recursos de radio y establecer inicialmente un canal dedicado de baja tasa de datos.

b) La MS inicia la sesión de paquetes de datos enviando una indicación al PDSN/FA para inicializarla. Antes de comunicarse con el PDSN/FA, se le asignan los recursos en la interfaz de radio paquetes a través del ANC/PCF, para luego a través de éstos inicializar la conexión PPP con el PDSN.

Antes de que se complete la conexión PPP, la MS se debe autenticar con el servidor AAA para permitírsele utilizar los servicios de Internet y realizar el registro IP Móvil en la conexión PPP.

c) El PDSN/FA envía un Anuncio de Agente a la MS. La MS puede enviar un mensaje de solicitud de agente al PDSN/FA según este configurado el servicio en la red.

d) La MS genera una petición de Registro IP Móvil conteniendo entre otros parámetros el NAI (Network Access Identifier).

e) El Agente Foráneo crea el mensaje de Petición AAA del Nodo Móvil (AMR – AAA Mobile Node Request) y lo dirige hacia el servidor AAA Foráneo (AAAF – Foreign AAA).

f) El AAAF utiliza el NAI en el AMR que recibe para dirigir el mensaje al servidor AAA Local (AAAH – Home AAA) indicado. El mensaje puede entregarse utilizando seguridad AAA entre la red local y la red foránea.

g) EL AAAH recibe el AMR. Si el AAAH está programado para asignar un HA y la dirección del Agente Local se conoce, el AAAH envía una Petición MIP de agente local (HAR – Home Agent MIP Request), la cual contiene el mensaje de Petición de Registro IP Móvil para el Home Agent Requerido o Asignado. Adicionalmente el AAAH puede asignar la Dirección IP Local al nodo móvil. En éste caso la dirección IP Local se incluirá en el HAR. Si el AAAH no ha asignado una dirección IP local al nodo móvil, esta responsabilidad de asignación se la deja al Agente Local. El HA procesa la +petición de registro MIP e incluye una respuesta de registro MIP en la Respuesta de Agente Local (HAA – Homa Agent Answer) para finalmente enviarla al AAAH.

h) El AAAH dirige la Respuesta de AAA del nodo Móvil (AMA - AAA Mobile Node Answer) al AAAF que puede entregarse utilizando seguridad AAA entre la red local y la red foránea.

i) El AAAF redirige la AMA al PDSN/FA.

j) El PDSN FA envía la respuesta de registro IP móvil a la MS que indica que puede realizar el registro y le asigna, si no le ha sido asignada, la dirección IP local que viene en la respuesta del HA.

k) Se inician los procedimientos de registro IP Móvil.

l) Opcionalmente el PDSN/FA puede crear una asociación IPsec hacia el HA utilizando IKE. Esto puede involucrar tanto una clave IKE pre-compartida entregada por la respuesta de autorización AAA como por intercambio certificado con IKE.

La operación específica IP Móvil puede empezar.

2.1 *HANDOVER* ENTRE PDSN/FAs

Durante una sesión activa en la red CDMA2000 se puede dar el caso en que la estación móvil cambie de red de acceso (AN – Access Network) debido su ubicación, generando de esta manera un cambio de PDSN/FA por la configuración de la red. En la figura D.5 se ilustra el proceso de *handover* entre PDSN/FAs.

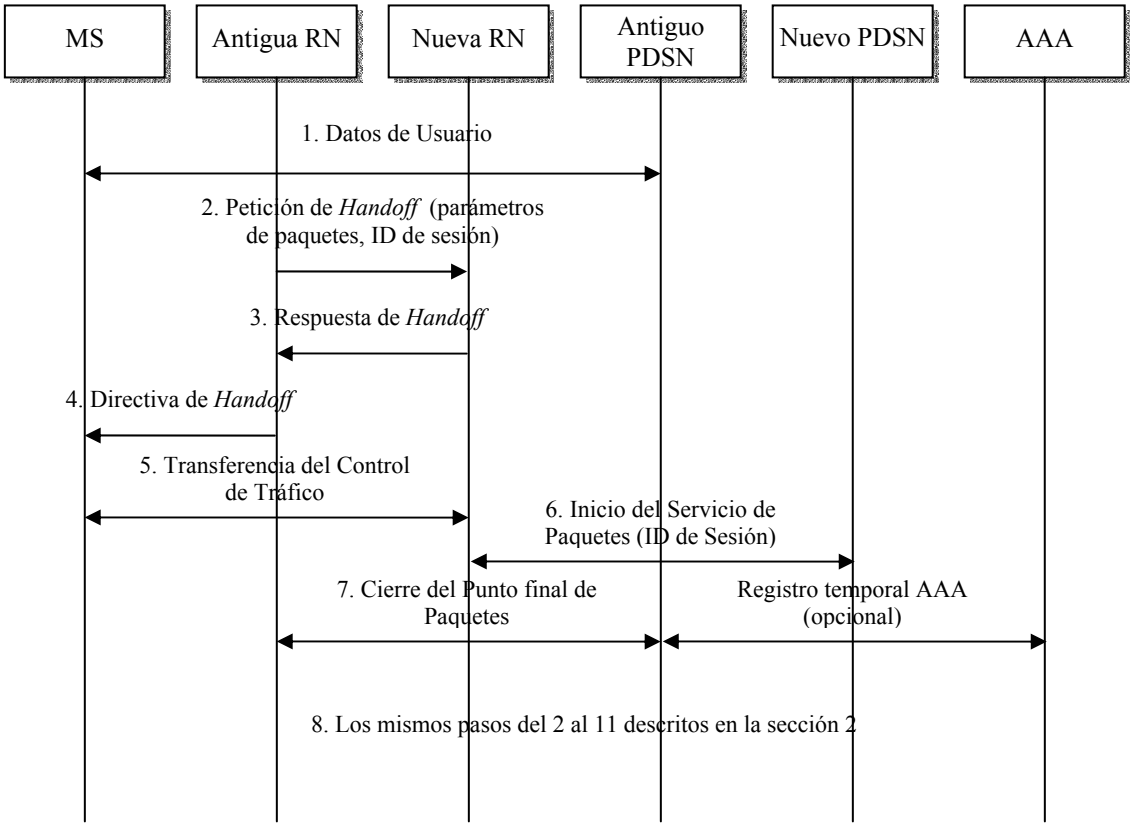

Figura D.5. *Handover* entre PDSN/FAs utilizando IP Móvil. [15]

1. El flujo de datos se encuentra activo utilizando una sesión PPP entre la estación móvil y el servidor PDSN actual en ese momento (denotado en la figura como antiguo PDSN).

2. En algún punto el sistema de radio decide que se requiere un *handoff* – el Control de Radio Recursos (RRC - Radio Resource Control) debe cambiar. La Red Radio activa en ese momento (denotada en la figura como antigua RN – Radio Network) envía una petición a la Red Radio objetivo (denotada en la figura como nueva RN). Los parámetros de los paquetes, incluyendo el identificador de sesión, pasan a la nueva RN para facilitar el *handoff* de los datos de paquetes. Esta información es retransmitida entre RNs utilizando los procedimientos de *handoff* existentes.

3. La nueva RN decide permitir el *handoff* y envía una respuesta a la antigua RN a través de los procedimientos existentes en el VLR.

4. La antigua RN notifica a la MS para realizar el *handoff* a la nueva RN.

5. El canal de tráfico se transfiere a la nueva RN.

6. La nueva RN notifica al nuevo PDSN para establecer un servicio de paquetes. El ID de la sesión se envía al nuevo PDSN, con el fin de el PDSN se de cuenta que éste es un nuevo enlace RN-PDSN (no existe el enlace).

7. Después que el *handoff* se ha completado, la antigua RN notifica al antiguo PDSN que el punto final del túnel para la estación móvil con éste RN es cerrado. Un registro de Facturación Temporal AAA puede enviarse opcionalmente al servidor AAA.

8. El flujo que continúa es el mismo que en la sección 2, pasos del 2 al 11 en donde se establece la sesión PPP con el PDSN y se realiza el registro y activación IP Móvil de la MS con el HA.

2.2 *ROAMING* PDSN/FA (RED CDMA2000) - FA (RED WLAN)

Este proceso es necesario para que la MS mantega una sesión activa mientras realiza un cambio de acceso desde la red CDMA2000 a la red WLAN. En la figura D.6 se ilustra el proceso de *roaming* entre la red CDMA2000 y la red WLAN.

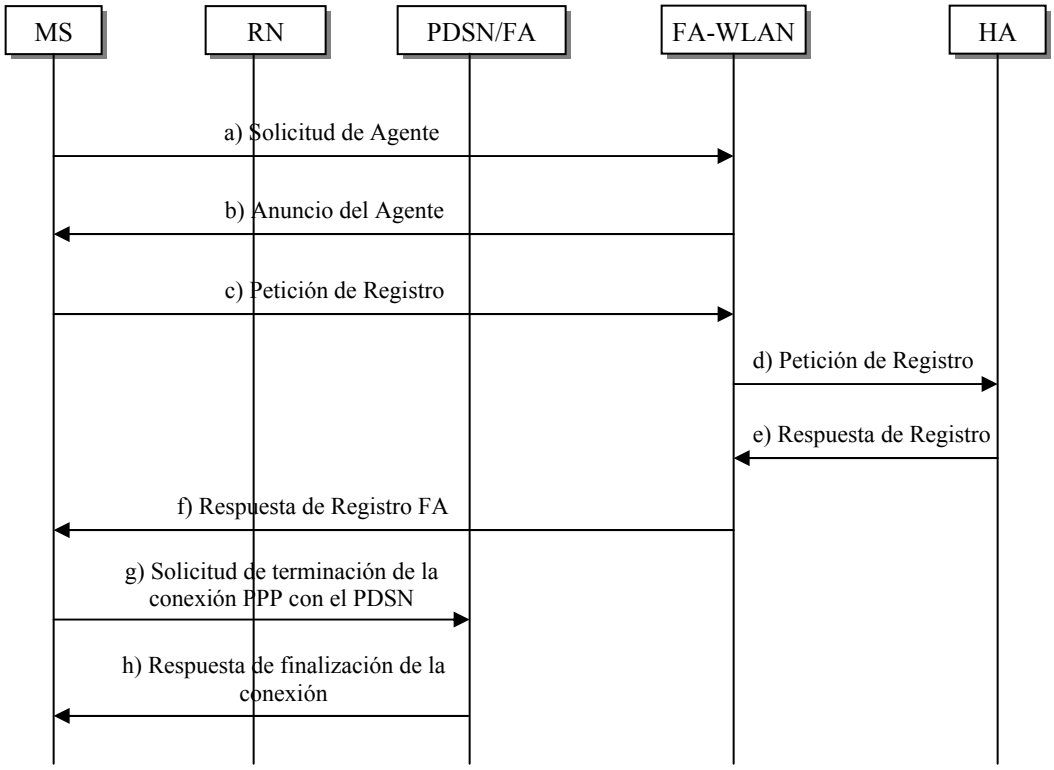

Figura D.6. Proceso de *roaming* red GPRS – WLAN

En este escenario la MS se encuentra asociada a la red CDMA2000, recibiendo datos a través de ella hasta que entra en el área de cobertura de una red WLAN. En ese momento se origina el procedimiento de *roaming* entre las dos redes.

a) Una vez la MS (TE) detecta un buen nivel de señal proveniente de una WLAN, realiza una solicitud de anuncio de agente de ese segmento de red. Esta es idéntica a una solicitud de enrutador ICMP y evita que la MS (TE) tenga que esperar hasta el próximo anuncio de agente.

b) El FA envía un mensaje de anuncio ICMP a través de un Punto de Acceso WLAN con una extensión de anuncio de agente de movilidad, el cual contiene parámetros que la MS necesita, entre los cuales están una o más direcciones *care-of* que el FA ofrece.

c) Las MS (TE) envía una petición de registro, entre cuyos parámetros más importantes se incluye la dirección *care-of* deseada, la dirección IP de su HA, y la dirección IP que tiene asignada localmente. La petición de registro se hace a través del FA ya que la MS (TE) va a utilizar una de sus direcciones *care-of.*

d) El FA hace un reenvío hacia el HA de la petición de registro proveniente de la MS (TE).

e) El HA actualiza sus tablas de configuración y registro teniendo en cuenta la dirección IP del FA y la dirección *care-of* asignada a la MS. Luego envía una respuesta a la MS (TE) confirmando o rechazando la operación de registro.

f) El FA hace un reenvío de la respuesta de registro proveniente del HA hacia la MS.

g) La MS (MT) inicia la desactivación de la sesión PPP con la PDSN enviándole un mensaje a través de la RN de la red CDMA2000 con el fin de liberar los recursos utilizados en la red celular para que puedan ser reutilizados por otra MS.

h) La PDSN envía una respuesta de finalización de la conexión.

Una vez realizado este proceso, el usuario puede continuar con la sesión recibiendo y transmitiendo datos a través de la WLAN.

Nota:

En caso de que la MS (TE) reciba un anuncio de Agente perteneciente a su HA, no requiere de enviar solicitudes de registro IP Móvil ya que se encuentra en su área local, pero de igual forma, realiza el proceso de terminación de sesión con la CDMA2000.

Cuando la MS (TE) detecta un nivel de señal bajo proveniente de la red WLAN, solicita que se active un contexto PDP en la red GPRS para que le sea posible registrarse con la GGSN/FA y pueda continuar con la sesión de transferencia de datos activa.

ANEXO E. FORMATO ENCUESTAS ENVIADAS A OPERADORES COLOMBIANOS

Todas las encuestas tuvieron la misma introducción, y el formato de las preguntas se realizó de acuerdo a la tecnología que cada empresa del sector maneja. Avaya y Links, tecnologías WiFi; Comcel y Ola, tecnología de red basada en GSM/GPRS; Movistar, tecnología de red basada en CDMA2000.

Las encuestas fueron enviadas a través de correo electrónico el día 18 de Agosto de 2005 a los profesionales del sector: Ingeniero Marcelo Gómez, Links S.A.; Ingeniero Tulio E. Sandoval Rivas, Telefónica Móviles S.A.; Ingeniero Hernán Felipe Cucalón Merchán, Telefónica Móviles S.A.; Ingeniero Ricardo Pérez, Colombia Móvil S.A. E.S.P.; y se contacto vía telefónica al Ingeniero Edilberto Carreño, Avantel S.A., al cual no se le pudo enviar el correo debido a dificultades en su localización en el momento del diligenciamiento, además, se envió un correo a través del Ingeniero en Electrónica y Telecomunicaciones Pedro Andrade, egresado de la Universidad del Cauca, a un profesional de Comcel S.A. Esta encuesta fue enviada junto con una carta de presentación del proyecto firmada por el Decano de la Facultad de Ingeniería Electrónica, Ingeniero Rafael Rengifo Prado.

Solo se recibió respuesta de la encuesta enviada al Ingeniero Marcelo Gómez, la cual fue diligenciada por el Ingeniero Gonzalo LLano R., Gerente Regional de Links S.A. a través de correo electrónico el día 24 de Agosto de 2005.

A continuación se muestra el formato de encuesta enviado independientemente a cada profesional, dependiendo de la tecnología manejada en la empresa donde labora actualmente.

- **AVAYA, LINKS S.A.**

La presente encuesta forma parte del mecanismo de obtención de datos para el trabajo de grado: “Caracterización del Roaming entre la Red Móvil Celular y la Red Inalámbrica de Área Local con Aplicación al Entorno Colombiano”, y su objetivo es servir de base para establecer ciertas condiciones que definen al entorno colombiano con respecto a las redes de servicio móvil e inalámbricas y el de conocer cuales son las perspectivas que los operadores del sector tienen frente a la implementación de una tecnología que permite el roaming de terminales entre estas redes.

1. **¿En la empresa donde labora actualmente, qué estándares 802.11 están utilizando?**
    a) 802.11a
    b) 802.11b
    c) 802.11g
    d) Otro, ¿Cuál?:

2. **¿Cuáles protocolos mencionados, se utilizan para enlaces punto - multipunto y cuales para enlaces punto - punto?**
    a) Enlaces punto - multipunto:
    b) Enlaces punto - punto:

3. **¿Qué esquemas de seguridad están empleando actualmente para protección de la información y autenticación de los clientes?**

4. **¿Qué servicios se ofrecen sobre las redes Wi-Fi que tienen implementadas actualmente?**

5. **¿Qué otros servicios piensan implementar sobre estas redes?**

6. **¿De que fabricantes son los equipos que usualmente utilizan?**

7. **¿Se han planteado la utilización de tecnologías de una generación posterior como por ejemplo WIMAX?**
    a) Si
    b) No
    ¿Por qué?:
    Si la respuesta es si, ¿sería a corto, mediano o largo plazo?:

8. **¿Considera que la tecnología WIMAX podría sustituir la tecnología Wi-Fi?**
    c) Si
    d) No
    ¿Por qué?:
    Si la respuesta es si, ¿sería a corto, mediano o largo plazo?:

9. **¿En la empresa donde labora actualmente, se ha considerado la implementación del *roaming* de terminales entre las redes Wi-Fi y las redes celulares para sesiones de voz y/o datos?**
    a) Si
    b) No
    ¿Por qué?:

10. **¿Considera que la ínter-operabilidad de estas dos tecnologías a través del proceso de *roaming* favorecería y ampliaría el mercado tanto para operadores inalámbricos como celulares?**
    a) Si

b) No
¿Por qué?:

11. **¿Cuentan actualmente con estudios propios acerca de la implementación del *roaming* entre las redes Wi-Fi y las redes celulares?**
    a) Si
    b) No

12. **Si la respuesta a la anterior pregunta es no, ¿sería importante que el sector contara con un estudio para la consecución del *roaming* entre estas dos redes heterogéneas?**
    a) Si
    b) No
    ¿Por qué?:

- **MOVISTAR**

1. **¿En la empresa donde labora actualmente, se presta algún servicio a través de la tecnología Wi-Fi?**
    a) Si
    b) No

   Si la respuesta es no, ¿se tiene planeado a corto, mediano o largo plazo utilizar esta tecnología?:

2. **¿Si se presta servicio a través de Wi-Fi que protocolos se utilizan para la transmisión de información?**
    a) 802.11a
    b) 802.11b
    c) 802.11g
    d) Otro, ¿Cuál?:

3. **¿Considera que en la empresa donde labora actualmente, existen las capacidades suficientes en el núcleo de la red móvil celular para asumir sin inconvenientes el tráfico generado por una red Wi-Fi?**
    a) Si
    b) No

4. **¿Cree que resultaría conveniente prestar servicios de VoIP sobre la red Wi-Fi?**
    a) Si
    b) No
    ¿Por qué?:

5. **¿En la empresa donde labora actualmente, se ha considerado la implementación del *roaming* de terminales entre la red móvil celular y redes Wi-Fi para sesiones de voz y/o datos?**
   a) Si
   b) No
   ¿Por qué?:

6. **¿Considera que la ínter-operabilidad de estas dos tecnologías a través del proceso de *roaming* favorecería y ampliaría el mercado tanto para operadores celulares como inalámbricos?**
   a) Si
   b) No
   ¿Por qué?:

7. **¿Considerando la implementación del *roaming* de terminales entre la red móvil celular y la red Wi-Fi, resultaría mas conveniente instalar puntos de acceso propios o establecer convenios con operadores Wi-Fi y utilizar los puntos de acceso ya existentes?**
   a) Si
   b) No
   ¿Por qué?:

8. **¿En la empresa donde labora actualmente, se piensa continuar con la evolución de la red CDMA2000 o se centrarán en evolucionar la red GSM?**
   a) Si
   b) No
   ¿Por qué?:

9. **¿En la empresa donde labora, a través de que tecnologías están prestando servicios de datos actualmente?**
   a) CSD (Circuit Switched Data)
   b) HSCSD (High Speed Circuit Switched Data)
   c) SMS (Short Message Service)
   d) GPRS (General Packet Radio Service)
   e) EDGE (Enhanced Data Rates for GSM and TDMA Evolution)
   f) Otra, ¿Cuál?:

10. **¿En la empresa donde labora actualmente, se encuentran soportados servicios sobre IP Móvil en el núcleo de red CDMA2000?**
    a) Si
    b) No
    Si la respuesta es no, ¿se planea prestar servicios soportados sobre IP Móvil?:

11. **¿En la empresa donde labora, cuentan actualmente con estudios propios acerca de la implementación del *roaming* entre la red móvil celular y las redes WiFi?**
    a) Si
    b) No

12. **Si la respuesta a la anterior pregunta es no, ¿sería importante que el sector contara con un estudio para la consecución del *roaming* entre estas dos redes heterogéneas?**
    a) Si
    b) No
    ¿Por qué?:

- **COMCEL, OLA**

1. **¿En la empresa donde labora actualmente, a través de que tecnologías están prestando servicios de datos actualmente?**
    a) CSD (Circuit Switched Data)
    b) HSCSD (High Speed Circuit Switched Data)
    c) SMS (Short Message Service)
    d) GPRS (General Packet Radio Service)
    e) EDGE (Enhanced Data Rates for GSM and TDMA Evolution)
    f) Otra. ¿Cuál?:

2. **¿En la empresa donde labora actualmente, se presta algún servicio a través de la tecnología Wi-Fi?**
    a) Si
    b) No
    Si la respuesta es no, ¿se tiene planeado a corto, mediano o largo plazo utilizar esta tecnología?:

3. **¿Si se presta servicio a través de Wi-Fi que protocolos se utilizan para la transmisión de información?**
    a) 802.11a
    b) 802.11b
    c) 802.11g
    d) Otro. ¿Cuál?:

4. **¿En la empresa donde labora actualmente, se ha considerado la implementación del *roaming* de terminales entre la red móvil celular y redes Wi-Fi para sesiones de voz y/o datos?**
    a) Si
    b) No
    ¿Por qué?:

5. **¿Considera que la ínter-operabilidad de estas dos tecnologías a través del proceso de *roaming* favorecería y ampliaría el mercado tanto para operadores celulares como inalámbricos?**
    a) Si
    b) No
    ¿Por qué?:

6. **¿Considerando la implementación del *roaming* de terminales entre la red móvil celular y la red Wi-Fi, resultaría mas conveniente instalar puntos de acceso propios o establecer convenios con operadores Wi-Fi y utilizar los puntos de acceso ya existentes?**
    a) Si
    b) No
    ¿Por qué?:

7. **¿Considera que en la empresa donde labora actualmente, existen las capacidades suficientes en el núcleo de la red móvil celular para asumir sin inconvenientes el trafico generado por una red Wi-Fi?**
    a) Si
    b) No

8. **¿Considera que es conveniente prestar servicios de VoIP sobre la red Wi-Fi?**
    a) Si
    b) No
    ¿Por qué?:

9. **¿Cuentan actualmente con estudios propios acerca de la implementación del *roaming* entre la red móvil celular y las redes WiFi?**
    a) Si
    b) No

10. **Si la respuesta a la anterior pregunta es no, ¿sería importante que el sector contara con un estudio para la consecución del *roaming* entre estas dos redes heterogéneas?**
    a) Si
    b) No
    ¿Por qué?:

ANEXO F. TENDENCIAS DEL MERCADO DE TELECOMUNICACIONES COLOMBIANO

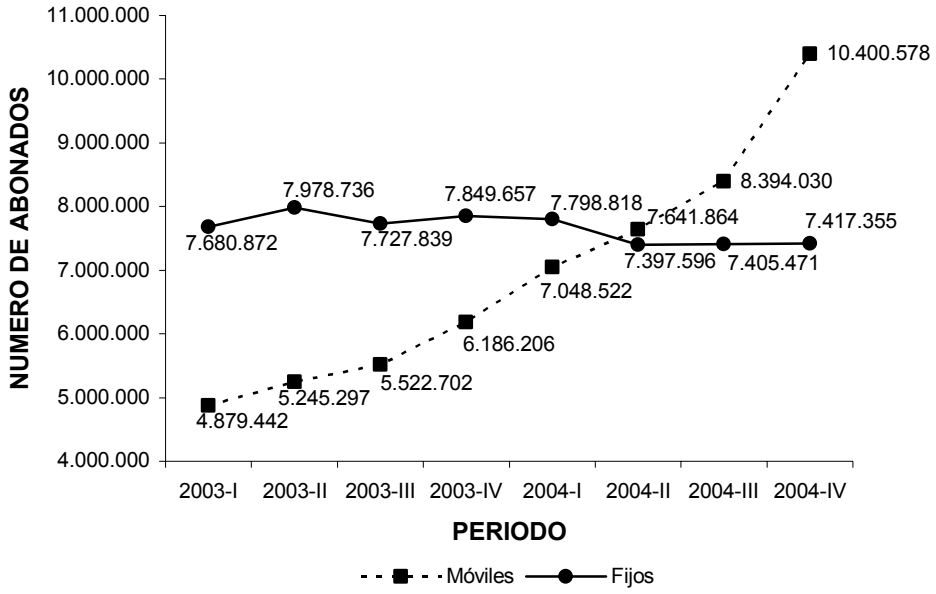

Figura F.1. Evolución trimestral del número total de Abonados Fijos y Móviles en Colombia. [16]

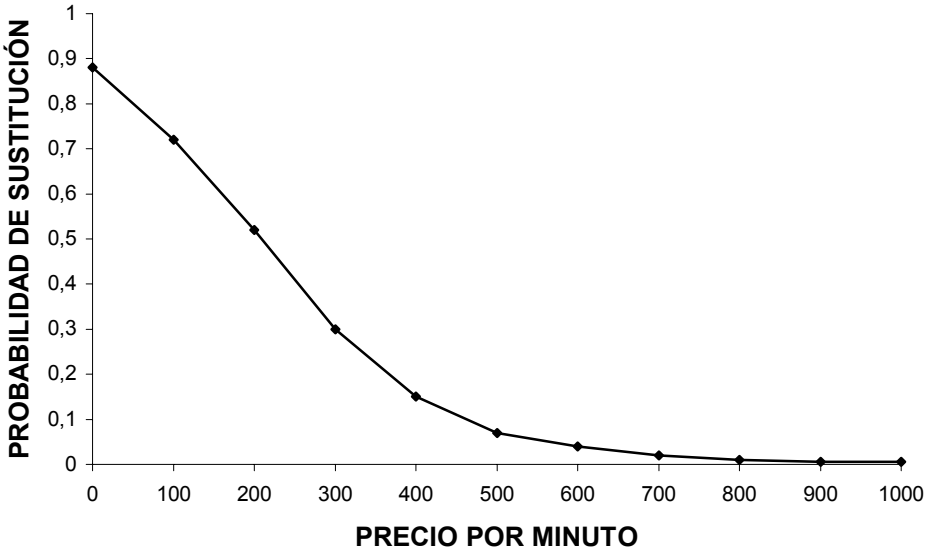

Figura F.2. Probabilidad de sustitución de fijo a celular a en el hogar de acuerdo al precio por minuto celular. [17]

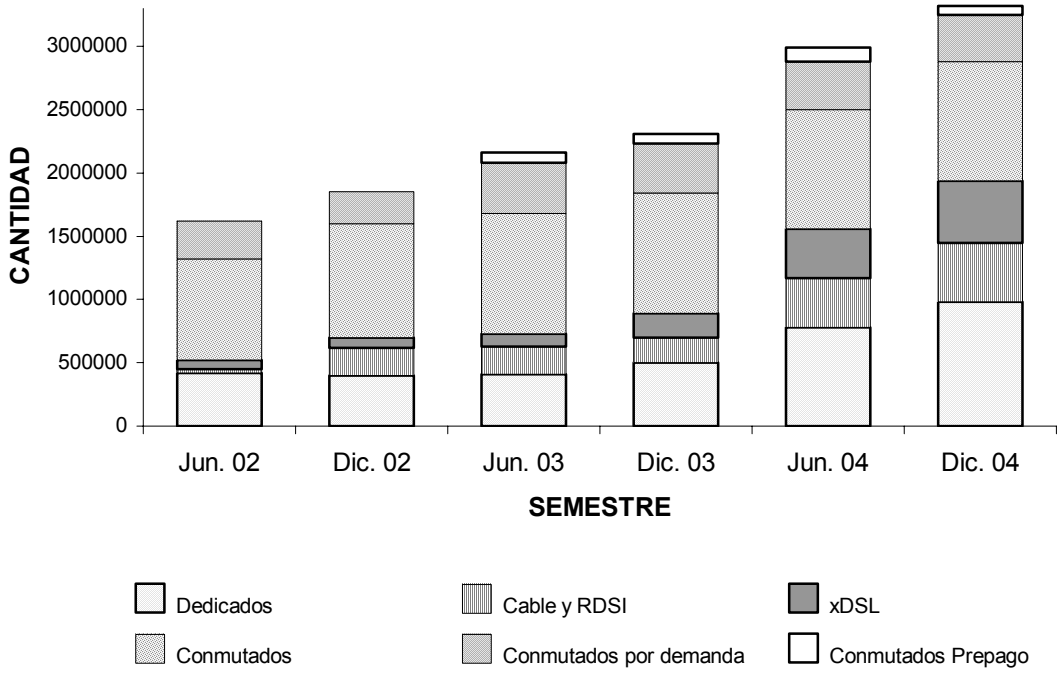

Figura F.3. Evolución de usuarios de Internet por medio de acceso [18]

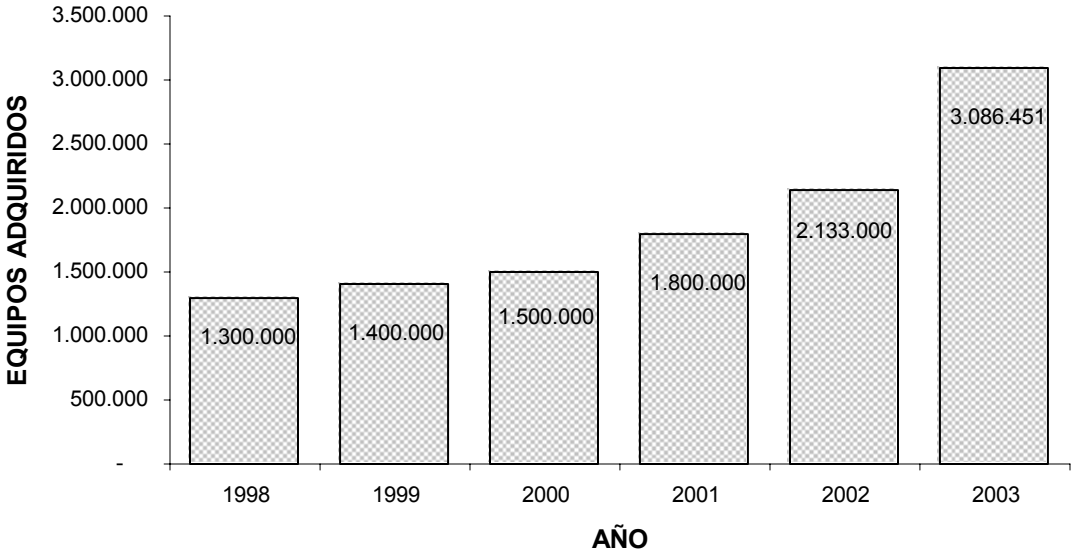

Figura F.4. Evolución de computadores personales adquiridos en Colombia. [17]

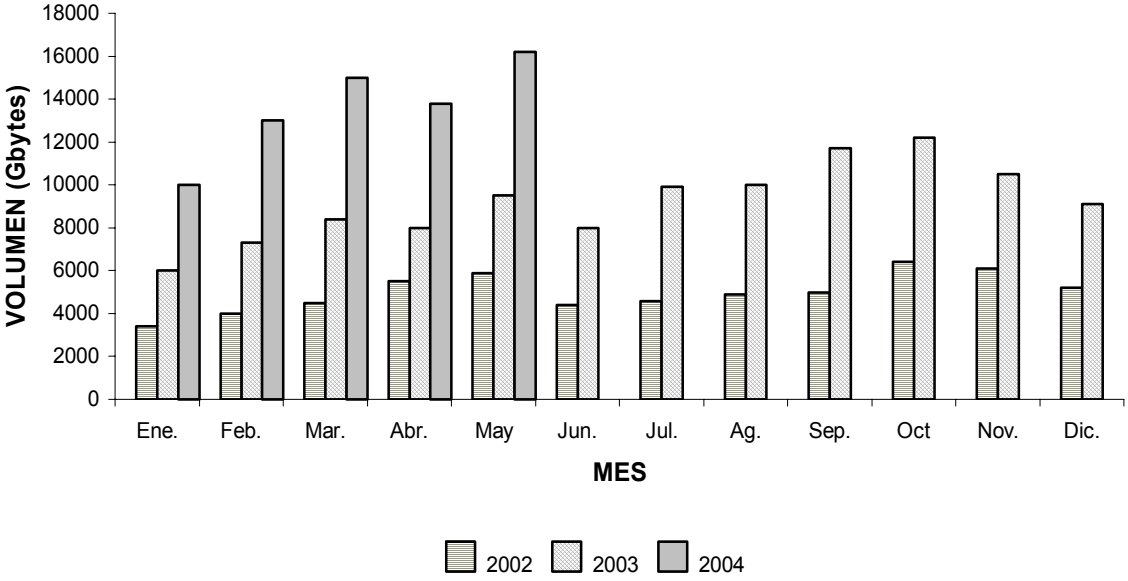

Figura F.5. Evolución del trafico NAP[7] en Colombia

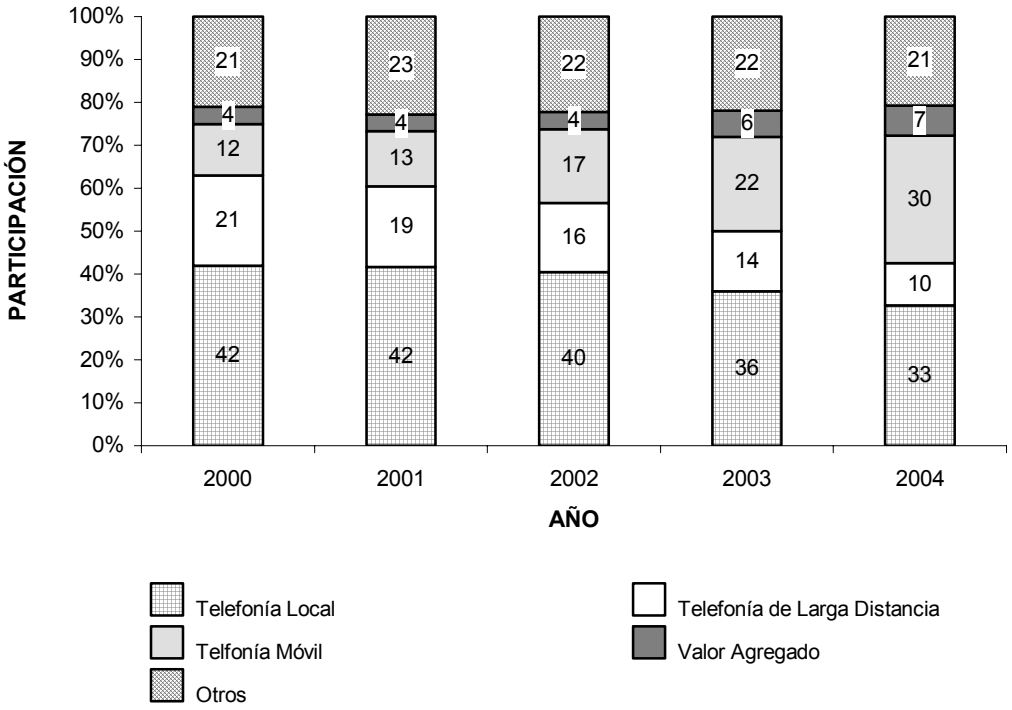

Figura F.6. Participación Ingresos del sector de Telecomunicaciones en Millones de Pesos [17]

[7] NAP es un punto de conexión nacional de las redes de las empresas que proveen el servicio de acceso de Internet en Colombia, con el cual se logra que el tráfico de Internet que tiene origen y destino en nuestro país, utilice solamente canales locales o nacionales. En línea: www.nap.com.co.

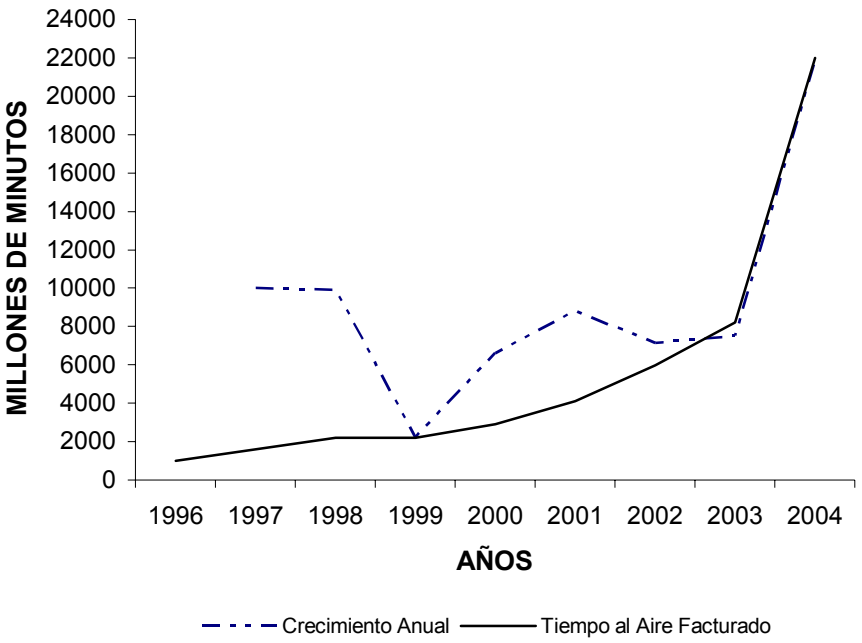

Figura F.7. Evolución del tráfico en servicios móviles (Celular y PCS). [16]

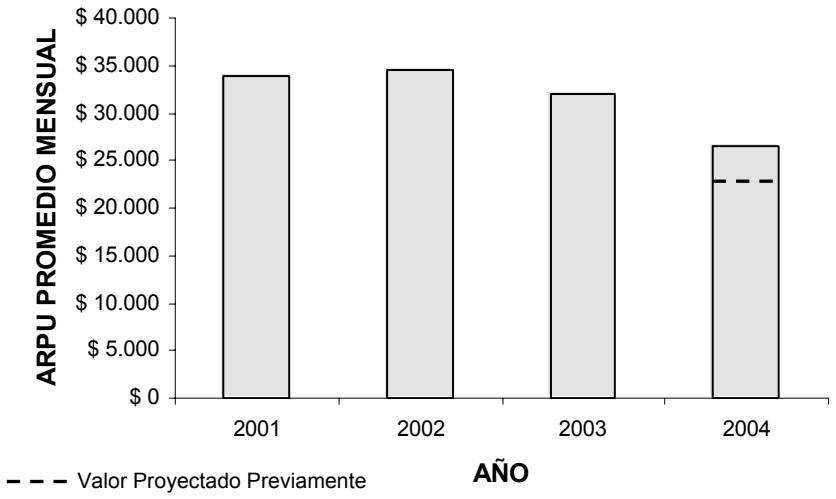

Figura F.8. ARPU mensual promedio para los operadores de telefonía móvil. [17]

ANEXO G. EXPERIENCIAS

1. OMNICON

En este proyecto se implementan demonios de Comunicación (CD – Communication Deamons) en el Nodo Móvil y en el Agente Foráneo GPRS, que permiten establecer una conexión TCP sobre el enlace GPRS y que interactúan con el modulo de decisión en el nodo móvil para poder establecer el momento en que se debe realizar el proceso de *roaming*.

La figura G.1 muestra el diagrama de Gant del *roaming* IP Móvil de WLAN a GPRS y GPRS a WLAN. Para lograr que el *roaming* se realice en forma exitosa, es decir sin que la sesión iniciada por el usuario se vea afectada, el modulo de decisión debe prever el posible cambio de tecnología de acceso de manera anticipada por medio de la medición periódica de la potencia de la señal. El punto de inicio en el diagrama corresponde al momento en que el módulo de decisión notifica al CD para iniciar el proceso de *roaming*. En el *roaming* WLAN a GPRS, el CD del FA de la red GPRS libera un anuncio de FA con 2 milisegundos de tiempo de notificación. IP Móvil responde a este anuncio invalidando el anuncio de agente previo y enviando una petición de registro después de 2 milisegundos. El FA GPRS responde con una respuesta de registro después de aproximadamente 800 a 1100 milisegundos, intervalo de tiempo que corresponde al tiempo de ida y vuelta en el enlace GPRS.

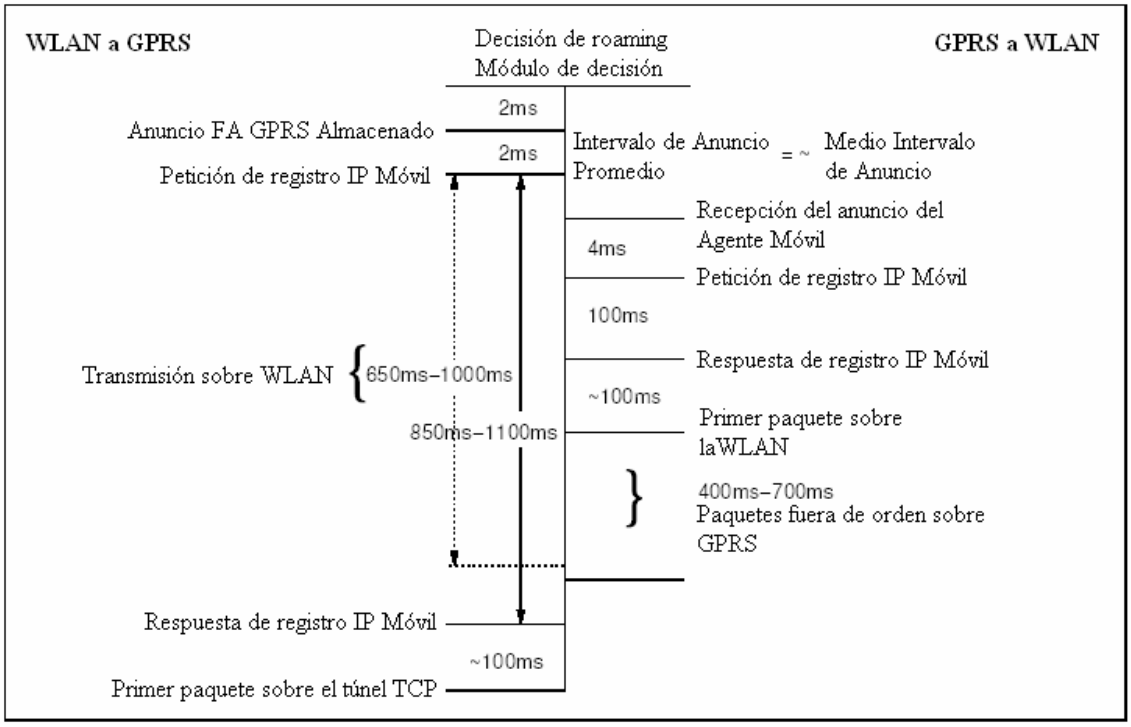

Figura G.1. Diagrama de Gant del proceso de *roaming* de la red WLAN a la GPRS, y de la red GPRS a la WLAN. [19]

El *roaming* de la red GPRS a la WLAN es relativamente mas corto en términos de duración que el de la red WLAN a la GPRS, ya que su intervalo de duración es inferior a los 250 milisegundos, después, se recibe un anuncio desde el agente móvil. Ya que esta duración es más corta que la latencia en el enlace GPRS (800 a 1100 milisegundos), el nodo móvil continúa recibiendo algunos paquetes fuera de orden a través del enlace GPRS por una duración de aproximadamente 400 a 700 milisegundos que corresponden a la latencia del enlace. Si la notificación del modulo de decisión es bien anticipada, no hay perdida de paquetes durante en *roaming.*

Si la conexión con la red WLAN se deteriora antes de que el módulo de decisión pueda anticipar el *roaming,* existe pérdida de paquetes durante este proceso, lo cual se puede evitar almacenando en buffer previamente los paquetes enviados. La figura G.2 muestra el comportamiento de la perdida de paquetes para el tráfico de subida durante el proceso de *roaming,* cuando se deshabilita el almacenamiento de paquetes en el buffer del nodo móvil. Cuando el tráfico de subida se envía con una tasa máxima de datos posible de 8 Kbps con un tamaño de los paquetes mínimo posible de 64 bytes, el número de paquetes perdidos es 36. La pérdida decrece con el decrecimiento de la tasa de datos y el incremento del tamaño de los paquetes, por lo que para esta situación en particular por ejemplo, una maquina virtual en el nodo móvil necesita almacenar al menos 36 paquetes para eliminar completamente la perdida de datos para el tráfico de

subida en el caso de que ocurra un *roaming* no anticipado por el modulo de decisión.

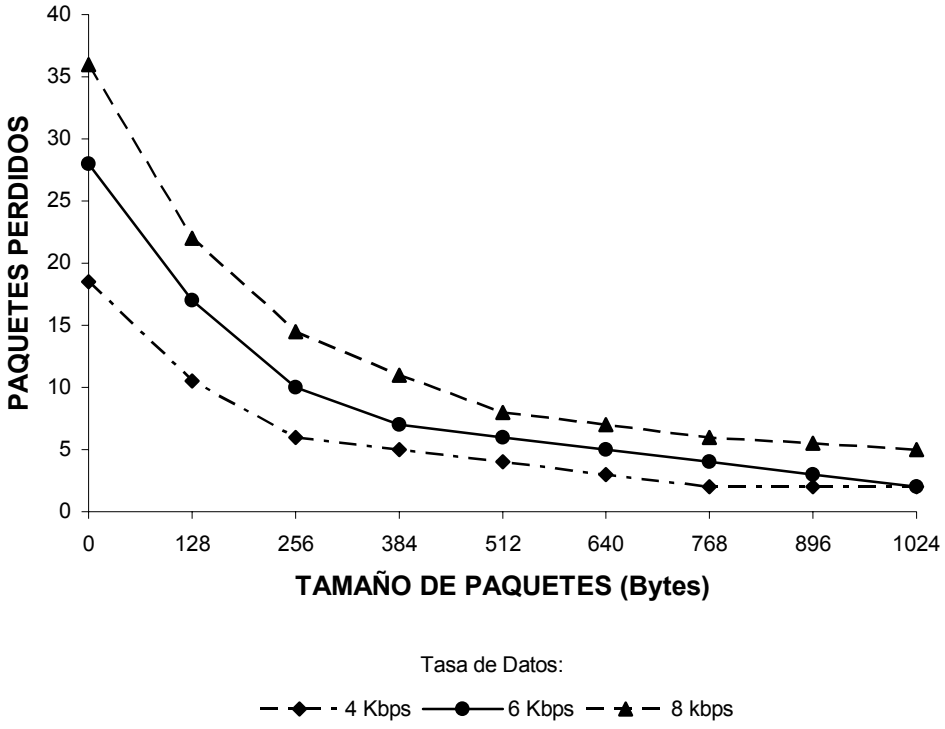

Figura G.2. Perdida de paquetes en el tráfico de subida cuando no hay almacenamiento en buffer en el nodo móvil. [19]

Los datos enviados sobre el enlace GPRS se entunelan a través de una conexión TCP, disminuyendo el *througput* de los mismos debido a los encabezados adicionales y a los reconocimientos enviados en el enlace. La figura G.3 muestra el *overhead* que se presenta en la transmisión con paquetes de diversos tamaños, teniendo en cuenta una variación en la carga del enlace. En caso de que el enlace no esté saturado, los paquetes pequeños de 64 bytes generan cerca de un 120% de *overhead*, debido a que cada paquete se envía separadamente y un ACK TCP debe ser enviado de vuelta sobre el mismo enlace. Cuando el enlace se satura, múltiples paquetes pequeños se combinan en una única transmisión TCP y el *overhead* se reduce. Para paquetes de 64 bytes, éste se reduce a un 27% y para paquetes más grandes éste es relativamente inmejorable. La diferencia entre el porcentaje de *overhead* a velocidades de un enlace saturado y uno no saturado, se reduce con el incremento en el tamaño de los paquetes, ya que hay menos oportunidades de combinar múltiples paquetes en una única transmisión.

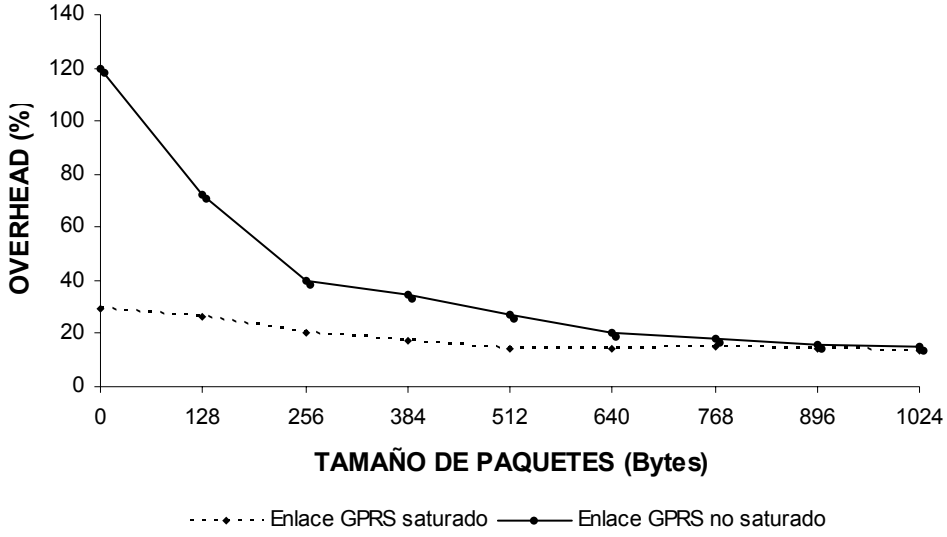

Figura G.3. Overhead ocasionado debido a los encabezados TCP adicionales y a los ACKs. [19]

2. ROTUAARI

La escala que manejan los usuarios en el proyecto Rotuaari, con el fin de brindar la información de acuerdo a la calidad del servicio recibido, se muestra en la tabla G.1.

CALIFICACIÓN	EXPLICACIÓN
6	Excelente: "El servicio trabaja impecablemente."
5	Bueno: "El servicio trabaja bien, yo note únicamente pocas deficiencias."
4	Estuvo bien: "El servicio trabajo lo suficientemente bien considerando el propósito de utilización."
3	Algo malo: "La operación del servicio fue un poco molesta, pero yo usaría el servicio de todas formas."
2	Insatisfactorio: "Yo usaría el servicio solo si fuera absolutamente necesario."
1	Inutilizable: "Yo no podría utilizar el servicio en absoluto."

Tabla G.1. Escala de la evaluación subjetiva de la calidad de la aplicación. [20]

En el estudio que se realizó sobre este proyecto se configuró el cliente para que la WLAN poseyera mayor prioridad que la red GPRS y para que el *roaming* de la WLAN hacia la red

GPRS ocurriera si la potencia de la señal del enlace caía por debajo del 20% para evitar el efecto de “ping-pong” con la reselección de la red de acceso. Para ser reasociado a la WLAN el nivel debía ser superior al 40% de la señal máxima.

Durante la evaluación se obtuvieron datos objetivos capturando el tráfico de usuario en la MS con software de cliente Ethereal y Segco MIP con el objeto de registrar tanto las duraciones de descargas de contenido que el usuario experimentaba, como los tiempos y cantidades de tráfico transferido cuando se utilizaron conexiones PPP (enlaces a través de la red GPRS). De esta forma, se mapearon datos objetivos con evaluaciones subjetivas proporcionadas por los usuarios. Los datos obtenidos por Ethereal y Segco fueron suficientes para especificar cual red de acceso se utilizó en un determinado tiempo, aunque no precisaron medidas del proceso de *roaming*, como por ejemplo, la duración de los tiempos de desconexión o perdidas de paquetes. De igual forma, y para complementar la información obtenida desde el cliente, en el servidor se almacenó información completa acerca de la sesión de usuario, la cual incluyó información de la manera en que los usuarios utilizaban el servicio.

Se debe tener en cuenta que antes de realizar la evaluación, los usuarios fueron informados que usarían distintas redes de acceso durante la misma, pero cuando la evaluación estuvo en curso, no se les proporciono ninguna información acerca de cual tecnología de acceso se encontraban utilizando en ese preciso momento, de manera que todo el proceso de transporte y *roaming* entre las redes fue transparente a ellos.

En esta evaluación, el 35% de los usuarios reportaron que no se notan cambios en la calidad del servicio, el 40% notaron que la calidad cambió una vez, y el 25% notaron de dos a tres cambios en la calidad del servicio. Únicamente el 30% de los usuarios mencionaron que notaron un claro mejoramiento en la calidad del servicio, principalmente en la descarga de video. El 65% de los usuarios no notaron que su ubicación tuvo algún efecto en la calidad del servicio. La cantidad de *roamings* por sesión de usuario se presenta en la figura G.4.

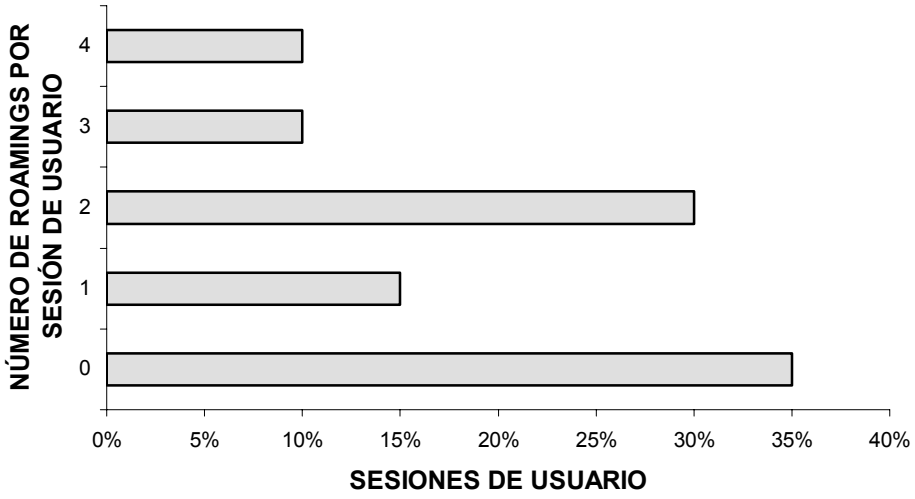

Figura G.4. Cantidad de *roamings* por sesión de usuario. [20]

La duración de las conexiones WLAN intermedias variaron entre 33 segundos a 5 minutos y 56 segundos, incluyendo los retardos por el *roaming* en ambas direcciones, mientras que la duración de las conexiones GPRS intermedias variaron de 8 segundos a 7 minutos y 18 segundos.

Después de las pruebas, se solicitó a los usuarios evaluar el grado de variación de QoS experimentado en una escala del 1 al 7, donde 1 corresponde a cambios apenas perceptibles y 7 a cambios extremadamente altos. Los resultados obtenidos se presentan en la figura G.5.

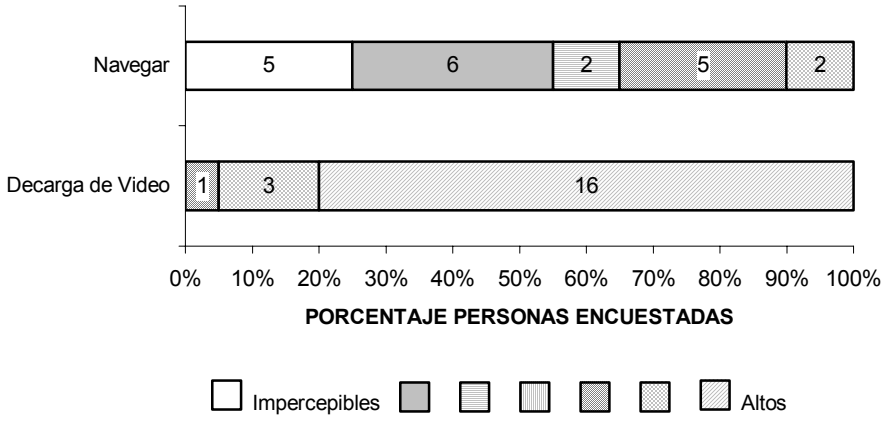

Figura G.5. Grado de variación de QoS experimentado en distintos servicios. [20]

De forma similar, a los usuarios se les solicitó evaluar cuan aceptable fue la variación de QoS experimentada durante las pruebas. Estos resultados se muestran en la figura G.6.

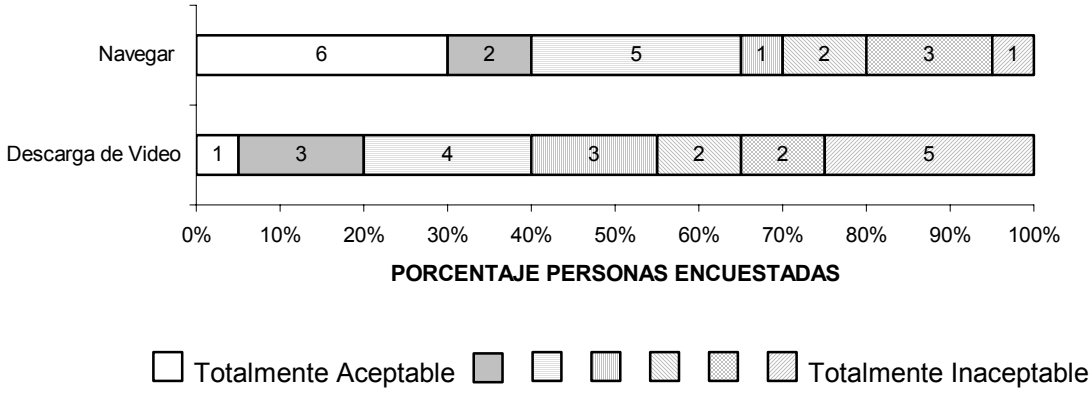

Figura G.6. Aceptabilidad de las variaciones de QoS experimentada. [20]

Hay una variación considerable en los resultados obtenidos. El 25% de los usuarios observaron que la operación básica del servicio, incluyendo la descarga de pequeños archivos multimedia (texto e imágenes) trabajaba impecablemente, mientras que con las descargas de video algunas variaciones se toleraron considerando el tamaño de los archivos. De otra manera, el 45% de los usuarios opinaron que la descarga de grandes archivos de una forma práctica, como los videos proporcionados, requeriría que la tecnología de acceso utilizada fuera capaz de entregar el servicio en un tiempo razonable, por lo tanto, en el caso de pequeños archivos de video, no se debería demorar más de unos pocos minutos.

De las respuestas de los usuarios se observa que algunas bajas en la velocidad de operación pueden tolerarse si el servicio opera con normalidad. Sin embargo, si la calidad del servicio se degrada algunas veces a un nivel donde la operación del servicio es apenas satisfactoria, existe la posibilidad de que se afecte el comportamiento futuro de los usuarios frente al servicio.

Una vez realizadas las pruebas, se les proporcionó a los usuarios una corta descripción de las características de las redes WLAN y GPRS, y se les solicitó responder unas pocas preguntas relacionadas con el acceso múltiple basándose en la descripción dada y en lo que experimentaron durante las pruebas. Los resultados obtenidos se muestran el la figura G.7.

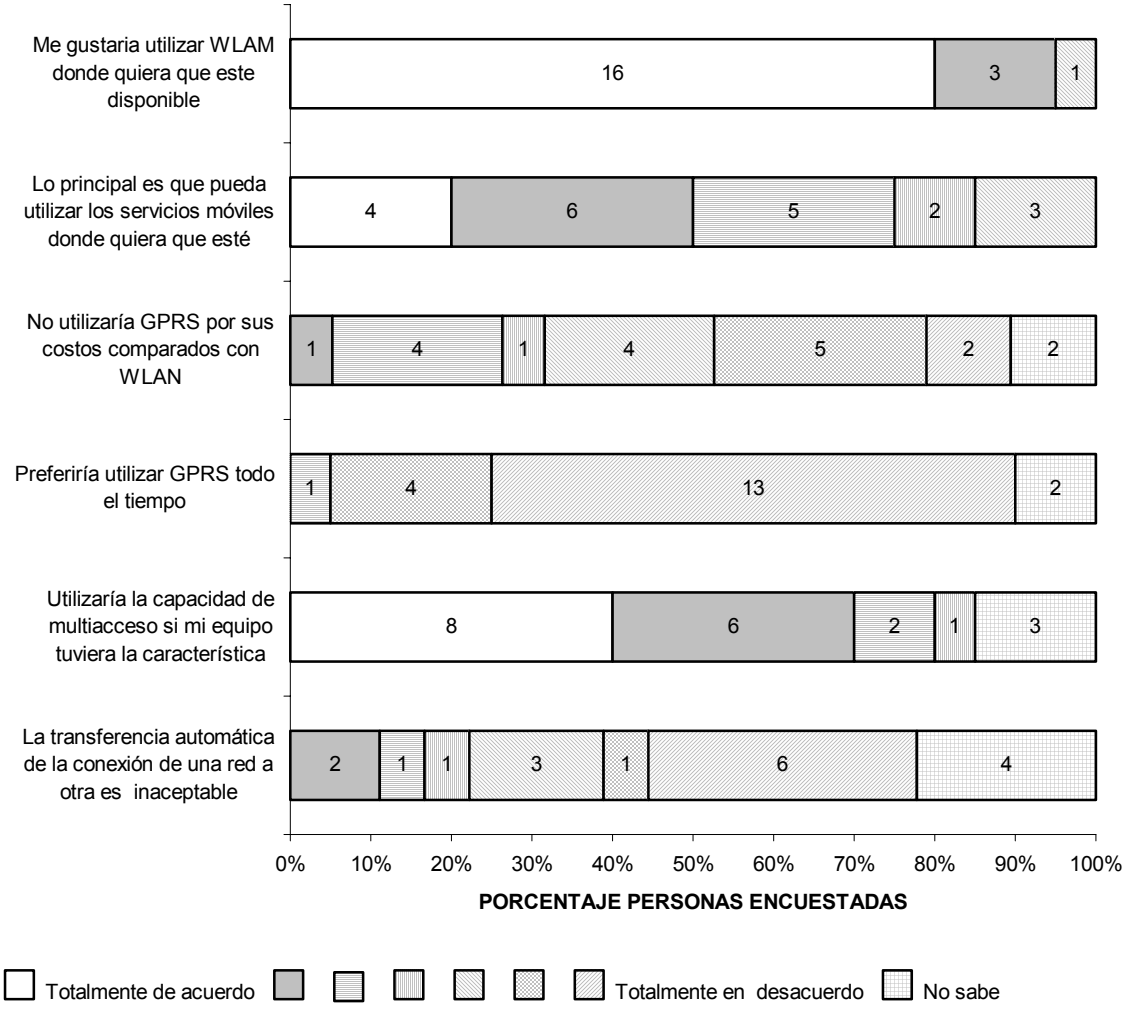

Figura G.7. Opinión de los usuarios acerca de la red de múltiple acceso. [20]

Adicionalmente se consultó a los usuarios su opinión acerca de como debería ser la selección de la red de acceso y el *roaming* desde su punto de vista. El 90% de los usuarios preferiría un control automático del *roaming* a un control manual, con un 67% de estos usuarios esperando una notificación o alguna otra solución que les permita darse cuenta cual red de acceso están utilizando en cualquier tiempo dado.

ANEXO H. EQUIPOS Y PRODUCTOS

1. TARJETAS DUALES

En la tabla H.1 se listan algunas de las tarjetas duales (manejan estándares celulares y WLAN) de importantes fabricantes del sector.

TARJETA	ESTÁNDARES SOPORTADOS	BANDAS DE FRECUENCIA (Mhz)	VEL. MAX. REDES CEL. (Kbps)	SISTEMAS OPERATIVOS SOPRTADOS
Nokia D311	GPRS, GSM (Datos), IEEE 802.11b	GSM 850/1900	GPRS – 40.2 GSM – 14.4	Windows 98, SE, ME, 2000, XP y CE 3.0 (Pocket PC/2002, Handhled PC 2000)
Nokia D211	GPRS, EGSM (HSCSD), IEEE 802.11b	EGSM 900/1800	GPRS – 40.2 HSCSD – 43.2	Windows 98, SE, ME, 2000, XP y CE 3.0 (Pocket PC/2002, Handhled PC 2000), Linux
Sony Ericsson GC79	GPRS, HSCSD, IEEE 802.11b	GSM 900/1800/1900	No disponible	Windows 98 SE, ME, 2000, XP
Sony Ericsson GC89	GSM EDGE/GPRS, IEEE 802.11b, IEEE 802.11g	GSM EDGE/GPRS 850/900/1800/ 1900	EDGE/GPRS 247 (Downlink) 123 (Uplink)	Windows 98 SE, ME, 2000, XP, MAC OS X
OPTION GlobeTrotter FUSION	UMTS, GPRS/GSM, IEEE 802.11b, IEEE 802.11g	UMTS 2100 GSM 900/1800	UMTS 384 DL/64 UL GPRS/GSM 85.6 DL/42.8 UL	Windows 2000, XP, Linux, MAC OS
OPTION GlobeTrotter COMBO EDGE PCMCIA	EDGE, GPRS/GSM, IEEE 802.11b, IEEE 802.11g	GSM 850, EGSM 900, DCS 1800, PCS 1900	EDGE – 236.8 GPRS/GSM – 85.6	Windows 2000, XP Home/XP Pro
OPTION GlobeTrotter COMBO PCMCIA	GPRS/GSM, IEEE 802.11b	EGSM 900, GSM 1800, PCS 1900	53.6	Windows 98SE, ME, 2000, XP
Benq Multi function PC Card	GPRS, IEEE 802.11b	900/1800/1900	85.6 DL 42.8 UL	No disponible

Swisscom Mobile Unlimited EDGE/GPRS/ WLAN	GSM, GPRS, EDGE, IEEE 802.11b, IEEE 802.11g	GSM/GPRS/ EDGE 850/900/1800/ 1900	No disponible	Windows 2000, XP
Swisscom Mobile Unlimited UMTS/GPRS/W LAN	UMTS, GPRS/GSM, IEEE 802.11b, IEEE 802.11g	GSM/GPRS 900/1800 UMTS 2100	No disponible	Windows 2000, XP

Tabla H.1. Tarjetas duales

Para más información acerca de cada una de las tarjetas duales, puede ingresar a los siguientes enlaces en Internet:

- *Nokia D311:*
  http://www.nokia.com/nokia/0,8764,2022,00.html
- *Nokia D211:*
  http://www.nokia.com/nokia/0,8764,1450,00.html
- *Sony Ericsson GC79:*
  http://www.sonyericsson.com/spg.jsp?cc=global&lc=en&ver=4001&template=pp5_1&zone=pp&lm=pp5_1&pid=10057
- *Sony Ericsson GC89:*
  http://www.sonyericsson.com/spg.jsp?cc=global&lc=en&ver=4001&template=pp5_1&zone=pp&lm=pp5_1&pid=10225
- *OPTION GlobeTrotter FUSION:*
  http://www.option.be/products/gt_fusion_spec.shtml
- *OPTION GlobeTrotter COMBO EDGE PCMCIA:*
  http://www.option.be/products/edge_spec.shtml
- *OPTION GlobeTrotter COMBO PCMCIA:*
  http://www.option.be/products/2_3_1_specifications.shtml
- *Benq Multi function PC Card:*
  http://www.expansys.com/product.asp?code=111328&partner=register
- *Swisscom Mobile Unlimited EDGE/GPRS/WLAN:*
  http://www.swisscom.com/onlineshop/productdetails.aspx?cat=41000_Mobilfunkkarten&sub=41100_Mobile+Unlimited&opn=O&sku=000000000000109516&lang=en-GB&sendingPageType=products
- *Swisscom Mobile Unlimited UMTS/GPRS/WLAN:*
  http://www.swisscom.com/onlineshop/productdetails.aspx?cat=41000_Mobilfunkkarten&sub=41100_Mobile+Unlimited&sku=000000000000103303&lang=en-GB&ct=1

2. DISPOSITIVOS MÓVILES DUALES (PDAs, POCKET PC Y TELÉFONOS MÓVILES)

En la tabla H.2 se listan algunos de los dispositivos móviles duales (manejan estándares celulares y WLAN) de importantes fabricantes del sector.

DISPOSITIVO	ESTÁNDARES SOPORTADOS	BANDAS DE FRECUENCIA (Mhz)	VEL. MAX. REDES CEL. (Kbps)	SISTEMAS OPERATIVOS SOPRTADOS
HP iPAQ h6315 Pocket PC – Phone Edition	GPRS/GSM, IEEE 802.11b, Bluetooth	GSM 850, 900,1800,1900	No disponible	Windows Mobile 2003 (Premium with Phone Edition)
HP iPAQ h6320 Pocket PC – Phone Edition	GPRS/GSM, IEEE 802.11b, Bluetooth	GSM 850, 900,1800,1900	No disponible	Windows Mobile 2003 (Premium with Phone Edition)
HP iPAQ h6325 Pocket PC – Phone Edition	GPRS/GSM, IEEE 802.11b	GSM 850, 900,1800,1900	No disponible	Windows Mobile 2003 (Premium with Phone Edition)
i-mate JASJAR PDA	UMTS, GPRS, GSM, IEEE 802.11b	GSM 900/1800/1900 UMTS 2100	No disponible	Windows Mobile 2005 Phone Edition
Nokia 9500 Communicator	EDGE, GPRS, IEEE 802.11b	GSM 1800/1900	EDGE – 236.8 GPRS – 53.6	Symbian 7.0S OS
Samsung SCH-i730	CDMA2000 EVDO, IEEE 802.11b	CDMA 800/1900	No disponible	Windows Mobile 2003 Pocket PC
MOTOROLA CN620	GPRS/GSM, 802.11a	GSM 850,1900	No disponible	Windows CE .NET 4.2
MOTOROLA MPx100	GPRS/GSM, IEEE 802.11b	GSM 900/1800/1900	No disponible	Windows Mobile 2003

Tabla H.2. Equipos Duales

Para más información acerca de cada una de los equipos móviles duales, puede ingresar a los siguientes enlaces en Internet:

- *HP iPAQ h6315 Pocket PC – Phone Edition:* http://h10010.www1.hp.com/wwpc/us/en/sm/WF06b/215348-64929-215381-314903-f60-430120-430121-405360.html
- *HP iPAQ h6320 Pocket PC – Phone Edition:* http://h10010.www1.hp.com/wwpc/us/en/sm/WF06b/215348-64929-215381-314903-f60-430120-451971-468915.html

- *HP iPAQ h6325 Pocket PC – Phone Edition:* http://h10010.www1.hp.com/wwpc/us/en/sm/WF06b/215348-64929-215381-314903-f60-430120-451973-468916.html
- *i-mate JASJAR PDA:* http://www.clubimate.com/t-JASJAR_technical.aspx
- *Nokia 9500 Communicator:* http://www.nokia.com/nokia/0,,54108,00.html
- *Samsung SCH-i730:* http://product.samsung.com/cgi-bin/nabc/product/b2c_product_detail.jsp?eUser=&prod_id=SCH-I730&selTab=Specifications
- *MOTOROLA CN620:* http://www.motorola.com/Enterprise/us/en_us/solution.aspx?navigationpath=id_803i
- *MOTOROLA MPx100:* http://www.motorola.com/mot/doc/1/1055_MotDoc.pdf

3. PRODUCTOS COMERCIALES PARA EL *ROAMING* CELULAR/WLAN

En la tabla H.3 se listan algunas de las soluciones para la implementación del *roaming* entre la red móvil celular y la red WLAN.

PRODUCTO	CARACTERISTICAS PRINCIPALES	SISTEMAS OPERATIVOS SOPORTADOS
Greenpacket SONaccess Unified Mobility	- Roaming a través de redes GPRS, EDGE, CDMA2000 y WLAN basado en IP Móvil - Soporte de VPNs basado en IPSec - Múltiples esquemas de autenticación incluyendo Web y SIM - Soporte de AAA a través de RADIUS, DIAMETER y SS7 - Hardware incluido: Mobile Enterprise Server (MES), Mobile Access Gateway (MAG), Mobile Service Home Agent (MSHA), Mobile Service Foreign Agent (MSFA), Network Management System (SONview) - Software incluido: Mobile IP/Enterprise Client Software (SONmobile)	*Cliente SONmobile*: Windows 2000, XP, Pocket PC 2002, Windows Mobile 2003
Columbitech Wireless VPN	- *Roaming* a través de redes GPRS, CDMA2000 y WLANs basado en IP Móvil, IPSec y en el nivel de sesión utilizando WTLS[8] - Soporte de AAA a través de RADIUS - Software Incluido: Columbitech Wireless VPN Server, Columbitech Gatekeeper, Columbitech	- *Servidor Columbitech Wireless VPN Server:* Windows 2000 Pro, Server, 2003 Server, Wireless Switch, Linux

[8] Seguridad de Nivel de Transporte Inalámbrico (WTLS – Wireless Transport Layer Security)

	Wireless VPN Clients	- *Columb. Gatekeeper:* Windows 2000 Pro, Server - *Cliente Columbitech Wireless VPN Clients:* Windows 2000, XP, Pocket PC 2002, Windows Mobile 2003, Windows CE 3.0, Windows .Net
ipUnplugged Mobile VPN	- *Roaming* a través de redes GPRS, CDMA2000 y WLANs basado en IP Móvil e IPSec - Soporte de AAA a través de RADIUS - Hardware incluido: Roaming Gateway, Roaming Server - Software incluido: Roaming Client	*Cliente ipUnplugged Roaming Client:* Windows 2000, XP, Pocket PC
Motorola UMA Solution	- *Roaming* a través de redes GPRS/GSM, WLAN y Bluetooth basado en el estándar UMA - Ofrece todas las capacidades de AAA con la red GSM/GPRS - Hardware incluido: Motorola UNC (UMA Network Controller), Motorola EMS (Element Management System), Motorola Service Provisioning System - Software incluido: Motorola UMA Client Software	*Cliente Motorola UMA Client Software:* Windows CE .NET 4.2
Kineto UMA Technology	- *Roaming* a través de redes GPRS/GSM y WLANs basado en el estándar UMA - Ofrece todas las capacidades de AAA con la red GSM/GPRS - Hardware incluido: Kineto UNC, Kineto EMS - Software incluido: Kineto UMA Client Software	*Cliente Kineto UMA Client Software:* Microsoft Pocket PC Phone Edition, Plataformas de Philips y Texas Instruments. En desarrollo soporte para Symbian y Linux.

Tabla H.3. Soluciones de *roaming* Celular/WLAN

Para más información acerca de cada una de las soluciones para el *roaming* Celular/WLAN, puede ingresar a los siguientes enlaces en Internet:

- *Greenpacket SONaccess Unified Mobility:* http://www.greenpacket.com/2005/en/solutions/so_03.asp
- *Columbitech Wireless VPN:* http://www.columbitech.com/product_papers/ColumbitechWVPN_Description.pdf
- *ipUnplugged Mobile VPN:* http://www.ipunplugged.com/products.asp?mi=2.3
- *Motorola UMA Solution:* http://www.motorola.com/content/0,,5856-9163,00.html
- *Kineto UMA Technology:* http://www.kinetowireless.com/products/index.html

BIBLIOGRAFÍA

[1] Patil Basavaraj, Saifullah Yousuf, Faccin Stefano, Sreemanthula Srinivas, Aravamudhan Lachu, Sharma Sarvesh, Mononen Risto. “IP in Wireless Networks”. Prentice Hall PTR, Enero 31 2003.

[2] Instituto de Estándares de Telecomunicaciones Europeo. “Digital Cellular Telecomunications System (Phase 2+), General Packet Radio Service – Overall description of the GPRS radio interface GSM 03.64”. Version 6.1.0, Release 97, Octubre 1999.

[3] Muñoz Ante Juan Carlos, Valencia Rojas Diana Maria. “EDGE – Evolución Tecnológica para la Evolución de la Red Móvil Celular de Colombia hacia una Infraestructura de Tercera Generación”. Tesis de Grado, Facultad de Ingeniería Electrónica y Telecomunicaciones, Universidad del Cauca; Popayán 2002.

[4] Fritz Jordan, Wireless LAN Report, Mobile Trax Enterprise IT Research Service, 2003.

[5] WLAN Security Standards
En línea: www.smartaxis.gr/WLAN%20Security%20Standards.doc

[6] Falk Magnus. “Fast and Secure Roaming in WLAN”. Tesis de Grado, Linköping Institute of Technology; Suecia 2004.

[7] En línea:
[http://www.gemplus.com/solutions/telecom/wlan/WLANwhitepaper130303.pdf.]

[8] Joakim Nyström, Mikael Seppälä. “Experimental Study of GPRS/WLAN Systems Integration”. Tesis de Maestria, Linköping Institute of Technology; Suecia 2003.

[9] Internet Draft: draft-salki-pppext-eap-gprs-02.txt

[10] G. Sidebottom, et al. “Signaling System 7 (SS7) Message Transfer Part 3 (MTP3) – User Adaptation Layer (M3UA)”. RFC 3332.
En línea:http://www.ietf.org/rfc/rfc3332.txt

[11] Bjørnar Salberg. “WLAN – GPRS Interworking”. Tesis de Grado, Agder University College; Noruega 2001.

[12] Li Ma, Fei Yu, Victor Leung. "A New Method to Support UMTS/WLAN Vertical Handover Using SCTP”. University of British Columbia; Vancouver, BC, Canadá.

[13] 3GPP “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Combined GSM and Mobile IP Mobility Handling in UMTS IP CN; (Release 3)”. (3G TR 23.923).

[14] “Network design with Mobile IP”.
En línea:
http://www.isoc.org/isoc/conferences/inet/01/CD_proceedings/T40/inet_T40.htm

[15] 3GPP2 “3rd Generation Partnership Project 2; Wireless IP Architecture Based on IETF Protocols; *Version 1.0.0*”. (3GPP2 P.R0001).

[16] Comisión de Regulación de Telecomunicaciones. Informe Sectorial de Telecomunicaciones”. Bogota DC. Julio 2004
En línea: http://www.crt.gov.co/documentos/biblioteca/

[17] Ministerio de Comunicaciones. “Industria de telecomunicaciones: tendencias y perspectivas”. Bogota DC. Octubre 2004
En línea:
http://www.agenda.gov.co/documents/files/1-PRESENTA%20MINISTRA%20-%20CINTEL%20-%20OCT%202004.ppt

[18] Comisión de Regulación de Telecomunicaciones. “Informe Sectorial de Telecomunicaciones”. Bogota DC. Julio 2005
En línea: http://www.crt.gov.co/documentos/biblioteca/

[19] Srikant Sharma, Inho Baek, Yuvrajsinh Dodia, Tzi-cker Chiueh. OmniCon: A Mobile IP-based Vertical Handoff System for Wireless LAN and GPRS Links. Computer Science Department, Stony Brook University, Stony Brook, NY.
En línea:
http://csdl.computer.org/dl/proceedings/icppw/2004/2198/00/21980330.pdf

[20] Sutinen, Tiia. End User Service Quality in Multi-Access Networks. Tesis de Maestria, Universidad de Oulu, Departamento de Ingeniería Electrica e Información, Oulu, Finlandia.