CAPÍTULO II: "ASPECTOS GENERALES DEL SISTEMA DE TELEFONÍA MÓVIL UMTS DE TERCERA GENERACIÓN"

OBJETIVOS DEL CAPÍTULO II

- Describir los componentes que conforman la arquitectura de red UMTS.
- Exponer la tecnología, los protocolos y la seguridad utilizada por el sistema UMTS.
- Especificar los tipos de servicios y la calidad con que son proporcionados por el sistema UMTS.

INTRODUCCIÓN AL CAPÍTULO II

Este capítulo define los aspectos más importantes relacionados al sistema móvil de tercera generación UMTS, en donde se detallan puntos como: historia, tecnología, modos de transmisión, arquitectura, protocolos, calidad de servicio, seguridad y servicios ofrecidos por el sistema. El estándar UMTS busca establecer un sistema universal de telecomunicaciones con capacidades flexibles que faciliten el roaming de los usuarios en cualquier parte del mundo, con mejores servicios y mayor velocidad en la transferencia de datos. Implícitamente mejora todos los aspectos técnicos y de infraestructura de las tecnologías anteriores. Proporciona nuevos servicios además de los tradicionales con mayor seguridad y mejor definición de la calidad del servicio.

2.1 HISTORIA DE UMTS

UMTS es un sistema móvil de tercera generación que fue diseñado para la entrega flexible de cualquier tipo de servicio, en donde cada nuevo servicio no requiere de una optimización particular de la red.

La cronología concerniente al sistema móvil UMTS se resume a continuación:

- En 1985 se comenzó el estudio del sistema IMT-2000, donde, IMT significa «Las Telecomunicaciones Móviles Internacionales» (International Mobile Telecommunicacitons), mientras que el número 2000 posee tres significados que son: la ITU esperaba que en el año 2000 el sistema estuviese disponible, que las velocidades de información serían de 2000 Kbps y que las frecuencias estarían en la banda de los 2000 MHz.
- Entre 1987 y principios de 1990 se realizaron reuniones tres veces al año en Europa, Estados Unidos y Japón, en donde participaron diferentes proyectos de investigación de UMTS como: RACE1[30] y RACE2 que fueron fundados por la CEC Commission of European Communities (Comisión Europea de Comunidades) y FAMOUS Future Advanced Mobile Unviersal Telecommunications Systems (Futuro de los Sistemas Avanzados de Telecomunicaciones Móviles Universales).
- Entre 1991 y 1995 la CEC fundó dos proyectos de investigación llamados: CODIT Code Division Testbed (Plataforma de Prueba de División por Códigos) y ATDMA Advanced Time Divison Multiple Access (Acceso Múltiple por División de Tiempo Avanzado) que fueron apoyados por las compañías manufactureras de telecomunicaciones de Europa y los operadores de red. Ambos proyectos investigaron el acondicionamiento de WCDMA[31] Wideband Code Division Multiple Access (Acceso Múltiple por

[30] R&D in Advanced Communications-technologies for Europe (R&D en el avance de las tecnologías de comunicaciones de Europa) que se conoce como RACE, del cual, hubieron dos grupos RACE1 y RACE2.
[31] Es una tecnología de alta velocidad utilizada en la red móvil UMTS de tercera generación.

División de Códigos de Banda Ancha) y TDMA. El trabajo fue posteriormente continuado por el proyecto FRAMES Future Radio Wideband Multiple Access System (Sistema Futuro de Radio Acceso Múltiple de Banda Ancha) y se convirtió en la base del trabajo sobre UMTS que sería realizado por ETSI.

- En Febrero de 1992 la Conferencia Mundial de Radiocomunicaciones (WRC[32]-92) celebrada en España, dispuso que las frecuencias a utilizar por el sistema UMTS futuro serían las bandas de 1885~2025MHz y 2110~2200MHz.
- En Diciembre de 1996, fue establecido el fórum de UMTS con un encuentro inaugural en Suiza.
- En Enero de 1998 el SMG05 de ETSI se reunió en París para proponer la combinación de W-CDMA y TD-CDMA para la especificación de la interfaz aérea de UMTS.
- En Junio de 1998 se propuso para la interfaz Tierra-Aire las tecnologías: UTRAN UMTS Terrestrial Radio Access Network (Red de Acceso a Radio Terrestre de UMTS), WCDMA y EDGE. Las cuales fueron entregadas a la ITU-R International Telecommunicacitons Union - Radioelectric Section (Unión Internacional de Telecomunicaciones - Sección Radioeléctrica).
- El 4 de Diciembre de 1998 el SMG de ETSI, el T1P1, el ARIB TTC y TTA crearon el 3GPP en Dinamarca.
- En Marzo de 1999 la ITU aprobó las interfaces de radio para la tercera generación de los sistemas móviles.

[32] WRC, World Radicommunication Conference (Conferencia Mundial de Radiocomunicaciones), la cual se celebra cada 3 ó 4 años.

- En Diciembre de 1999 Se finalizó la estandarización de ETSI para las especificaciones de UMTS versión 99[33] tanto para FDD Frequency Division Duplex (Duplex por División de Frecuencia) y TDD Time Division Duplex (Duplex por División de Tiempo).
- El 31 de Enero de 2003, Ericsson condujo la primera demostración de IPv6 Internet Protocol verssion 6 (Protocolo de Internet versión 6) sobre una red UMTS.
- El 16 de Diciembre de 2004 fue la fecha de congelamiento para la versión 6 de UMTS.
- El 14 de Febrero de 2005, Ericsson demostró la velocidad de transferencia de 9 Mbps con HSDPA High Speed Downlink Packets Access (Acceso a Paquetes descendentes de alta Velocidad) fase 2 sobre la red WCDMA.
- En Agosto de 2007, Ericsson fue el primero en completar las llamadas en WCDMA para todas las bandas de frecuencia definidas por 3GPP.
- En Marzo de 2008, el organismo «3G Americas» publica recomendaciones para la transición a IPv6 en América. Además, en El Salvador CTE Telecom Personal despliega sus servicios de videotelefonía de tercera generación.

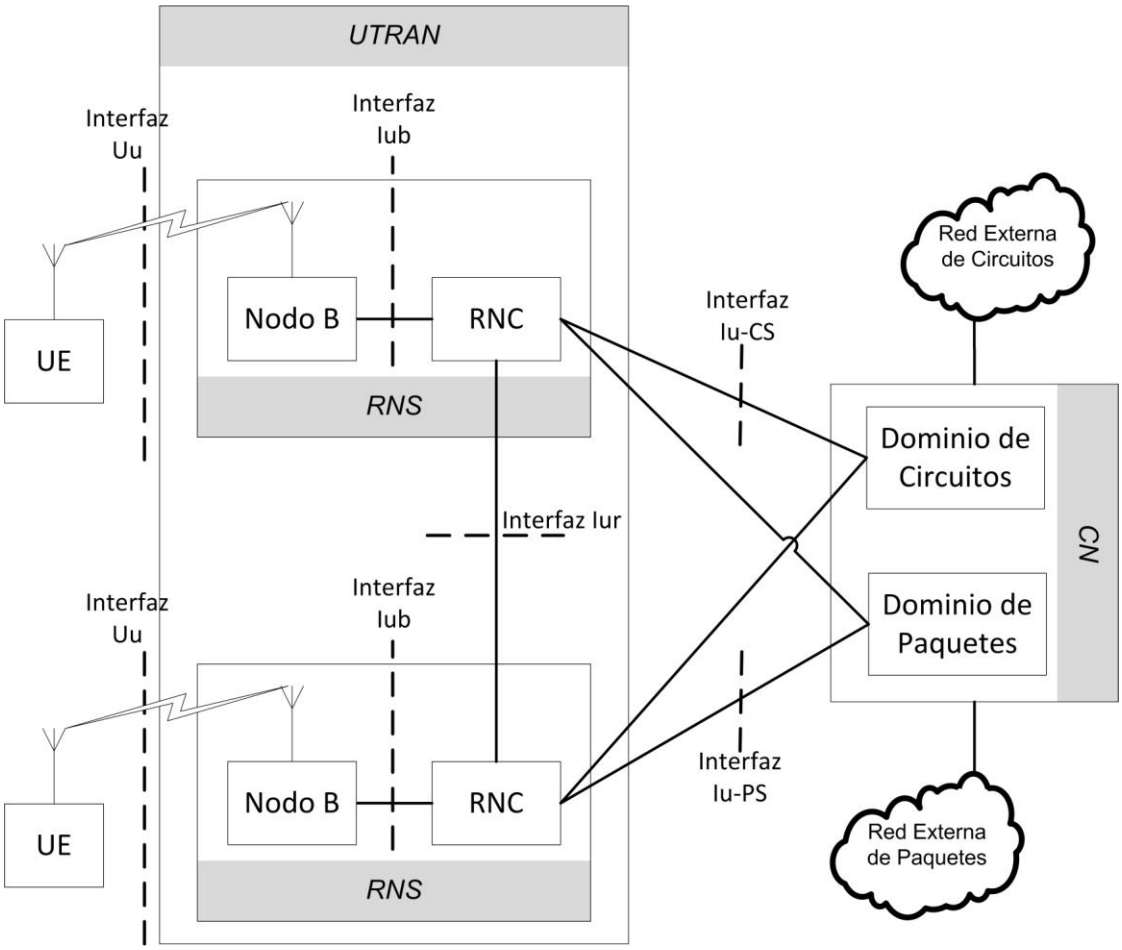
2.2 ARQUITECTURA DE UMTS

El UE User Equipment (Equipo de Usuario) es el dispositivo encargado de hacer visibles al usuario los servicios que la red UMTS puede brindar. Aunque el concepto de una red UMTS es el de tener un acceso a múltiples redes, la principal red de acceso es la UTRAN, cuya función principal es brindar, mantener, controlar y gestionar una conexión entre el UE y el CN Core Network (Núcleo de Red) de tal

[33] Las especificaciones de 3GPP están siendo mejoradas constantemente con nuevas características. Para proveer a los desarrolladores una plataforma para la implementación de productos. Al mismo tiempo, permiten agregar nuevas características, el 3GPP utiliza una sistema de versiones paralelas las cuales se denominan por ejemplo: versión 99, versión 4, versión 5, etc.

forma que en este último se desliguen las funciones antes dichas y pueda enfocarse en los aspectos de servicio de aplicaciones al usuario. La UTRAN está constituida por varios RNS Radio Netwok Subsystem (Subsistema de Red de Radio), un RNS está conformado por un cierto número de Nodos B y un RNC Radio Network Controller (Controlador de Red Radioeléctrica).

Figura 2.1 Arquitectura de una red UMTS



El Nodo B es el encargado de proveer la cobertura de la señal de acceso a la red. EL RNC es el encargado de controlar y gestionar la conexión establecida por el Nodo B. El CN se encarga de la movilidad y la QoS.

Las principales interfaces son las siguientes:

- Interfaz Uu: se encuentra entre el UE y la UTRAN.
- Interfaz Iub: se encuentra entre el Nodo B y su RNC.
- Interfaz Iur: se encuentra entre dos RNS.
- Interfaz Iu: se encuentra entre un RNS y el CN.

2.2.1 Equipo de Usuario

El UE también llamado terminal UMTS, es el comúnmente conocido teléfono celular. El funcionamiento del UE está sujeto a normas y estandarizaciones necesarias para interactuar con el resto de elementos de la red UMTS, pero algunas características adicionales en los servicios son determinadas por el fabricante.

El UE deberá cumplir con los siguientes requisitos esenciales para su funcionamiento en la red:

- Una interfaz para albergar la UICC Universal Integrade Circuit Card (Tarjeta de Circuito Integrado Universal), la cual esta constituida por un USIM Universal Subscriber Identity Module (Módulo de Identidad de Abonado Universal) y el ISIM IMS Subscriber Identity Module (Módulo de Identidad de IMS).
- Proveer servicios y registros.
- Actualización de la ubicación.
- Envió y recepción de servicios con o sin conexión.
- IMEI.
- Identificación básica de las características del Terminal.
- Posibilidad de realizar llamadas de emergencia sin USIM.

- Soporte para la ejecución de algoritmos necesarios para la autenticación y la encriptación.

Además deberá cumplir con los siguientes requisitos para facilitar una evolución futura:

- Una API Application Program Interface (Interfaz de Programación de Aplicaciones).
- Un mecanismo para la descarga de información relacionada con nuevos servicios (parámetros y software) los cuales representan: nuevos protocolos, nuevas funciones y nuevas API.

- **Arquitectura del UE**

El UE está formado por dos módulos, el ME y la UICC, los cuales cumplen funciones determinadas.

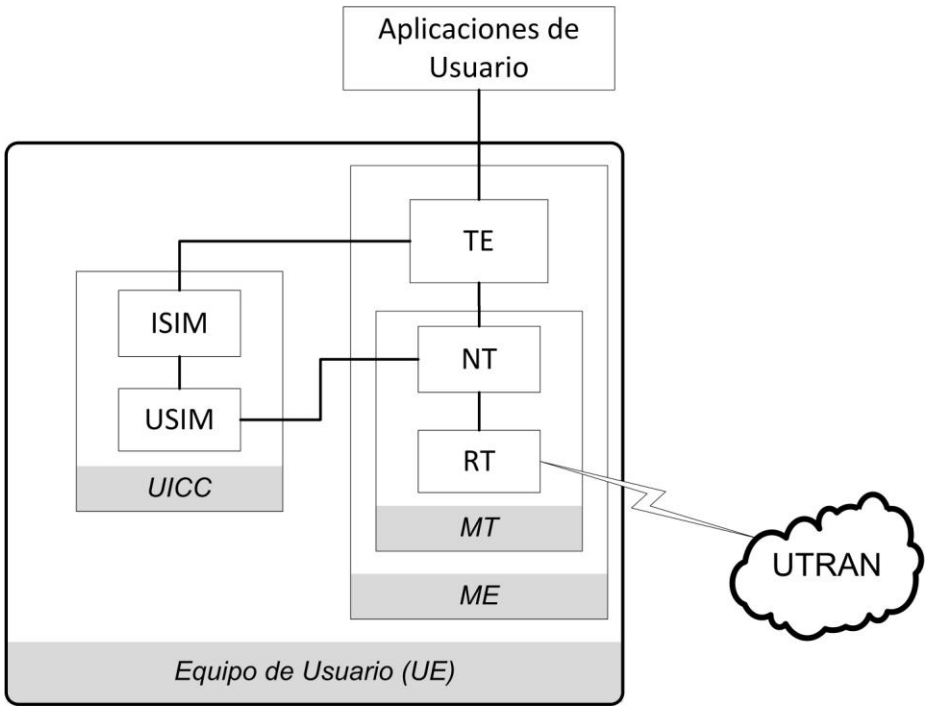
La UICC es un circuito integrado extraíble que almacena la información pertinente al usuario y a los servicios que éste posee, está constituida por el USIM y el ISIM. El USIM posee la información referente de suscripción del usuario de la red y se encuentra conectado a los perfiles de servicio del usuario, esta información está almacenada en el HLR. La diferencia más notoria entre el SIM de GSM y el USIM, es que en este último la información se actualiza utilizando la red de UMTS.

Los datos que se almacenan en el USIM son cinco:

- Datos Administrativos: entre los cuales están valores clave para algoritmos de seguridad, el IMSI e información de clase de acceso para la red.
- Datos de Red Temporales: relacionados con la gestión de movimiento como el identificador del área de ubicación actual, el TMSI y el valor clave de cifrado calculado.

- Datos sobre los servicios: información acerca de la disponibilidad de los diferentes servicios para el usuario del USIM.
- Datos de aplicación: almacena aplicaciones necesarias para servicios específicos las cuales se pueden descargar, almacenar en el USIM y ejecutar posteriormente.
- Datos personales: son datos que el usuario almacena, por ejemplo: números telefónicos, mensajes de texto y otros.

Figura 2.2 Arquitectura del UE



El ISIM es utilizado para acceder a las aplicaciones IMS IP Multimedia Subsystem (Subsistema Multimedia IP), la finalidad de éste es proveer autenticación del abonado y el acuerdo de claves para el cifrado de información para acceder a los servicios IMS. Dentro de la información que gestiona el ISIM se encuentra:

- Claves de seguridad de usuario.
- La IMPI, IP Multimedia Private Identity (Identidad de Usuario Privada Multimedia IP).
- La IMPU, IP Multimedia Public User identity (Identidad de Usuario Pública Multimedia IP).
- El nombre del dominio que identifica el punto de entrada en el extremo de red.
- Una variedad de datos administrativos más.

El ISIM necesita del USIM para acceder a la red base, no obstante, si se utiliza una tecnología de acceso complementaria el ISIM puede funcionar por sí solo.

El ME o dispositivo móvil se divide en dos módulos: el TE y el MT. El TE es la parte del UE que se encarga de manejar las aplicaciones de los servicios de usuarios, básicamente se encarga de manejar los datos referentes a las aplicaciones como: control de llamadas, paquetes IP y codificación multimedia de IMS.

El MT es la parte del ME que se encarga de terminar la transmisión radioeléctrica y adaptar las características del TE a las necesidades de transmisión, es decir, se encarga de gestionar todas las características del radioenlace y de la red UMTS. El MT se divide en la NT Network Termination (Terminación de Red) y la RT Radio Termination (Terminación de Radio).

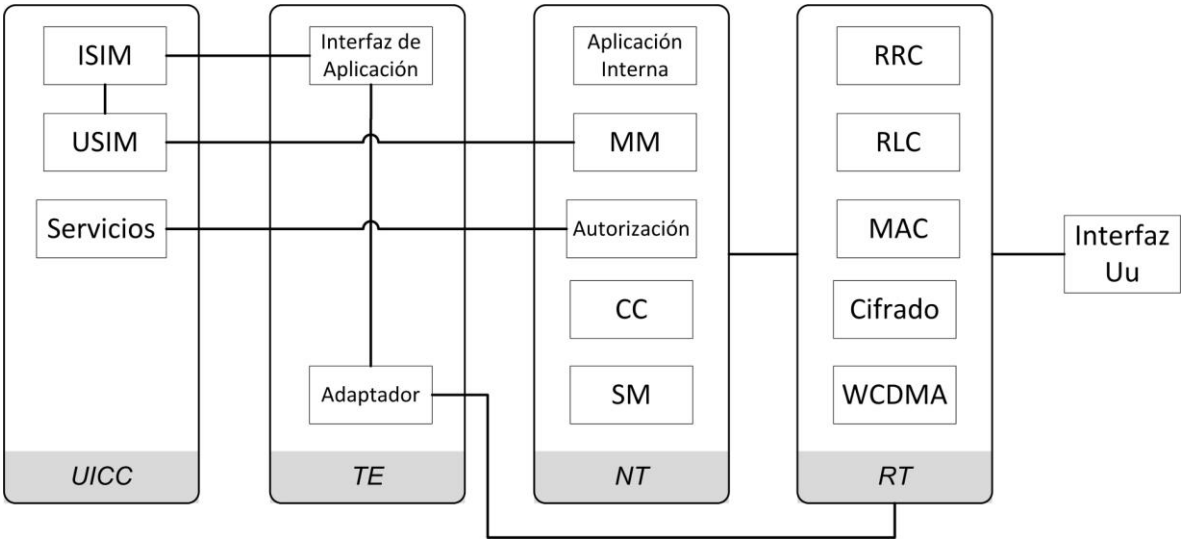
La NT es la parte que interactúa con el CN, es decir, los datos generados por la NT pasan de forma transparente por la UTRAN y llegan al CN. La NT se encarga de la gestión de movilidad tanto para la conmutación de paquetes como de circuitos y también de la gestión de sesiones.

La RT es la parte de la MT encargada de gestionar los recursos de radio y de acceso a la red, ésta interactúa con la UTRAN empleando protocolos como: el

MAC Meduim Access Control (Control de Acceso al Medio), RLC y el RRC Radio Resources Control (Control de Recursos de Radio).

En la Figura 2.3 se muestran las partes del UE y sus funcionalidades.

Figura 2.3 Las partes del UE y sus funcionalidades.



Existen cuatro tipos de MT los cuales se derivan de las características que tengan tanto la NT como la RT, es decir, las características de radio y de red. Estos son los siguientes:

- Un MT con un solo Modo de Radio: éste puede utilizar un solo tipo de interfaz de radio que en este caso para UMTS corresponde a WCDMA.
- Un MT Multi-Radio: este puede utilizar distintas interfaces de radio, un ejemplo de esto es: el teléfono dual GSM/ UMTS, el cual es definido por las especificaciones de la 3GPP, éste tiene la particularidad de poder emplear redes GSM fuera de la cobertura de la red UMTS. Este teléfono es el utilizado en la etapa de transición GSM a UMTS.

- Un MT de una Sola Red: éste solo puede utilizar un sólo CN. Puede operar en modo conmutación por paquetes, conmutación por circuitos o en modo híbrido.
- Un MT Multi-Red: éste puede utilizar varios CN simultáneamente aparte de los CN de UMTS.

- **Tipos de UE en UMTS**

Se definen cuatro tipos de terminales:

- El Terminal Clásico: es fabricado con la intención de que sea económico y por lo tanto ofrece funciones limitadas comparado con los servicios que ofrece la red, por ejemplo: acceso a voz por conmutación de circuitos y acceso a datos de bajas velocidades de transmisión, pero mejores que las que ofrece GSM/ GPRS. Este Terminal admite los métodos de acceso GSM y WCDMA pero no de forma simultánea. Es decir, en este Terminal se implementa un MT de una sola red. Su mejor característica es que puede emplear las redes GSM existentes. Se puede decir que es un móvil de GSM mejorado.
- Terminal Modo Dual: este puede acceder a redes GSM o WCDMA, y seleccionar de forma automática el método de acceso a utilizar, por ejemplo: las llamadas de voz se realizan normalmente a través de GSM y los servicios de datos de alta velocidad a través de WCDMA. Una característica importante de este terminal es que puede realizar handover de un sistema a otro en ambas direcciones y si es posible, adapta el servicio que esta en uso al nuevo acceso a radio adquirido después del handover. Este terminal emplea un MT multi-red.
- Terminal Multimedia: este terminal es similar al terminal modo dual pero más inteligente desde el punto de vista de las aplicaciones. Se puede decir

que es la combinación de un teléfono móvil y una computadora portátil, ofreciendo numerosas aplicaciones para los servicios multimedia.

- Terminales Especiales: están destinados para fines especiales como por ejemplo: se pueden poner en un vehículo y a través de la red UMTS brindar la ubicación del mismo. Este tipo de terminales utilizan el modo de conmutación por paquetes ya que el área de aplicaciones para este modo es muy extensa.

- **Negociación de capacidades de un UE**

Antes de comenzar la transmisión de datos, el UE deberá negociar características básicas con la red, esta información se conoce como «marca de clase de la estación móvil». Las clases de marcas son: la clase 1 que consta de dos octetos, es utilizada por GSM; la clase 2 que es de cinco octetos, es utilizada por GSM y UMTS (en el caso de UMTS se utiliza para negociar con el CN) y la clase 3 que es utilizada sólo por UMTS, se utiliza para negociar con la UTRAN. La información que guarda la clase 3 incluye los siguientes datos:

- Los modos WCDMA disponibles (TDD o FDD).
- Las capacidades del modo dual (soporte para las diferentes variantes de GSM y otras características especiales).
- Algoritmos de cifrado disponibles.
- Propiedades del UE para el cálculo de una célula próxima.
- Posibilidad de utilizar los métodos de posicionamiento.
- Posibilidad de utilizar el conjunto de caracteres universales 2 (estándar de código de caracteres de 16 bits conocido como ISO/IEC 10646 ó UNICODE) en lugar del conjunto de caracteres de 7 bits utilizados en los SMS.

2.2.2 Nodo B

El nodo B desde el punto de vista del usuario es el encargado de proveer la cobertura de la red. Dentro de las principales funciones que posee el Nodo B está la generación de códigos para el acceso a la red y el control de potencia de la señal destinada al UE.

Como se observó en la Figura 2.1 de la arquitectura de una red UMTS, el nodo B posee dos interfaces: la interfaz Uu que se conecta con el UE y la interfaz Iub que se conecta con el RNC. El Nodo B implementa la interfaz Uu por medio de los canales físicos, transfiriendo la información desde los canales de transporte hasta los canales físicos basándose en la disposición predeterminada por el RNC.

- **Estructura física del Nodo B.**

El Nodo B es un elemento transceptor, es decir, transmite y recibe señales de radio del UE. Para este fin posee los elementos que se muestran en la Figura 2.4.

Los bloques RX y TX son los encargados de transmitir y recibir las señales radioeléctricas, el modulador se encarga de adaptar las señales binarias para la transmisión debido a que una señal binaria posee demasiada componente de corriente continua, además, es un mecanismo para la optimización del ancho de banda disponible. Las modulaciones utilizadas son QPSK, Dual QPSK y 16QAM Quadrature Amplitude Modulation (Modulación por Amplitud en Cuadratura).

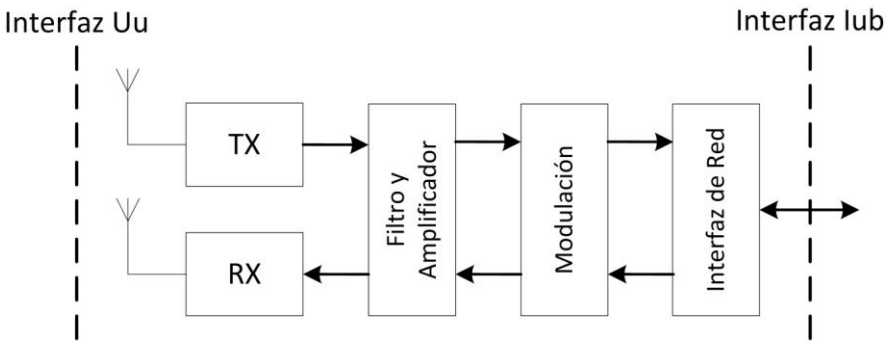
- **Estructura lógica del Nodo B.**

En la parte de la interfaz Iub, el Nodo B está compuesto por dos entidades lógicas: el transporte común y los TTP Traffic Termination Point (Puntos de Terminación de Tráfico). El transporte común se realiza por los canales de transporte común que son utilizados por el UE para el acceso inicial a la red. El transporte común

también posee un puerto destinado para actividades de O&M Operation & Maintenance (Operación y Mantenimiento).

En la interfaz Uu, el Nodo B está compuesto por una célula. Una célula posee un código de aleatorización y un número de identificación que es utilizado por el UE para identificarse y registrarse en la topología de red.

Figura 2.4 Estructura física del Nodo B



2.2.3 Controlador de Red de Radio

El RNC es el elemento de la UTRAN que se encarga de gestionar un RNS, está ubicado entre la interfaz Iub (conexión que viene del Nodo B) y la interfaz Iu (conexión que va hacia el CN). Además de estas dos interfaces posee la interfaz Iur, que es utilizada para el establecimiento de conexiones entre subsistemas de la UTRAN.

El RNC es el encargado de las dos funciones más importantes en la UTRAN: el RRM Radio Resource Management (Gestión de Recursos de Radio) y la función de control.

El RNC se divide lógicamente en tres tipos:

- CRNC Control RNC (RNC de Control): provee el control sobre las entidades de transporte común y determina el tráfico del Nodo B.

- SRNC Service RNC (RNC de Servicio): establece y mantiene conexiones de radio con el fin de conducir el tráfico común y dedicado entre el UE, RNC y CN.
- DRNC Drifting RNC (RNC de Transferencia): es el encargado de realizar los handover.

- **Función de Gestión de Recursos de Radio**

Para esta función el RNC es el encargado de estabilizar el trayecto radioeléctrico y hacer que se cumplan los requisitos de QoS, todo esto lo hace mediante el protocolo RRC Radio Resource Control (Control de Recursos de Radio). Dentro de la gestión de recursos de radio se tienen las siguientes funciones:

- Control de Handover: Cuando el UE se encuentra en movimiento y se genera la necesidad de cambiar de célula y establecer otra conexión con una nueva célula, a este proceso se le denomina handover. El handover se puede producir también cuando la capacidad de una célula alcanza o se aproxima al máximo de congestionamiento. Existen tres tipos de handover: Hard handover, cuando el UE realiza un cambio de célula utilizando una sola conexión con el Nodo B. Soft handover, cuando el UE estable más de una conexión con diferentes Nodos B. Softer handover, cuando el UE establece más de una conexión con diferentes sectores del mismo Nodo B.

  Los pasos para realizar un handover son: mediciones, decisiones y ejecución. Las mediciones son tomadas por el UE y enviadas al RNC, estás mediciones están estrechamente relacionada con la QoS de la conexión. Si se cuenta con una baja QoS y se está en el límite de una célula en donde la señal es muy débil, mientras el UE se aleje de la célula bajará aún más la calidad de la conexión necesitando realizar un handover.

En la especificación TS 25.33 del 3GPP se definen las mediciones que debe realizar el UE, las cuales son: Intra-frecuencia, Inter-frecuencia, Inter-sistema, volumen de tráfico, calidad, internas.

- Control de Potencia: La finalidad del control de potencia es ajustar la potencia del transmisor a un nivel adecuado para satisfacer la QoS exigida, sin aumentarla innecesariamente, ya que sí el nivel de potencia es demasiado alto aumentarán las interferencias hacia los demás transmisores.

  Hay dos tipos de control de potencia: El primero es el control de potencia de bucle abierto, que sirve para ajustar la potencia de los enlaces ascendentes (uplinks) en donde el UE ajusta la potencia del nivel de transmisión en base a un cálculo del nivel de la señal recibida desde el canal CPICH Common Pilot Channel (Canal Piloto Común) del Nodo B antes de establecer la conexión. Una vez establecida la conexión, se emplea el segundo tipo que es el control de potencia de bucle cerrado para compensar las rápidas fluctuaciones de la intensidad del canal de radio.

- Control de Admisión y Programador de Paquetes: La función del control de admisión es analizar si una nueva llamada puede tener acceso al sistema sin tener que sacrificar los requisitos de QoS que imponen las llamadas ya existentes, por lo que el RNC debe predecir cual será la carga impuesta a la célula, sí esta nueva llamada es admitida y sí los recursos radioeléctricos que ésta posee lo pueden permitir de acuerdo a ello el RNC tomará una decisión.

  El programador de paquetes es el encargado de determinar el tiempo en el que se van a transmitir los flujos de información.

- Gestión de los Códigos: El RNC también es el encargado de la gestión de los códigos de aleatorización y canalización, utilizados para la conexión del UE a la red.

  Un conjunto de códigos son ortogonales cuando éstos no tienen ninguna relación entre ellos mismos. Los códigos de aleatorización son los encargados de identificar a la célula, éstos no son ortogonales entre sí. Esto se realiza para facilitar los procesos de handover, ya que en estos procesos al cambiarse de célula se cambia de código de aleatorización. Mientras que los códigos de canalización que son los encargados de identificar a los usuarios de una célula y son ortogonales, es decir, no tienen relación alguna con el fin de evitar las interferencias entre usuarios conectados a la misma célula.

  Una mala administración de los códigos utilizados en WCDMA puede traer como consecuencia la inestabilidad en el sistema, además, los códigos son limitados y es por ello que son gestionados por el RNC y no por el Nodo B. Los códigos de aleatorización para el enlace ascendente son un total de $2^{18} – 1 = 262{,}143$ códigos, de los cuales no todos son utilizados; mientras que para el enlace descendente existen 2^{24} códigos. En cuanto a los códigos de canalización existen 256 disponibles.

- **Funciones de control**

Las funciones de control del RNC son las siguientes:

- Difusión de la Información del Sistema: El RNC ayuda a la UTRAN en las funciones de control facilitando al UE la información del sistema y los datos básicos para la comunicación con la UTRAN, por ejemplo: los criterios de medida radioeléctricos, la indicación de la primera llegada de la información de localización, información sobre el trayecto de radio,

datos de ayuda para la localización. El UE puede recibir esta información en todo momento.

- Gestión de Acceso Inicial y Gestión de Señalización: Antes de que el RNC establezca una conexión RAB Radio Access Bearer (Portadora de Acceso a Radio) para la transferencia de información, el RNC debe crear un canal de señalización entre el UE y el CN el cual se define en la especificación TS 25.990 del 3GPP, este canal es llamado SRB Signalling Radio Bearer (Portador de Radio Señalización).
- Gestión de la Portadora de Radio: Una vez establecido el SRB entre el CN y el UE, las solicitudes de RAB son negociadas, luego el RNC analiza los atributos de los RAB solicitados, evalúa los recursos de radio disponibles para ver la factibilidad de la conexión y por último activa y reconfigura los canales de radio del Nodo B para establecer el RAB entre el UE y la red.
- Seguridad en la UTRAN: EL RNC cifra la información de señalización y los datos de usuario con algoritmos predefinidos, con el fin de proveer seguridad a la conexión establecida, también se encarga de descifrar los mensajes recibidos utilizando los mismos algoritmos.
- Gestión de la Movilidad a Nivel de la UTRAN: Consiste en las funciones que gestiona el RNC para que el UE se mantenga en contacto con las células radioeléctricas.
- Tratamiento de la Base de Datos: El RNC mantiene un almacén de información relacionada con las células que éste tiene a su disposición, esta información la envía a los Nodos B y éstos la distribuyen a los UE realizando la tarea de difusión de información. Esta información puede ser: información de los “ID” Identification (Identificación) de las células, de control de potencia, de handover y de las células vecinas.

- Posicionamiento del UE: El RNC es el encargado de controlar los mecanismos de posicionamiento del UE en una célula, además de coordinar los recursos radioeléctricos para realizar esta tarea.

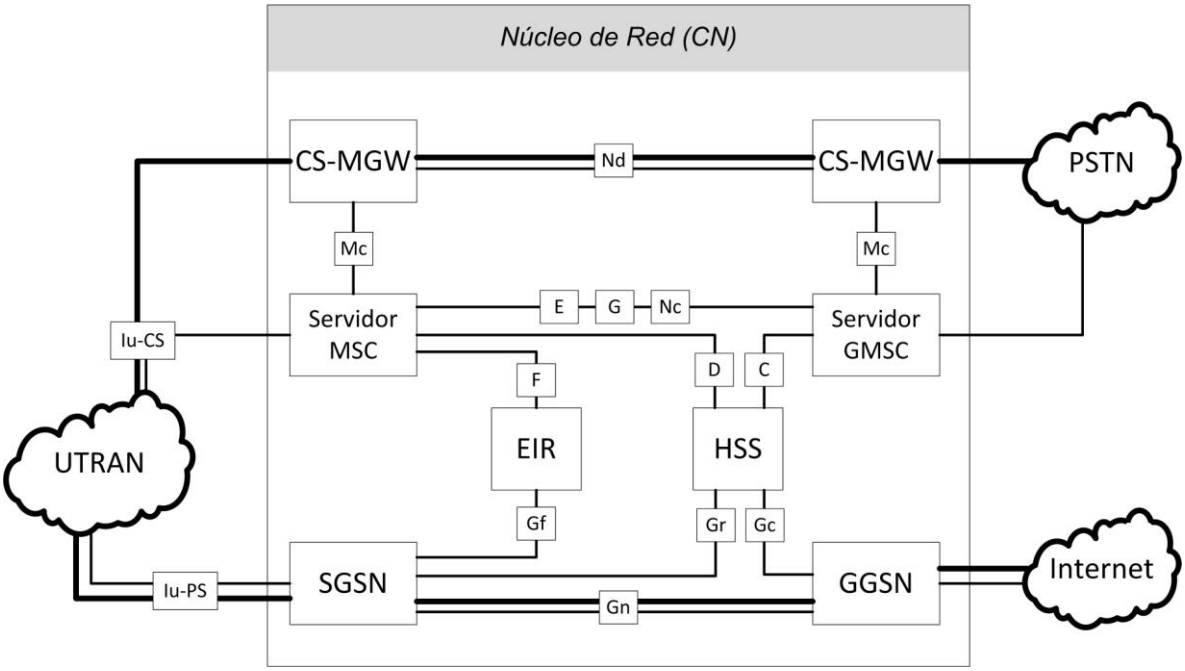
2.2.4 Núcleo de Red

El CN de UMTS es la plataforma básica de todos los servicios de comunicaciones que proporciona la red, que incluyen la conmutación de llamadas por CS Circuit Switched (Conmutación por Circuitos) y el encaminamiento de datos por PS Packet Switched (Conmutación por Paquetes). En UMTS el CN es heredado de la tecnología GSM/GPRS, debido a las características de interworking con GSM.

Posteriormente el CN evoluciona hasta introducir el sub-sistema denominado IMS, el cual es el encargado de los servicios basados en el protocolo IP.

En la Figura 2.5 se muestra el CN con los elementos necesarios para procesar el tráfico de PS, el tráfico de CS y las interfaces internas que posee.

Figura 2.5 Esquema básico del CN de UMTS



En dicha figura, las líneas más gruesas representan el tráfico de usuario (plano de usuario) y las líneas más delgadas representan la señalización (plano de control). En la Figura 2.5 se puede resaltar que el CS-MGW Circuit Switched Media Gateway (Gateway Multimedia de CS) y el GMSC se pueden combinar en una sola entidad física, que en este caso se denomina GMSC. Además, el servidor MSC es la combinación del MSC y el VLR, que se puede escribir como «MSC/VLR».

El HLR y el AuC se integraron para formar el HSS Home Subscriber Server (Servidor de Suscriptores Locales), esta entidad realiza funciones que son comunes a los dos dominios que se encuentra en el CN.

Dentro de las funcionalidades que proporcionan el HLR y el Auc se encuentran:

- Gestión de la Movilidad: almacenamiento de la información de localización que puede indicar la posición de un usuario.
- Generación de Información de Seguridad de Usuario: esta función la cumple el AuC, el cual envía señales a través del HLR.
- Presentación de Servicios: el HSS proporciona acceso a los datos del perfil de los servicios.
- Establecimiento de Llamadas y Sesiones: soporta los procesos para el establecimiento de llamadas (para el dominio CS) y de sesiones (para el dominio PS).
- Tratamiento de la Identificación: proporciona las relaciones adecuadas entre todos los identificadores utilizados en el dominio CS (IMSI, MSISDN) y en el dominio PS (MSISDN, IMSI y direcciones IP).
- Autorización de los Servicios: proporciona las autorizaciones básicas para el establecimiento de sesiones y llamadas.

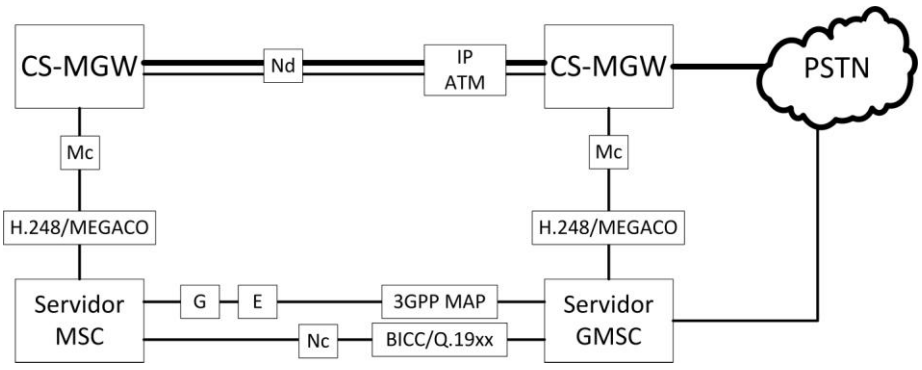
Además del HSS, se encuentra el EIR que es una funcionalidad común a los dos dominios del CN.

- **Dominio de Conmutación por Circuitos (CS)**

Esta estructura proviene de GSM, aunque posteriormente se propuso un método de implementación alternativo en el cual se puede ajustar el control (plano de control) y el tráfico (plano de usuario) de forma separada, como se muestra en la Figura 2.6.

El objetivo de separar el plano de control del plano de usuario, es para proporcionar estabilidad al sistema, ya que una MSC puede controlar varios CS-MGW. El servidor MSC es el encargado de re-gestionar la señalización y proveer el control a los Gateways. Como se observa en la figura, el plano de control está constituido por el servidor GMSC que es una Gateway de señalización, su función es realizar la correspondencia entre la señalización utilizada en el dominio CS y la señalización utilizada en la PSTN. En el plano de usuario se encuentra el CS-MGW que es un Gateway que cumple la misma función que el GMSC pero con el tráfico de usuario.

Figura 2.6 Dominio CS del núcleo de red (CN)



El servidor MSC controla al CS-MGW mediante la interfaz Mc, la cual emplea el protocolo MGCP Media Gateway Control Protocol (Protocolo de Control de Gateway) definido por la UIT-T en la recomendación H.248 y conocido también como MEGACO.

La interfaz Nc transmite información de control de llamadas mediante el protocolo BICC Bearer Independent Call Control (Portador de Control de Llamadas Independiente), éste incluye un conjunto de paquetes definidos para utilizarlos conjuntamente en la especificación Q.1950 de la UIT-T.

La interfaz Nd opera tanto en el plano de control como en el plano de usuario, en esta interfaz se tienen protocolos de trama apropiados y mecanismos para la transferencia de datos hacia la PSTN a través de un CS-MGW. Se puede implementar con los protocolos ATM o IP, estas opciones se contemplan en la especificación TS 24.414 de 3GPP.

Las interfaces E y G sirven para la comunicación entre los MSC, esto se realiza por ejemplo: cuando ocurre un handover y se nenecita cambiar de MSC. En estas interfaces se implementa el protocolo MAP, en la especificación TS 29.002 se describe detalladamente el protocolo MAP.

- **Dominio de Conmutación por Paquetes (PS)**

El SGSN contiene la función de registro de posiciones, donde se almacenan los datos necesarios para iniciar y concluir la trasferencia de información de datos por paquetes como la IMSI entre varias identidades temporales, información de la posición de direcciones PDP (por ejemplo: direcciones IP). Para la transferencia de paquetes el SGSN necesita saber con que GGSN se está comunicando el usuario final, por esta razón el SGSN almacena las direcciones del GGSN, mientras éste almacena las direcciones del abonado como el número IMSI y las direcciones PDP.

Se observa en la Figura 2.7 el servidor DHCP Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host) que es el encargado de la asignación de direcciones IP dinámicas para los usuarios finales, esta asignación dinámica se produce por motivos de seguridad y pueden ser de tipo IPv4 Internet Protocol verssion 4 (Protocolo de Internet versión 4) ó IPv6.

Un servidor DNS Domain Name Server (Servidor de Nombres de Dominio), el cual es utilizado para saber el nombre del dominio de los elementos de la red.

Los APN Access Point Name (Nombre de Punto de Acceso) especifican los servicios que el usuario va a utilizar (por ejemplo: un APN puede ser Internet).

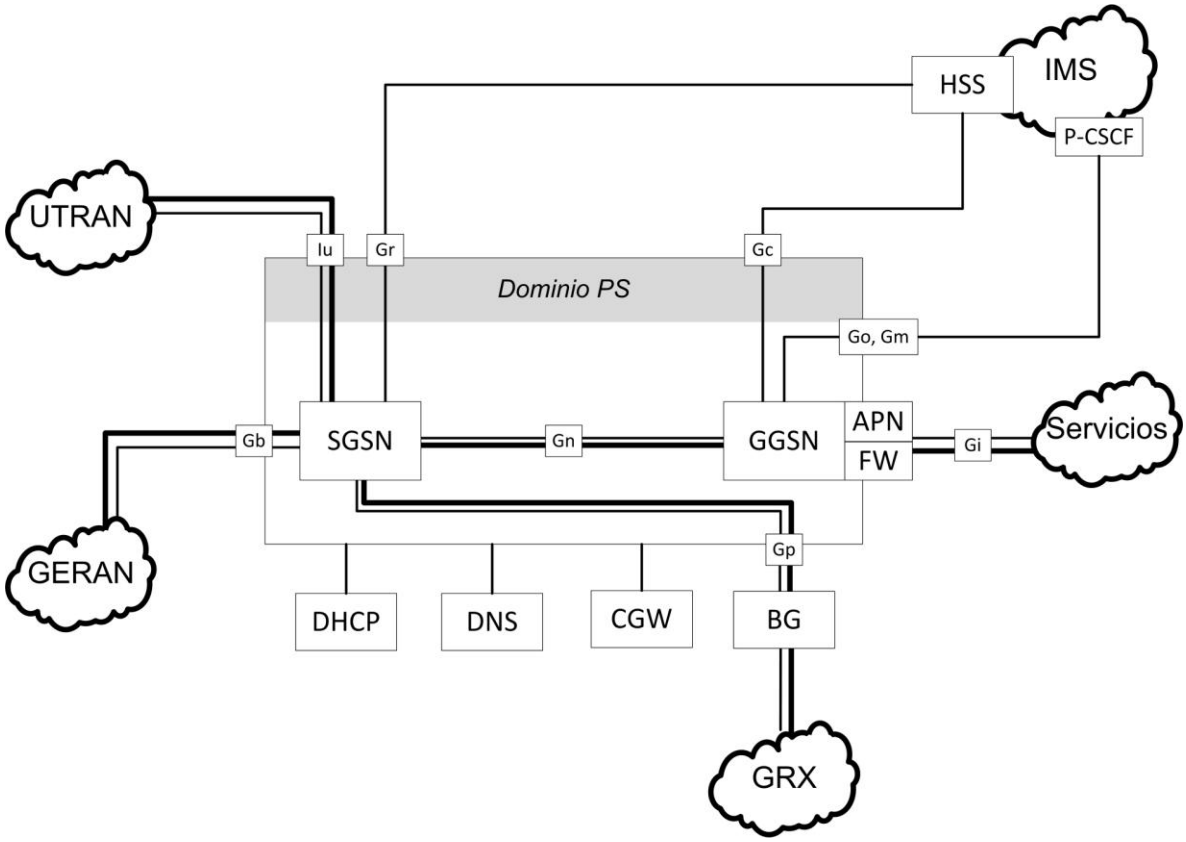
Los FW Firewall (Cortafuegos) son barreras de seguridad implementadas cuando se utiliza el protocolo IP en el borde de una red, estas barreras filtran el tráfico de la red con propósitos de seguridad.

El BG Border Gateway (Gateway de Frontera) es un Gateway que se utiliza para establecer conexión con otra red de paquetes externa, con la cual se poseen servicios de roaming. Todas las redes que brindan servicios de roaming entre si, se conectan a un punto en común llamado GRX GPRS Roaming Exchange (Intercambio de Roaming GPRS).

El CGW Charging Gateway (Gateway de Tarificación) recopila los datos de tarificación del dominio PS y los envía al centro de facturación para su procesamiento.

El IMS, se le denomina subsistema porque es parte del dominio PS, éste es una plataforma de servicios multimedia. En las interfaces Gn y Gp se implementa el protocolo de transporte GTP-U GPRS Tunelling Protocol - User´s Plane (Protocolo para Túneles de GPRS - Plano de Usuario) para el plano de usuario y GTP-C GPRS Tunelling Protocol - Control´s Plane (Protocolo para Túneles de GPRS - Plano de Control) para el plano de control.

Figura 2.7 Dominio PS del núcleo de red (CN)



- **Identidades de usuarios manejadas por el CN**

El CN maneja varios tipos de identidades las cuales son utilizadas para diferenciar los servicios y el dominio en el que se brindan. Las identidades utilizadas:

- El IMSI[34]. Está formado por tres componentes: MCC + MNC + MSN. El MCC[35] Mobile Country Code (Código del País Móvil) conformado por tres dígitos, el MNC Mobile Network Code (Código de Red Móvil) posee un dígito y el MSN que es el número del abonado móvil son siete dígitos. Este número se almacena en la USIM y es utilizado como clave única de búsqueda en la base de datos de los registros HLR, VLR, AuC y SGSN.

[34] En base a la recomendación ITU-T E.214
[35] En base a la recomendación ITU-T E.214, E.160 y E.164

- El MSISDN[36] Mobile Subscriber ISDN (Número ISDN de Suscriptor Móvil) es el número utilizado para la diferenciación de servicios y el establecimiento de las llamadas con el dominio CS, un abonado puede tener varios números MSISDN para diferentes servicios de CS. Se divide en tres partes: CC + NDC + SN. El CC[37] Country Code (Código de País) es de 1 a 3 dígitos, NDC National Destination Code (Código del País Destino) es de 1 a 3 dígitos y el SN Subscriber Number (Número de Abonado), que es variable dependiendo de cada país.
- El MSRN[38] Mobile Station Subscriber Roaming Number (Número de Roaming de Abonado Móvil). Se utiliza para que el GMSC envié información de encaminamiento de las llamadas al servidor MSC, también se emplea para la conexión entre dos MSC/VLR cuando se produce un handover.
- La TMSI. Por motivos de seguridad, la IMSI no se debe transferir siempre que sea posible, en lugar de ella se utiliza una identidad temporal llamada TMSI la cual se utiliza en el dominio CS y es asignada desde el VLR. En el dominio PS se utiliza la P-TMSI Packet TMSI (TMSI para Paquetes) y es asignada desde el SGSN.
- El IMEI está compuesto por tres partes: TAC + SNR + Libre. TAC Type Allocation Code (Código de Asignación de Tipo) lo define el fabricante y el tipo de teléfono y el SNR Serial Number (Número de Serie) es el número de serie del teléfono. Este número es gestionado desde el EIR y no se puede alterar ya que está grabado en el hardware del teléfono.

El nombre del dominio de la red base IMS tiene una estructura que se ajusta con la propuesta para Internet: «Ims.mnc#.mcc#.3gppnetwork.org»

[36] En base a la recomendación ITU-T E.164
[37] En base a la recomendación ITU-T E.214
[38] En base a la recomendación ITU-T E.164

En donde el primer numeral corresponde al número MNC obtenido del IMSI del usuario y el segundo es el número MCC obtenido también del IMSI. La identidad de usuario privada para el IMS es la identidad que el usuario utiliza para conectarse de forma local en la red móvil y tiene el siguiente formato:

«IMSI@dominio»

En dónde, «IMSI» es el número IMSI y el «dominio» es el dominio de la red base. La identidad de usuario pública para el IMS es la identidad que utiliza el usuario para conectarse a una red externa como Internet, es por ello que tiene el formato URI Universal Resource Identifier (Identificador Universal de Recursos) de SIP Session Initiation Protocol (Protocolo de Inicio de Sesión):

«nombre.apellido@operador.com»

- **Gestión de movilidad (MM)**

La gestión de la movilidad para el dominio CS es llamada MM y para el dominio PS es llamada PMM Packet MM (MM de Paquetes).

- MM en modo CS: Desde el punto de vista de la movilidad, el UE puede encontrarse en tres estados: desconectado de la MM, en estado de reposo y conectado a la MM. Cuando el terminal esta desconectado de la MM, la red no tiene ningún conocimiento del terminal (terminal apagado). En estado de reposo, la red conoce la ubicación del terminal con la precisión de una LA. Una LA es el área en donde el UE puede moverse sin necesidad de actualizar su ubicación en el VLR. En el estado conectado a MM, la red conoce la ubicación del terminal con la precisión de una célula. Cuando un terminal se enciende, éste envía un mensaje «IMSI Attach» con el cual le comunica a la red que se encuentra activo y a su vez actualiza su posición, cuando se apaga el terminal se cambia del estado de reposo a

desconectado y cuando se inicia una llamada se cambia del estado de reposo a conectado.

- MM en modo PS: Para la PMM, los estados son los mismos pero desencadenan otros procedimientos. En el estado desconectado con la PMM la red no tiene información de encaminamiento válida para las conexiones PS. Cuando el terminal es encendido, éste envía un «IMSI Attach» adjunto para paquetes, éste posee un gran volumen de información que actualiza al SGSN y al GGSN, actualizando también la información de encaminamiento. En el estado de conexión a la PMM, se puede transferir información de señalización entre el terminal y la red. En el estado de reposo, tanto la red y el terminal poseen información de encaminamiento válida y están preparados para transmitir datos.

- **Gestión de Comunicación**

La gestión de comunicación en el dominio CS es conocida como CM, y en el dominio PS es conocida como SM Session Management (Gestión de Sesión).

- Gestión de Comunicación en modo CS: Está constituida por tres fases: En la primera fase, el conmutador comprueba si se puede acceder al número llamado o si existe algún tipo de restricción aplicada al abonado llamante. En la segunda fase, el sistema analiza la naturaleza de la transacción y determina si se trata de una llamada internacional o nacional, luego el sistema comienza a determinar posibles canales de conexión hacia el destino deseado con la ayuda de protocolos de señalización (por ejemplo: ISUP), luego de esto, se encamina la llamada a su destino. En la tercera fase se liberan todos los circuitos que fueron empleados para el establecimiento de la llamada, una vez finalizada.
- Gestión de sesiones en el modo PS: En el dominio PS las conexiones de paquetes se conocen como sesiones. El SM es una entidad lógica que

puede encontrarse en dos estados: activo o inactivo. Al protocolo utilizado para la transferencia de datos por paquetes se le denomina PDP, que usualmente es IP, son válidos pero poco frecuentes los protocolos como X.25.

La frase «contexto PDP» se utiliza para designar el conjunto de atributos y parámetros de la conexión de datos por paquetes de acuerdo con la QoS seleccionada. Por ejemplo: un contexto PDP guarda direcciones IP asignadas, el tipo de conexión y las direcciones IP de los elementos de red. Cuando un UE solicita una conexión por paquetes a la SM pasa del estado inactivo al activo y crea un contexto PDP basándose en la QoS negociada.

2.2.5 Subsistema Multimedia IMS

El IMS es un elemento que forma parte del dominio PS del CN y posee las siguientes características:

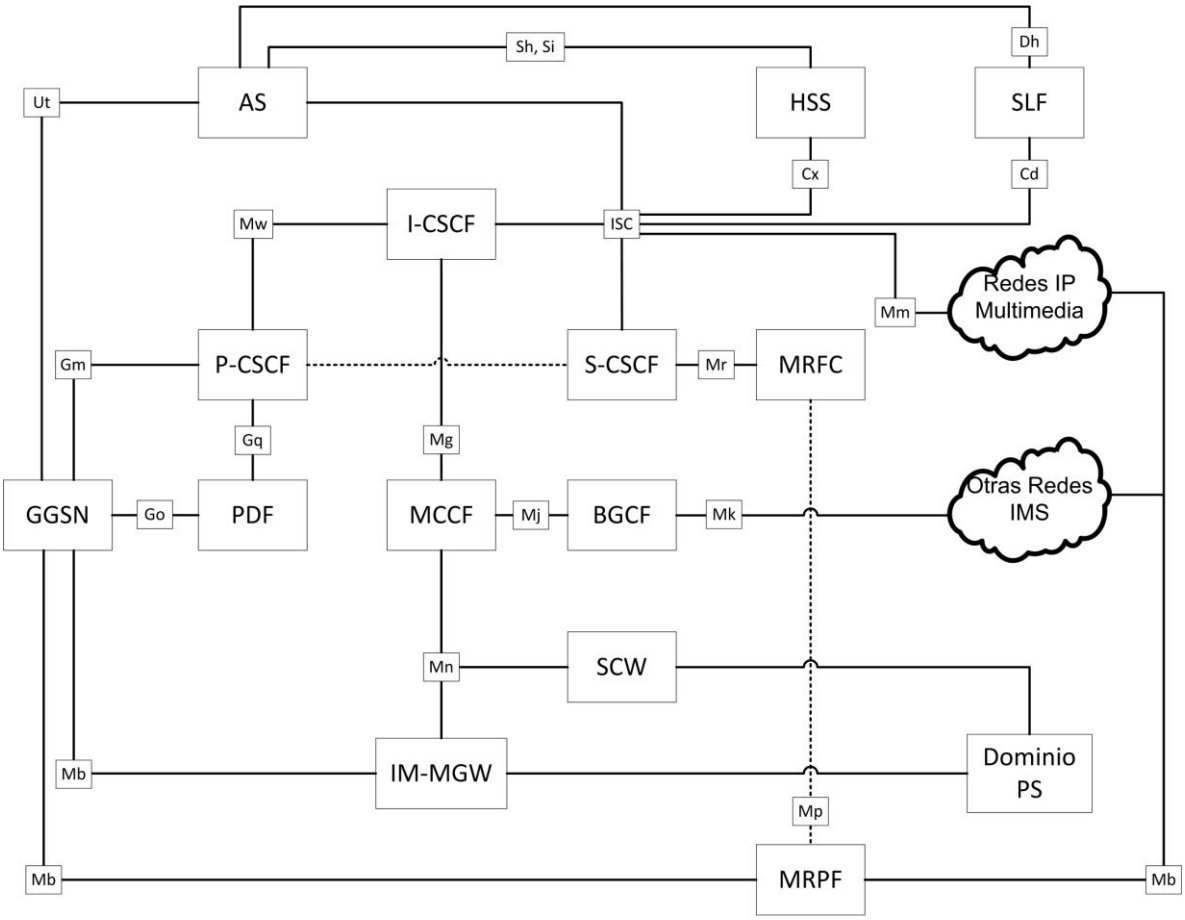
- Conectividad IP.
- Calidad de Servicio.
- Control de las Políticas sobre IP.
- Comunicaciones Seguras.
- Posibilidad de roaming.
- Interconexión con otras Redes.
- Desarrollo y Control de servicios para aplicaciones basadas en IP.

Además de estas características está diseñado para trabajar con IPv6, ya que no tiene limitación de direcciones, aunque en las primeras versiones puede trabajar con IPv4 por motivos de compatibilidad. También al igual que el dominio CS y PS, se establece una separación entre el plano de usuario y el plano de control, es

decir, la señalización se maneja por separado del tráfico de usuario, además de poseer un plano de aplicaciones. La señalización de este subsistema se realiza con el protocolo SIP debido a su simpleza y flexibilidad con algunos protocolos similares.

La estructura del subsistema IMS se muestra en la Figura 2.8.

Figura 2.8 Estructura del Subsistema Multimedia IMS



El IMS posee también las siguientes entidades y funcionalidades:

- **CSCF**

Existen tres diferentes tipos de CSCF Call Session Control Function (Funciones de Control de Sesión de Llamada): las P-CSCF Proxy CSCF (Proxy CSCF), S-CSCF Server CSCF (Servidor CSCF) y las I-CSCF Interrogatory CSCF (Interrogadoras CSCF).

La P-CSCF, es el punto por el cual pasa todo el tráfico SIP. Este elemento tiene a cargo cuatro funciones: la comprensión de los mensajes SIP, la SA Security Association (Asociación de Seguridad) de IPSec IP Security (Seguridad IP), la interacción con las PDF Policy Decisión Function (Funciones de Decisión de Políticas) y la detección de sesiones de emergencias. La P-CSCF es la responsable de mantener las SA y solicitar la confidencialidad y protección de los mensajes SIP, además, envía a la PDF la información relativa a las sesiones y servicios multimedia. La PDF en base a esta información obtiene la QoS y la envía al GGSN, una vez obtenida la QoS se decide la activación de un contexto PDP para establecer la conexión.

La I-CSCF, es el punto de contacto en la red del operador para todas las conexiones destinadas a un abonado de ese operador. Cumple con las siguientes funciones:

- Obtener el nombre de la S-CSCF del HSS.
- Asignar una S-CSCF en función de las capacidades recibidas del HSS.
- Encaminar solicitudes entrantes a una S-CSCF asignada.

La S-CSCF, es el punto central del IMS, puesto que es la encargada del proceso de registro y de tomar las decisiones de encaminamiento. La S-CSCF descarga el perfil de usuario del HSS que está asociado a la identificación pública del usuario. Basándose en esto, decide cuando y a que AS Application Server (Servidor de Aplicaciones) debe contactarse cuando el usuario envíe una solicitud SIP.

- **Bases de Datos**

Existen dos tipos de bases de datos en el IMS: el HSS y el SLF Subscriber Location Function (Función de Localización de Suscriptores).

El HSS contiene información de servicios y abonados del IMS, entre los datos más importantes se incluyen las identidades de usuario, la información de registro, los parámetros de acceso y la información de servicios.

El SLF sirve como mecanismo de resolución, que permite al I-CSCF, S-CSCF y al AS encontrar la dirección del HSS en situaciones donde existan varios HSS.

- **Función de interconexión**

La función de interconexión se realiza entre el IMS y el dominio CS del CN. El S-CSCF envía una solicitud SIP a la BGCF Breakout Gateway Control Function (Función de Control de Gateway de Interrupción), este decide en que momento debe realizarse la interrupción en el dominio CS. En este punto las opciones pueden ser dos: interrumpir en otra red o en la misma; sí es en otra red, la solicitud SIP es enviada al BGCF de la otra red; sí es en la misma, el BGCF selecciona una MGCF Media Gateway Control Function (Gateway Multimedia de Control de Funciones) el cual convierte la señalización SIP en una compatible con el dominio CS como lo son los protocolos ISUP o BICC; luego pasa la señalización al SGW Signalling Gateway (Gateway de Señalización) el cual la convierte a nivel de transporte. Como el tráfico de señalización se produce en los dos sentidos el SGW utiliza SCTP Stream Control Transport Protocol (Protocolo de Transporte de Control de Stream[39]) para el IMS y MTP/SS7 para la red del dominio CS. Al mismo tiempo el MGCF interactúa con el IMS-MGW IMS Media Gateway (Gateway Multimedia IMS) el cual reserva los recursos para el plano de usuario.

[39] El término “stream” hace referencia a una transmisión continua.

- **Funciones de servicios**

Existen tres funciones relacionadas con los servicios del IMS: el MRFC Multimedia Resource Function Controller (Controlador de Funciones de Recursos Multimedia), el MRFP Multimedia Resource Function Processor (Procesador de Funciones de Recursos Multimedia) y los AS.

El MRFC es el responsable de la comunicación SIP desde y hacia el S-CSCF y del control del MRFP. El MRFP proporciona los recursos de plano de usuario que solicita y ordena el MRFC. Además, se encarga del procesamiento de streams de datos multimedia como la codificación de sonido y el análisis multimedia.

Los AS son las entidades que proporcionan los servicios multimedia de valor agregado, éstos pueden ofrecer servicios SIP AS, servicios basados en entornos CAMEL Customized Application for Mobile Network Enhanced Logic (Aplicaciones Personalizadas para Lógica Mejorada de Redes Móviles) y servicios OSA Open Services Architecture (Arquitectura Abierta de Servicios).

- **Función de Soporte.**

Aquí se reconocen tres entidades: la PDF, la SEG Security Gateway (Gateway de Seguridad) y la THIG Topology Hiding Interworking Gateway (Gateway de Interworking para Ocultar la Topología).

La interacción global entre GPRS e IMS se conoce como SBLP Service Based Local Politic (Política Local Basada en Servicios), la PDF es el que toma las decisiones de las SBLP. El P-CSCF envía la información de solicitud de conexión de un UE a la PDF, el cual a su vez envía información al P-CSCF sobre la autorización de los flujos IP y de los componentes multimedia elegidos, además de los parámetros QoS de IP autorizados para su trasferencia al GGSN.

La SEG tiene la función de proteger el tráfico del plano de control que existe en los dominios de un operador. Todo el tráfico del IMS es encaminado a través de la

SEG, especialmente cuando el tráfico origen y destino están en diferentes dominios.

La THIG se emplea para ocultar la configuración, la capacidad y la topología de la red al exterior. Un operador que desea ocultar su red, coloca un THIG en la ruta de encaminamiento cuando recibe y envía información de otras redes IMS. El THIG cifra y descifra todas las cabeceras que revelan información sobre la topología de la red IMS.

2.3 TECNOLOGÍA DE UMTS

El concepto de una red UMTS hace referencia a una combinación de tecnologías que permiten la integración entre redes fijas y móviles, así como la convergencia de los sistemas de comunicación móvil de segunda generación. La convergencia, es uno de los principales objetivos de UMTS como tecnología de tercera generación. Es importante señalar que la tecnología de acceso WCDMA es la tecnología de acceso de UMTS y que brinda la capacidad de trasferir paquetes de datos a altas velocidades.

2.3.1 WCDMA

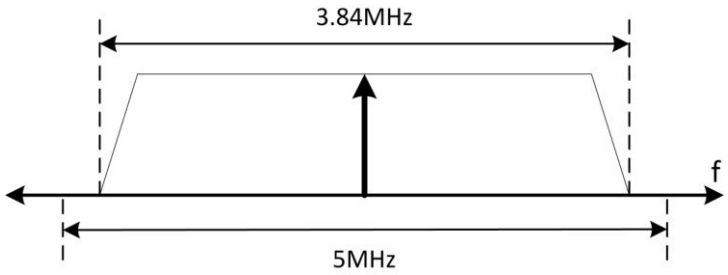
WCDMA es una tecnología derivada del CDMA tradicional utilizado en las redes IS-95[40]. Las principales diferencias entre ambas tecnologías, es que WCDMA utiliza una señalización y un canal de control diferente así como un mayor ancho de banda (5 MHz) para su funcionamiento, el cual lo provee de la capacidad para transmitir datos a velocidades de hasta 2 Mbps.

Esta tecnología emplea una técnica de ensanchamiento, es decir, la señal de datos es ensanchada para que ocupe todo el ancho de banda asignado para la

[40] Interim Standard 95 (Estándar Interino 95) es un estándar de telefonía móvil celular basado en tecnología CDMA. También conocido por su denominación comercial «cdmaOne».

transmisión. Este ensanchamiento se realiza con un código de ensanchamiento específico para cada usuario, con el cual se establece la diferencia entre cada usuario conectado a la red. Este procedimiento es llamado DS-WCDMA Direct Sequence WCDMA (WCDMA de Secuencia Directa).

Figura 2.9 Ancho de banda de WCDMA



- **Spreading y Despreading para la tecnología WCDMA**

Básicamente el funcionamiento de WCDMA es el siguiente: la información a transmitir es multiplicada por un código, el resultado de esta multiplicación produce una señal de mayor ancho de banda, específicamente de 3.84MHz, que representa el ancho de banda asignado para la transmisión en modo FDD-WCDMA, a este procedimiento se le denomina «Spreading». El receptor capta la señal ensanchada y la sincroniza con el mismo código que se utilizó para la transmisión, el resultado será: la información transmitida más algunos armónicos de alta frecuencia que no forman parte de la información y que pueden ser filtrados con facilidad, a este procedimiento se le denomina «Despreading».

El Spreading y el Despreading son realizados tanto por el Nodo B como por el teléfono móvil, debido a que la información transita en dos sentidos, uno desde el teléfono hacia el Nodo B (Uplink) y otro desde el Nodo B al teléfono (Downlink).

- **Chips**

Un concepto utilizado en WCDMA es el «chip», que corresponde a los bits utilizados en el código de pseudorruido conocido como código de ensanchamiento. La velocidad del código de ensanchamiento no se expresa en bits/ segundos (b/s), sino en chips/s (chips por segundo), de tal forma que la velocidad del código de ensanchamiento es de 3.84 Mchips/s que es lo necesario para que la señal de datos se ensanche a los 3.84MHz. La velocidad de códigos es conocida como SCR System Chips Rate (Tasa de Chips del Sistema).

- **Símbolos**

Los símbolos dependen de la modulación. Un símbolo es un elemento de transmisión como resultado de una modulación. Las modulaciones utilizadas en WCDMA son QPSK Quadratur Phase Shift Keying (Modulacion por Desplazamiento de Fase en Cuadratura) para el enlace descendente, en el cual se utilizan cuatro símbolos para la transmisión, de acuerdo a la siguiente ecuación:

$$2^{(\text{bits/simbolos})} = \text{símbolos utilizados por la modulación} \qquad (2.1)$$

Por tanto, se pueden generar combinaciones de dos bits por símbolo 2^2=4, es decir, se transmiten dos bits por cada símbolo. Para el enlace ascendente se utiliza Dual QPSK el cual utiliza dos símbolos para la transmisión, se transmite un bit por cada símbolo (2^1=2), a continuación se muestra en la Tabla 2.1 la relación de los símbolos.

Tabla 2.1 Relación de símbolos entre QPSK y Dual QPSK

QPSK	
Símbolos	**Combinaciones de bits**

A	00
B	01
C	10
D	11

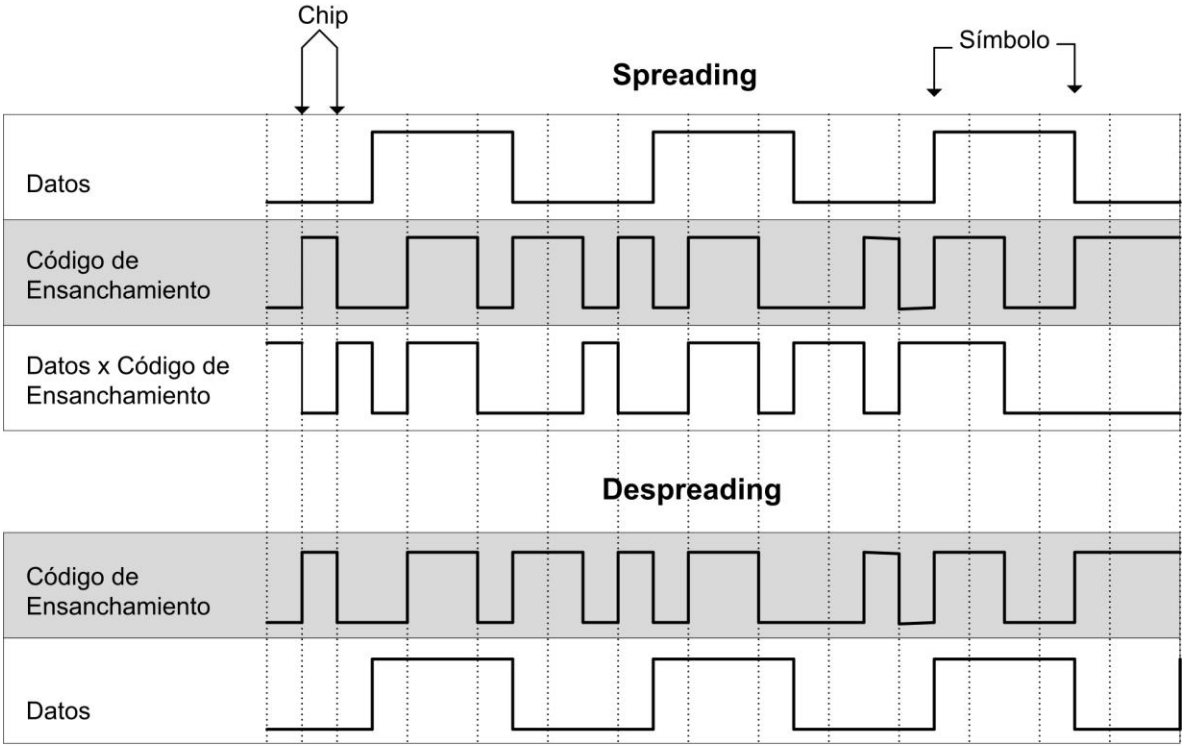
Dual QPSK	
Símbolos	**Combinaciones de bits**
A	0
B	1

De forma más específica, el ensanchamiento de la señal de datos binarios se realiza sobre los símbolos generados por éstos, como se muestra en la Figura 2.10, en donde se observa que el chip es la unidad de información del código de ensanchamiento. El código de ensanchamiento y los símbolos generados por los datos entran a una compuerta XNOR, en la cual sí los valores de entada son iguales el resultado es un «1» lógico y si son diferentes se genera un «0» lógico. El resultado de este procedimiento genera una señal cuya velocidad es de 3.84 MChips/s, que es la capacidad que posee el canal. En la Figura 2.10 también se observa el proceso de «Spreading» y «Despreading».

- **El código de ensanchamiento**

Un código de ensanchamiento es utilizado para diferenciar la información de cada usuario en el trayecto radioeléctrico, este código es asignado por la red al usuario antes de una transmisión de tal forma que ambos lo conocen y lo utilizan para la separación de la información. Este código de ensanchamiento está compuesto de un código de aleatorización y un código de canalización.

Figura 2.10 Procedimiento de Spreading y Despreading en WCDMA



El código de ensanchamiento es empleado para diferenciar al usuario en una misma banda de frecuencia y el código de canalización es utilizado para diferenciar los canales de datos y de control utilizados en WCDMA. El código de ensanchamiento se expresa mediante la siguiente ecuación:

$$\text{Cod. de ensanchamiento} = \text{Cod. de canalización} + \text{Cod. de aleatorización} \qquad (2.2)$$

- **Factor de ensanchamiento**

El factor de ensanchamiento es una cifra que describe el número de chips por cada símbolo utilizado para el ensanchamiento de la señal, se representa de la siguiente forma:

$$\text{Factor de ensanchamiento} = \frac{\text{tasa de chips del sistema}}{\text{símbolos generados por los datos}} \qquad (2.3)$$

En donde, la tasa de bits del sistema es igual a 3.84MChips/s y en los datos se contempla información adicional como señalización y control, además, se debe tener en cuenta que los símbolos generados por los datos son diferentes en dirección descendente que en dirección ascendente, ya que un símbolo es igual a un bit en dirección ascendente y en dirección descendente un símbolo es igual a dos bits. A continuación se muestra la Tabla 2.2 con las velocidades de datos, símbolos y su factor de ensanchamiento.

Tabla 2.2 Relación entre factor de ensanchamiento, símbolos y velocidad de transmisión para el uplink.

Factor de ensanchamiento	Tasa de símbolos generados por los datos (KSímbolos/s)	Velocidad del canal (Kb/s)
256	15	15
64	60	60
16	240	240
4	960	960

Tabla 2.3 Relación entre factor de ensanchamiento, símbolos y velocidad de transmisión para el downlink.

Factor de ensanchamiento	Tasa de símbolos generados por los datos (KSimbolos/s)	Velocidad del canal (Kb/s)
256	15	30
64	60	120
16	240	480
4	960	1920

Como se puede observar en la Tabla 2.2 y Tabla 2.3, a mayor velocidad binaria el factor de ensanchamiento será menor, es decir, requerirá menos chips por símbolos para ensanchar la señal.

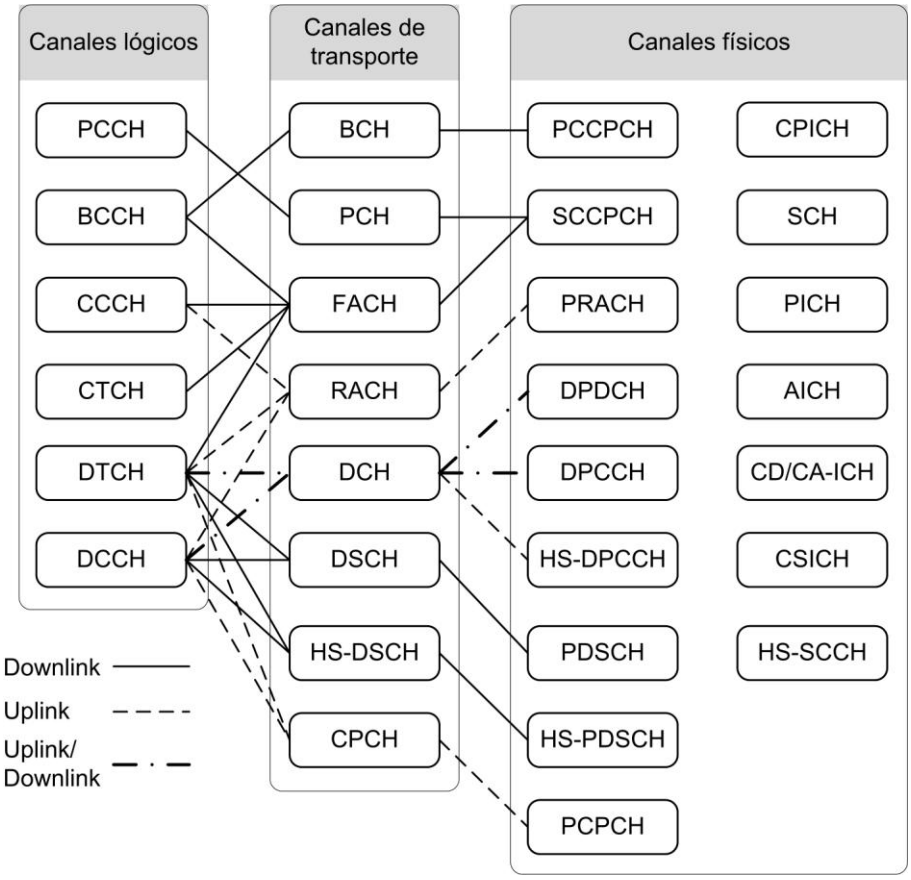
Con ello, se pueden deducir algunas características de la tecnología WCDMA, las cuales son esenciales en el aspecto de la transmisión: la información a transmitir requiere de una mayor cantidad de potencia si la información a transmitir es mayor, en el contexto técnico significaría que a mayor velocidad binaria mayor potencia. Lo anterior, relacionado con el factor de ensanchamiento denota que dicho factor es inversamente proporcional a la potencia, debido a que cuanto menor sea el factor de ensanchamiento mayor es la velocidad de transmisión y por ende mayor es la potencia utilizada para la transmisión.

- **Canales radioeléctricos de WCDMA**

Los canales radioeléctricos en WCDMA son los encargados de gestionar el ancho de banda asignado a cada usuario de la red, por medio de éstos se proprocionan funciones de control para el teléfono móvil e información de aplicación. Hay tres tipos de canales en WCDMA: los canales lógicos, los canales de transporte y los canales físicos.

Los canales lógicos describen el tipo de información que se transmite, los canales de transporte describen como se transfieren los canales lógicos y los canales físicos son el medio radioeléctrico por el cual se transmite la información, esto quiere decir, que dentro de los canales físicos se encuentran los canales de transporte. Desde el punto de vista de la red, el Nodo B administra los canales físicos ya que se encarga de proveer la interfaz radioeléctrica y el RNC Radio Network Controller (Controlador de Red de Radio) administra los canales de transporte y los canales lógicos.

Figura 2.11 Canales radioeléctricos de WCDMA y la relación entre ellos.



Los canales lógicos son un conjunto de tareas que la red debe realizar en un determinado momento, es decir, cada canal lógico representa una tarea. Los canales lógicos son los siguientes:

- BCCH Broadcast Control Channel (Canal de Control de Difusión): a través de este canal se le informa al teléfono móvil lo que está pasando en el entorno radioeléctrico, como por ejemplo: los valores de los códigos utilizados en su célula y las células adyacentes, los niveles de potencia permitidos, etc.
- PCCH Paging Control Channel (Canal de Control de Localización): La localización es un sistema mediante el cual se puede ubicar la posición de un teléfono móvil, esto es necesario cuando se quiere establecer una

llamada con un determinado teléfono móvil y no se conoce su posición, para la localización del teléfono móvil se utiliza este canal.

- CCCH Common Control Channel (Canal de Control Común): es un canal de control que puede ser utilizado simultáneamente por varios usuarios de una célula, por tal motivo, cada teléfono móvil se debe identificar con una U-NRTI UTRAN - Network Radio Temporal Identity (Identidad Temporal de Red de Radio UTRAN) para que pueda ser diferenciado por la red.
- DCCH Dedicated Control Channel (Canal de Control Dedicado): por este canal se envía información de control, pero a diferencia del CCCH este canal sólo puede ser utilizado por un usuario.
- DTCH Dedicated Traffic Channel (Canal de Tráfico Dedicado): por este canal se transmite el tráfico dedicado para los servicios de usuarios.
- CTCH Common Traffic Channel (Canal de Tráfico Común): es un canal que trasmite tráfico en dirección descendente para un conjunto de usuarios de una misma célula.

Los canales de transporte son los siguientes:

- BCH Broadcast Channel (Canal de Difusión): es un canal descendente que transporta el contenido del BCCH. Éste es transmitido con una potencia relativamente alta ya que todos los teléfonos móviles lo deben escuchar.
- PCH Paging Channel (Canal de Localización): es un canal descendente que transporta el contenido del canal PCCH, es decir, la información de radiobúsqueda o localización.
- FACH Forward Access Channel (Canal de Acceso Directo): es un canal descendente que transporta información de control, es decir, transporta a los canales lógicos BCCH y CCCH. Una célula posee múltiples canales

FACH, pero siempre hay uno configurado a baja velocidad binaria para que todos los terminales puedan recibirlo.

- DCH: es un canal bidireccional que transmite tráfico y control dedicado, es decir, transporta los canales lógicos DCCH y DTCH. Un DCH puede albergar varios DTCH, por ejemplo: cuando un usuario tiene activa una llamada de de voz y una llamada de video simultáneamente, ya que cada llamada requiere un DTCH.
- DSCH Downlink Shared Channel (Canal Compartido Descendente): es un canal descendente opcional que transporta información dedicada, es decir, a los canales lógicos DCCH y DTCH. Este canal lo pueden compartir varios usuarios, por lo tanto, es mejor que el DCH porque ahorra recursos de red en dirección descendente. Además, este canal puede aumentar de velocidad convirtiéndose en HS-DSCH.
- RACH Random Access Channel (Canal de Acceso Aleatorio): es un canal de dirección ascendente que transporta información de control, por ejemplo: solicitudes de establecimiento de conexión, por lo que alberga al canal lógico CCCH en sentido ascendente, además, transporta pequeñas ráfagas de datos por paquetes por lo que trabaja con el DTCH.
- CPCH Common Packet Channel (Canal de Paquetes Común): es un canal de transporte común en dirección ascendente destinado a la transmisión de paquetes, trabaja con el DTCH y el DCCH para dicho fin. Sí la capacidad para la transmisión de datos del canal RACH no es suficiente, se puede utilizar el CPCH.

Los Canales físicos son los siguientes:

- P-CCPCH Primary Commom Control Phisical Channel (Canal Físico de Control Común Primario): este canal transporta al BCH en dirección descendente, todos los terminales pueden demodular y escuchar este

canal ya que utiliza un código de canalización fijo, su velocidad binaria es de 30Kbps y se transmite con una potencia relativamente alta para que pueda ser escuchado por todos los usuarios de la célula.

- S-CCPCH Secundary Commom Control Phisical Channel (Canal Físico de Control Común Secundario): incluye los canales de transporte PCH y FACH. La velocidad binaria de este canal es fija y relativamente baja, además es transmitido con una potencia alta, su configuración es variable y está relacionada con el rendimiento que se desee en el sistema.
- PRACH Packets Random Access Channel (Canal de Acceso Aleatorio por Paquetes): éste utiliza el canal de transporte RACH y la información relacionada con el RAP Random Access Procedure (Procedimiento de Acceso Aleatorio). Mediante este canal el usuario envía una solicitud de acceso a la red.
- DPDCH Dedicated Phisical Data Channel (Canal de Datos Físico Dedicado): este canal transporta el tráfico dedicado de usuario en dirección descendente y ascendente, es decir, transporta la parte de tráfico de usuario del canal de transporte DCH. Es de longitud variable y en WCDMA modo FDD posee un factor de ensanchamiento máximo de 4, en el modo TDD el factor de ensanchamiento máximo es de 1. Un terminal móvil puede utilizar varios canales DPDCH para aumentar la capacidad de su conexión, esto se produce con la ayuda de los multi-códigos con lo cual se asigna un código para cada canal DPDCH.
- DPCCH Dedicated Phisical Control Channel (Canal de Control Físico Dedicado): este canal transporta información dedicada de control perteneciente al usuario, es decir, transporta la parte de control del canal de transporte DCH.

- HS-DPCCH High Speed DPCCH (DPCCH de Alta Velocidad): es un canal que cumple las mismas funciones que el DPCCH pero con velocidades más altas.
- PDSCH Phisical Downlink Shared Channel (Canal Fisco Compartido Descendente): éste contiene al canal de transporte DSCH, por lo tanto, es opcional así como el DSCH.
- HS-PDSCH High Speed PDSCH (PDSCH de Alta Velocidad): es un canal descendente que transporta al HS-DSCH con un factor de ensanchamiento de 16, mediante este canal se alcanzan velocidades altas para el enlace descendente del usuario.
- PCPCH Phisical Comunication Packets Channel (Canal Físico de Paquetes de Comunicación): éste contiene al canal de transporte ascendente CPCH que es utilizado cuando la capacidad del canal RACH no es suficiente.
- CPICH: este canal se utiliza para las estimaciones que realiza el terminal de los canales dedicados y para proporcionar referencias de los canales cuando intervienen canales comunes. Normalmente un célula solo tiene un CPICH, pero puede tener hasta dos, en este caso reciben el nombre de CPICH primario y secundario. Los terminales escuchan continuamente el CPICH, por lo tanto, es utilizado para el handover y para equilibrar la carga de la célula. El ajuste del nivel de potencia del CPICH equilibra la carga de la célula, debido a que el terminal busca la célula con el nivel de potencia del CPICH más alto.
- SCH Synchronization Channel (Canal de Sincronización): éste es la combinación de dos canales el P-SCH Primary SCH (SCH Primario) y el S-SCH Secondary SCH (SCH Secundario). El P-SCH utiliza un código de canalización fijo para que los terminales puedan acceder a él fácilmente, una vez que el terminal accede a este canal y lo demodula ha conseguido

sincronizarse con las tramas del sistema y posteriormente conocerá los códigos de aleatorización que utilizará para la transmisión.

- PICH Paging Indicador Channel (Canal Indicador de Localización): este canal transmite información de localización al terminal.
- AICH Acquisition Indicador Channel (Canal de Indicación de Adquisición): es un canal descendente mediante el cual la red confirma al usuario que se ha recibido satisfactoriamente su solicitud para el acceso a la red.
- CA-ICH CPCH Assignment Indicador Channel (Canal de Asignación CPCH): este canal indica la asignación de canales CPCH.
- CD-ICH Collition Detection Indicador Channel (Canal Indicador de Detección de Colisiones): éste transfiere al terminal móvil la información sobre la detección de colisiones.
- CSICH CPCH Status Indicador Channel (Canal Indicador de Estado del CPCH): éste informa sobre la existencia y configuración del CPCH.
- HS-SCCH High Speed Syncronization Channel (Canal de Control de Sincronismo de Alta Velocidad): es un canal de sincronismo de alta velocidad.

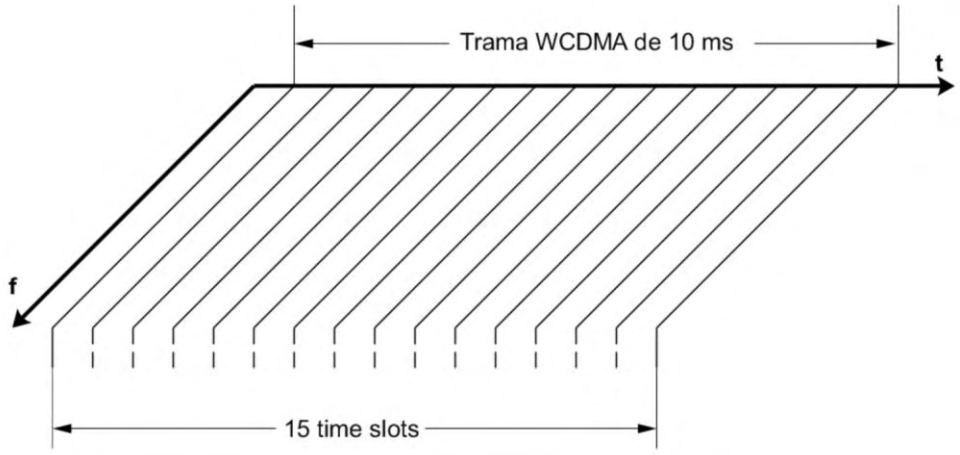
- **Estructura de trama para WCDMA**

La trama de WCDMA es la encargada de organizar los canales físicos antes descritos para que se puedan establecer de forma ordenada y estructurada las conexiones de control y tráfico de datos entre el terminal móvil y la red. Se puede inferir, que en las tramas se albergan los canales físicos y que a las tramas se les aplica la tecnología WCDMA para el acceso a los canales radioeléctricos.

La estructura de trama de WCDMA es de 10ms y está dividida en 15 timeslots. Sabiendo que la capacidad del sistema es de 3.84 MChips/s en 10ms se

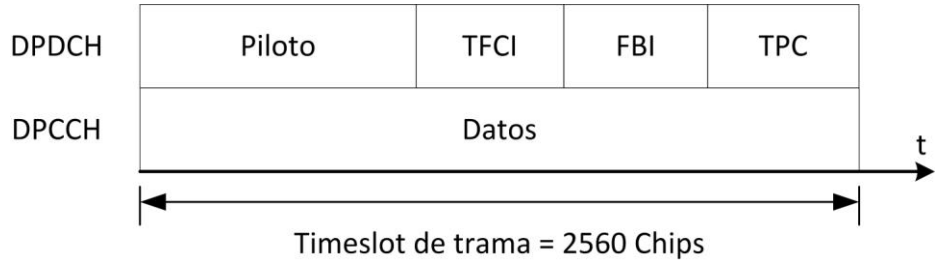
entregaran 38,400 Chips, que es el tamaño de la trama WCDMA, de esta forma cada timeslot es de 2,560 Chips.

Figura 2.12 Trama de WCDMA



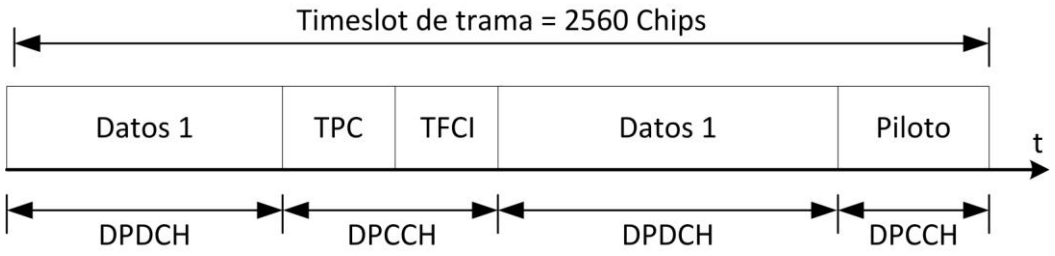
La conexión directa al terminal móvil se realiza a través de los canales dedicados de control DPCCH y de datos DPDCH, a estos dos canales se les asigna un timeslot para la transmisión. El DPCCH está dividido en tres partes: la primera parte está compuesta por bits piloto que se utilizan para ofrecer estimaciones del canal que permitan una capacidad de detección coherente, otro segmento llamado TPC Transmission Power Control (Control de Potencia de Transmisión) que se emplea para ajustar la potencia de transmisión, el FBI Feedback Information (Información de Retroalimentación) y el TFCI Transport Format Combination Indicator (Indicador de la Combinación del Formato de Transporte) que proporcionan la información sobre los canales de transporte multiplexados en el DPDCH. Por otro lado, el DPDCH lleva el flujo de datos correspondiente a la conexión establecida. Estos canales en dirección ascendente se encuentran separados por un código en el propio timeslot, es decir, son transmitidos en forma paralela.

Figura 2.13 Intervalo y trama para el DPDCH y DPCCH uplink.



En dirección descendente estos dos canales físicos se encuentran multiplexados en el tiempo en el propio timeslot como se ve en la Figura 2.14.

Figura 2.14 Intervalo y trama para el DPDCH y DPCCH downlink



Al resto de canales físicos se les asigna un timeslot para la transmisión.

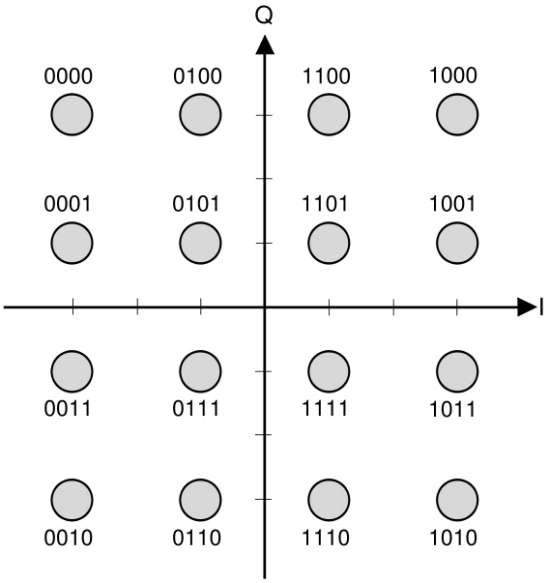
2.3.2 HSDPA

El HSDPA es una mejora de la interfaz aérea de WCDMA que provee una mayor capacidad de transmisión para el enlace descendente y la posibilidad de desarrollar nuevos servicios que requieran altas tasas de transferencia.

Originalmente, para el flujo de transmisión al usuario se utilizaban los canales de transporte DCH y el DSCH. Cuando se trataba de bajas velocidades se podía recurrir al canal FACH, para HSDPA se creó el canal de transporte HS-DSCH para

el transporte de la información de usuario. Sobre el HS-DSCH se introducen una nueva modulación denominada 16QAM que brinda una mejor optimización del canal de transferencia, esta modulación por ser multifasorial posee una baja relación S/N Signal/Noise (Señal/Ruido), es decir, que es susceptible a las interferencias producidas en el trayecto radioeléctrico. Para corregir este problema se implementan muevas técnicas de corrección de errores como: la AMC Adaptive Modulation and Coding (Modulación y Codificación Adaptativa) y la HARQ Hybrid Automatic Repead Request (Solicitud de Retransmisión Automática Hibrida).

Figura 2.15 Diagrama fasorial de 16QAM



Como se puede observar en la Tabla 2.4, el HS-DSCH posee un factor de ensanchamiento fijo de 16, puede utilizar la modulación 16QAM o QPSK. Además, posee la capacidad de realizar handover con un canal DCH de la misma interfaz, su TTI es de 2ms, esto quiere decir, que el canal transfiere información cada 3 timeslots garantizando un menor retardo de transmisión que los demás canales. También, en este canal se pueden utilizar hasta 15 multicódigos, es decir, 15

canales de transporte HS-DSCH paralelos para un sólo usuario y cada canal se identifica con un código para lograr una transferencia mayor a los 10Mbps.

Tabla 2.4 Comparación entre los distintos canales de transporte utilizados para la transmisión, incluyendo el HS-DSCH para HSDPA.

Canal	HS-DSCH	DSCH	DCH descendente	FACH
Factor de ensanchamiento	Fijo 16	Variable (256~4)	Fijo (521 ~ 4)	Fijo (256 ~ 4)
Modulación	QPSK / 16QAM	QPSK	QPSK	QPSK
Control de potencia	Fijo /lento	Basado en DCH	Rápido, ciclo de control: 1500/s	Fijo/lento
TTI[41]	2ms	10 ~ 80ms	10 ~ 80ms	10 ~ 80ms
Codificación	código turbo	código turbo y convolucional	código turbo y convolucional	código turbo y convolucional
Soft handover	cambiar a un DCH	cambiar a un DCH	Si	Si
Múltiplexación de canales	No	Si	Si	Si
Inclusión	3GPP v5	3GPP v99	3GPP v99	3GPP v99

En la modulación 16QAM se utilizan 16 fases, cada una representa un símbolo. Según la ecuación (2.1) se obtiene un resultado de: 2^4=16, de la cual se infiere que por cada símbolo se transmiten 4 bits obteniendo el doble de eficiencia que QPSK.

[41] TTI Transmission Time Interval (Intervalo de Tiempo de Transmisión)

- **AMC (Modulación y Codificación Adaptativa)**

El AMC es el encargado de compensar la inestabilidad del canal radioeléctrico ajustando los parámetros de transmisión, como lo son: la codificación y la modulación de los datos. Este ajuste lo hace basándose en la CQI Channel Quality Indication (Indicación de Calidad del Canal). Los métodos de modulación y codificación son denominados TFRC Transport Format and Resource Combination (Combinación de Recursos y Formatos de Transporte).

Tabla 2.5 Relación entre TFRCs y sus velocidades utilizando 15 multicódigos.

TFRC	Modulación	Eficiencia del código	Transferencia máxima (Mb/s)
1	QPSK	1/4	1.8
2	QPSK	2/4	3.6
3	QPSK	3/4	5.3
4	16QAM	1/4	7.2
5	16QAM	3/4	10.7

El AMC además de seleccionar las TFRCs adecuadas al canal, se encarga de fijar la potencia de transmisión en base a las mediciones hechas por el canal físico CPICH.

- **HARQ (Solicitud de Retransmisión Automática Híbrida)**

La AMC puede tomar deciciones basándose en información falsa del CQI, podría ocurrir que el ciclo de medida para el CQI no fuese lo suficientemente rápido para detectar un desvaneciendo rápido de la señal, en este caso se seleccionaría una modulación y codificación no adecuada al canal y quizás una potencia de transmisión distinta ocasionando errores en la transmisión de información, es aquí

donde se utiliza la HARQ que permite que un elemento de red detecte errores y solicite la retransmisión de los paquetes erróneos.

En comparación con el ARQ convencional, el híbrido posee la ventaja de combinar las transmisiones recibidas y las retransmisiones correspondientes, de esta forma ayuda a reducir el número de retransmisiones necesarias ya que cada paquete enviado tiene menos posibilidad de errores, a este método se le denomina «redundancia incremental»[Ψ] y es una de las modalidades de funcionamiento de la HARQ.

El método de retransmisión que se utiliza para evitar los retrasos es el más sencillo, éste funciona con un mecanismo de acuse de recibido que confirma que el paquete enviado posee o no errores. El ciclo de funcionamiento del HARQ es el siguiente: Se envía el paquete de datos junto con un CRC Cyclic Redundancy Check (Código de Redundancia Cíclica[42]), del otro lado, el receptor le aplica a los datos recibidos un algoritmo de redundancia cíclica, el resultado es comparado con el código enviado en la transmisión y sí ambos códigos son iguales el receptor envía un ACK Acknowledged (Acuse de Recibido), de lo contrario le envía un NACK No Acknowledge (Sin Acuse de Recibido) solicitando la retransmisión.

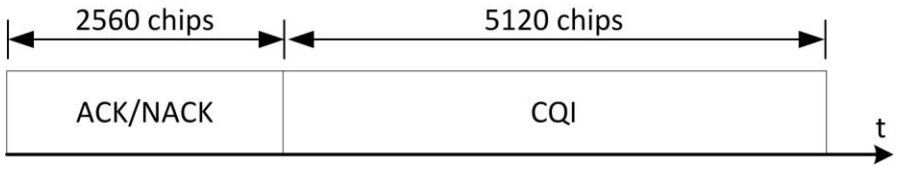
- **El canal físico HS-DPCCH**

Es el canal utilizado para brindar el control de los mecanismos de operación utilizados en HSDPA, en este canal se encuentra la información con la cual trabaja tanto el AMC como el HARQ, se eligió este canal de alta velocidad para adaptarse a las necesidades de rápido control que requiere HSDPA.

[Ψ] Referirse al glosario.

[42] Es un tipo de función que recibe un flujo de datos de cualquier longitud como entrada y devuelve un valor de longitud fija como salida. El término suele ser usado para designar tanto a la función como a su resultado. Pueden ser usadas como suma de verificación para detectar la alteración de datos durante su transmisión.

Figura 2.16 Estructura del canal HS-DPCCH



Por medio de este canal se reciben los acuses de recibido (ACK/ NACK) y la información pertinente a la CQI.

2.3.3 Modos de Transmisión FDD / TDD

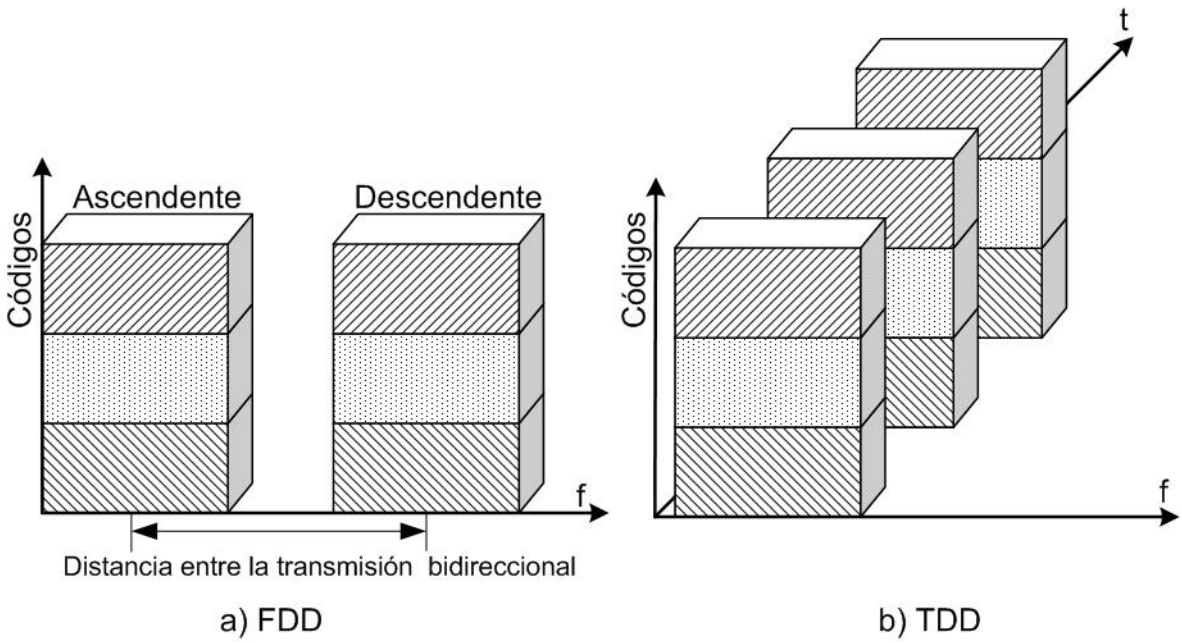
WCDMA posee dos modos fundamentales de transmisión, los cuales son: FDD que es el más utilizado y TDD. En el desarrollo de WCDMA se hizo énfasis en el modo FDD ya que es el más difundido, la diferencia de estos dos modos se puede ver en la Figura 2.17.

Como se puede observar en la Figura 2.17, en el modo FDD se asignan dos bandas de frecuencia; una para el enlace descendente y otra para el ascendente. Estas bandas tienen una anchura de 3.84MHz ascendiendo a 5MHz con las banda de guarda y poseen una distancia de separación entre la transimisión bidireccional[43].

En el modo TDD se destina una sola banda para el enlace ascendente y descendente, esta banda puede ser de 3.84MHz ascendiendo a 5MHz con bandas de guarda como en el FDD o de 1.28MHz ascendiendo a 1.66MHz con bandas de guarda.

[43] La distancia entre la transmisión bidireccional depende de la banda de frecuencia en que se implemente la tecnología. Para los primeros estándares que operan en la banda de 2000MHz la separación es de 190MHz.

Figura 2.17 Modos de transmisión a) FDD y b) TDD



En el modo TDD se destina un determinado espacio de tiempo para el enlace ascendente y otro para el enlace descendente. El TDD se considera adecuado para proporcionar servicios de datos en entornos pequeños o micro-celulares y no en entornos grades, debido a la necesidad de disponer de sincronización entre las estaciones base. Sí dos estaciones base TDD próximas no están sincronizadas se podrían originar problemas de interferencias, como por ejemplo: por falta de sincronización podrían coincidir en el enlace ascendente de una estación con el descendente de otra vecina, es por ello que esta tecnología se utiliza para entornos pequeños y aislados.

En la Tabla 2.6 se detallan las bandas de frecuencia para la telefonía móvil de tercera generación en El Salvador.

Tabla 2.6 Bandas de frecuencias para telefonía móvil de tercera generación en El Salvador.

Disposición de Frecuencias	Banda de Uplink (MHz)	Separación entre Uplink y Downlink (MHz)	Banda de Downlink (MHz)	Separación Dúplex (MHz)
B1	894~915	24	939~960	45
B2	1920~1980	130	2110~2170	190
B3	1710~1785	30	1805~1880	95
B4	1850~1910	20	1930~1990	80
B5 (Armonizada con B2 y B3)	1710~1785 1920~ 1980	20 130	1805~1880 2110~2170	95 190
B6 (Armonizada con B4 y partes de B2 y B3)	1850~1910 1710~1755 1755~ 1805	20 50 305	1930~1990 1805~1850 2110~2160	80 95 355
B7 (Armonizada con B4 y partes de B2 y B3)	1850~1910 1710~1770	20 340	1930~1990 2110~2170	80 400
B8	2500~2570	50	2620~2690	120
B9	450~460	1.25	460~470	10
B10	698~746	0.6	746~806	52
B11	2300~2350	0.5	2350~2400	50
B12	3400~3450	0.5	3450~3500	50

Fuente: Cuadro Nacional de Atribución de Frecuencias (CNAF, 2004).

- **Características físicas de TDD y FDD.**

En la siguiente tabla se muestra una comparación de las características físicas entre el modo de acceso terrestre TDD y FDD.

Tabla 2.7 Características físicas de UTRA: TDD y FDD

Modo	UTRA[44] TDD	UTRA FDD
Ancho de banda asignado	5MHz,1.66MHz	5MHz
Tasa de chips de la portadora	3.84Mchip/s,1.28Mchips/s	3.84Mchip/s
Timeslots por trama	15,14	15
Tamaño de la trama	10ms	
Multirate	Multislot, Multicodigos y OVSF	Multicodigos y OVSF
Modulación	QPSK, 8PSK y 16QAM (HSDPA)	QPSK, y 16QAM (HSDPA)
Codificación del canal	Convolucional (R =1/2, 1/3,1/4, K =9). Código turbo para datos de alta velocidad (R =1/2,1/3,1/4, K=4)	
Control de potencia	Canal ascendente: Ciclo de 100/s o 200/s Canal descendente: Ciclo menor a 800/s	Ciclo de 1500/s
Handover	Hard	Soft
Factor de ensanchamiento	1 ~ 16	Descendente: 4 ~ 512 Ascendente: 4 ~ 256

El multirate (multi-velocidad) puede ser definido como múltiples flujos de datos hacia un solo usuario con el propósito de aumentar la velocidad de transmisión, como se puede ver en la Tabla 2.7, para UTRA TDD se definen tres tipos de multirate: el de multislot que es el flujo de datos en diferentes intervalos de tiempo, los multicódigos que es la utilización de varios canales físicos (DPDCH, DPCCH y HS-DPCCH) utilizando un código por canal y el OVSF Orthogonal Variable Spreading Factor (Factor de Ensanchamiento Ortogonal Variable) que se trata de un factor de ensanchamiento que varía de acuerdo con la calidad del canal.

[44] Univeral Terrestrial Radio Access (Acceso a Radio Terrestre Universal).

2.4 PROTOCOLOS DE UMTS

Debido a la gran variedad de protocolos utilizados en UMTS, se han separado en tres grupos denominados «redes», cada una de estas «redes» está formada por varias capas del modelo OSI. De esta forma, en la parte inferior está la red de transporte, en la parte intermedia la red de radio y en la parte superior la red del sistema.

La red de transporte es la encargada de proveer servicios de transporte para fines generales a todos los elementos de la red en UMTS. La red de radio y la red del sistema, son las encargadas de proveer las funcionalidades de UMTS.

2.4.1 Protocolos de la de Red de Transporte

Los protocolos de la red de transporte están formados por las capas más bajas del modelo OSI, que se encuentran entre las capas 1 y 4 de dicho modelo. Los protocolos utilizados por las interfaces Iub, Iur, Iu-CS e Iu-PS para la red de transporte se muestran en la Figura 2.18 a la Figura 2.21. Estos protocolos tienen la función de proporcionar los medios para transportar y encaminar el tráfico de control y de usuario entre los elementos de UMTS.

Dentro de la red de transporte, el 3GPP ha especificado como protocolos comunes para todos los elementos de red, a los protocolos ATM e IP que se encuentran entre las capas 2 y 3 del modelo OSI. El ATM con sus capas de adaptación AAL2 y AAL5 Adatative ATM Layer (Capa de Adaptación ATM) fue la opción de transporte más aceptada, mientras que el transporte IP sólo se especificó para el tráfico de paquetes hacia el CN (interfaz Iu-PS). Posteriormente el transporte ATM e IP fueron considerados opciones igualmente válidas para todas las interfaces.

El transporte IP se considera una red privada dedicada únicamente para el tráfico del operador, de esta forma se superan problemas de seguridad y QoS característicos de este protocolo cuando se utiliza sobre una red pública.

En la capa 4 del modelo OSI se encuentran protocolos con fines específicos para el plano de control y el plano de usuario que se encargan de adaptar las funcionalidades de ATM o IP a los requerimientos de dichos planos.

Figura 2.18 Protocolos de la red de transporte para la interfaz Iub.

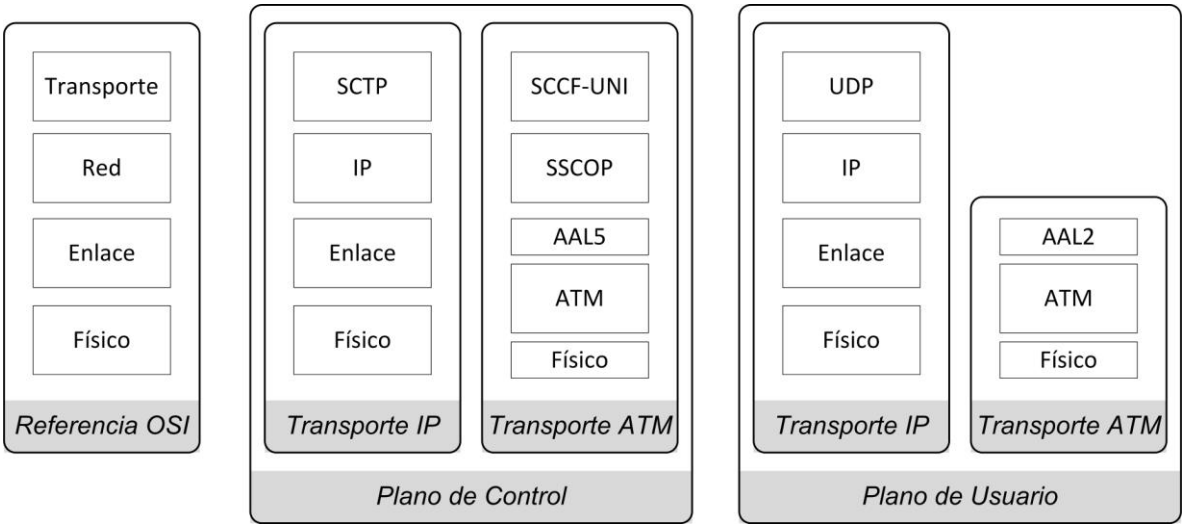


Figura 2.19 Protocolos de la red de transporte para la interfaz Iur.

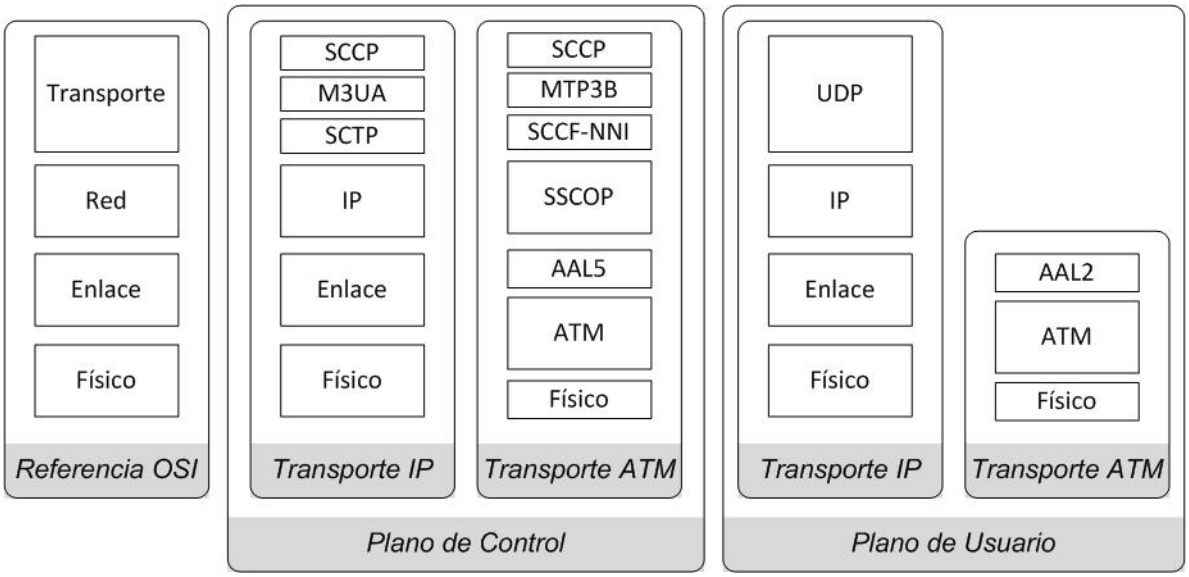


Figura 2.20 Protocolos de la red de transporte para la interfaz Iu-CS.

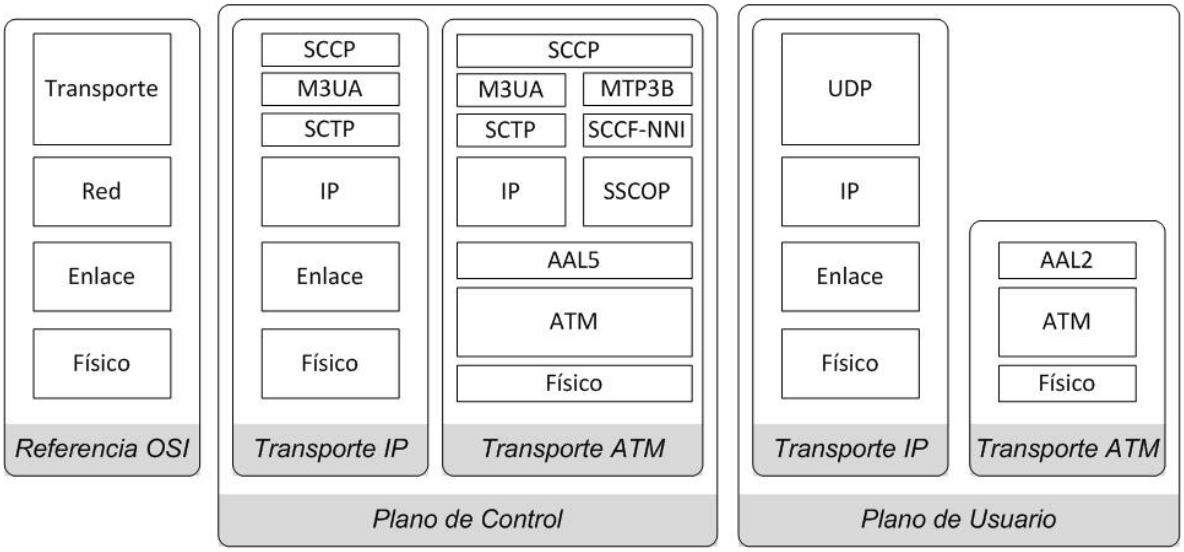
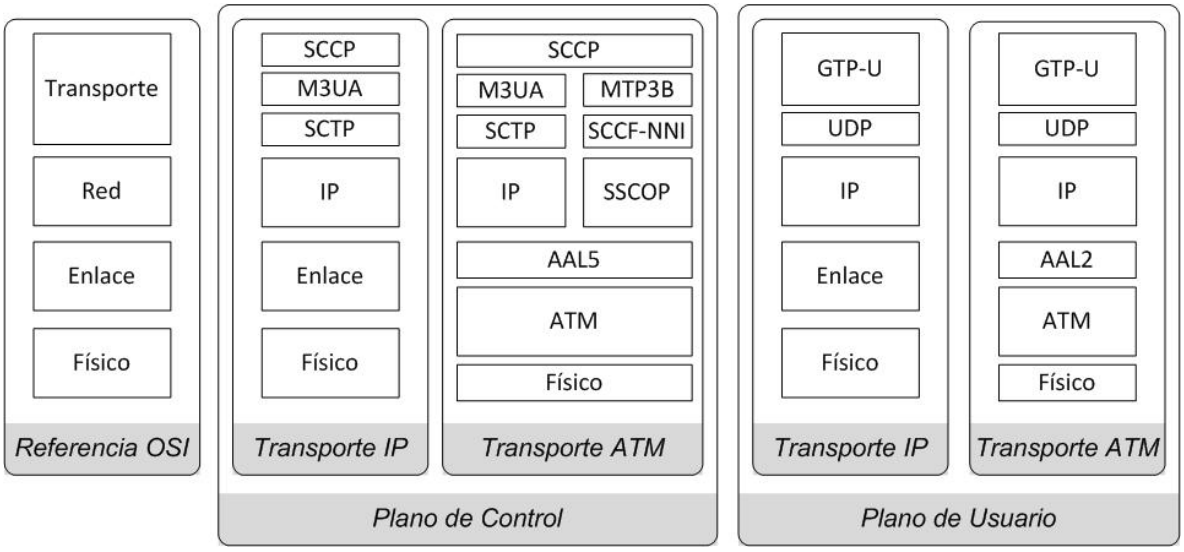


Figura 2.21 Protocolos de la red de transporte para la interfaz Iu-PS.



- **ATM.**

ATM funciona dividiendo el flujo de información que debe transferirse en pequeñas partes o paquetes, luego les añade una etiqueta llamada cabecera y el resultado se conoce como celda ATM. Posteriormente se transfiere a través del trayecto de transmisión físico. En la parte receptora, a las celdas ATM se les quita la cabecera y se unen los paquetes de información para obtener un flujo igual al original.

Las celdas ATM están formadas por dos partes: la cabecera que posee 5 bytes con la información de direcciones y la información a transmitir que se le denomina «carga útil» (Payload), esta última puede tener un máximo de 48 bytes.

La cabecera de la Celda ATM posee los siguientes elementos:

- VPI Virtual Path Identifier (Identificador de Ruta Virtual).
- VCI Virtual Channel Identifier (Identificador de Canal Virtual).
- PT Payload Type (Tipo de Carga Útil).
- CLP Cell Loss Priority (Prioridad de Pérdidas de Celdas).
- HEC Header Error Control (Control de Error en la Cabecera).

Una VP Virtual Path (Ruta Virtual) es una conexión semi-permanente que gestiona simultáneamente varios VC Virtual Channel (Canal Virtual). ATM debe adaptarse a capas de protocolos superiores y a capas físicas inferiores, esto lo hace a través de sus capas de adaptación las cuales son cuatro y están definidas para varias clases de servicios:

- AAL1: ofrece modo síncrono, orientado a la conexión y con flujo constante de datos.
- AAL2: ofrece modo síncrono, orientado a la conexión y con flujo variable de datos.

- AAL3/4: ofrece modo asíncrono, para servicios orientados a la no conexión y con flujo variable de datos.
- AAL5: ofrece modo asíncrono, orientado a conexión y con flujo variable de datos.

La capa AAL se divide en dos sub-capas: la subcapa de convergencia y la subcapa de segmentación y re-ensamblado. La subcapa de convergencia adapta la AAL a las capas de protocolos superiores, mientras que la subcapa de segmentación y re-ensamblado en el transmisor divide los datos a transmitirse en pequeños paquetes de carga útil y el receptor reúne todos esos paquetes para generar un flujo igual al original.

- **IP**

El protocolo IP comenzó a ganar impulso con el fin de sentar las bases para la utilización a gran escala de la tecnología de Intranets IP como medio de transporte para la evolución futura de las redes UMTS, tanto para el transporte de señalización como para el transporte de los datos de usuario.

En el protocolo IP, cada nodo se identifica con una dirección IP, estas direcciones sirven para propósitos de enrutamiento. Sí se desea enviar un paquete a un determinado nodo se necesitará saber la dirección IP del nodo.

En IPv4 existen dos tipos de direcciones IP: las privadas, que son las que se manejan a nivel de una red local administrada o una red privada; y las públicas, las cuales existen en Internet. En IPv4 las direcciones IP están formadas por 4 octetos (32 bits) brindando 4.29×10^9 posibles direcciones, las cuales con la popularidad de Internet se están agotando, para resolver dicho problema se creó el protocolo IPv6. En IPv6 una dirección IP está formada por 16 octetos (128 bits)

brindando 3.4×10^{38} posibles direcciones y tres clases de direcciones: las de enlace local, las de sitio local y las globales.

Aunque el 3GPP no específica el uso de ningún protocolo de la capa de enlace (del modelo OSI) para el funcionamiento con el protocolo IP, existe un requisito mínimo que es el soporte a la estructura de tramas del protocolo punto a punto HDLC High-level Data Link Control (Control de Enlace de Datos de Alto Nivel).

- **MTP3-B**

El protocolo MTP3-B Message Transfer Part layer 3 - Broadcast (Capa 3 de la Parte de Transferencia de Mensajes - Difusión) pertenece al conjunto de protocolos de SS7 y es el responsable del encaminamiento de los mensajes de señalización entre los puntos de señalización. El encaminamiento del MTP3 se basa en SPC Signalling Point Code (Códigos de Puntos de Señalización) y es capaz de encaminar mensajes dentro de un sólo espacio de direcciones SPC que normalmente es administrado por un operador, es decir, este protocolo es capaz de encaminar mensajes de señalización en el dominio de un operador. Si se desea encaminar mensajes de señalización fuera de las fronteras del operador, se deberá utilizar el protocolo SCCP Signalling Conection Control Part (Parte de Control de Conexión de Señalización).

- **SCTP**

El protocolo SCTP Stream Control Transmission Protocol (Protocolo de Transporte para Control de Flujo) es el protocolo de capa 4 elegido por el grupo SIGTRAN Special Interest Group TRAN (Grupo de Interés Especial TRAN) para llevar la señalización SS7 sobre redes del tipo IP. Se descartó el protocolo TCP Transport Control Protocol (Protocolo de Control de Transporte) por ser demasiado lento, ya que posee un mecanismo de acuse de recibido y el protocolo UDP User Datagram

Protocol (Protocolo para Datagramas de Usuario) por no tener ningún mecanismo de control de flujo. El propósito del SCTP es poner a disposición un portador de señalización robusto y fiable; para ello posee procedimientos de control de congestión adecuados y una rápida retransmisión en caso de pérdidas de los mensajes de señalización y se emplea para aumentar la seguridad durante la conexión a las redes UMTS de otros operadores.

- **M3UA.**

El protocolo M3UA MTP3 User Adaptation (Adaptación de Usuario MTP3) tiene como propósito adaptar la pila de protocolos IP que se encuentran debajo de él para utilizar el protocolo SCCP, como se muestra en el plano de control de las Figura 2.19~Figura 2.21. El transporte de control finaliza en este protocolo tanto para la pila IP como para la pila ATM, con el protocolo SCCP se termina el transporte de señalización. El M3UA logra su objetivo simulando algunas características del MTP3 de SS7, además de administrar los flujos del SCTP y adaptarse al rendimiento de su homólogo en SS7 (MTP3-B) proporciona operación en modo redundante, así como la capacidad de compartir la carga entre puntos extremos.

- **SCCP**

Es el protocolo de transporte de señalización común en las interfaces del RNC y el CN. El SCCP proviene del SS7 y ofrece servicios orientados a la conexión y orientados a la no conexión. Este segundo tipo de servicio se emplea con los portadores de señalización. Este protocolo utiliza direccionamiento de tipo global[45] para enrutar los mensajes de señalación entre los operadores.

[45] Se denomina direccionamiento global, porque las direcciones son utilizadas para el encaminamiento de señalización entre operadores.

- **UDP**

Es un protocolo de la capa de transporte que brinda servicios de transporte orientado a la no conexión entre dos nodos de una red IP. En UMTS, el UDP se emplea para identificar los puntos extremos del protocolo GTP-U y también ofrece un mecanismo de suma de comprobación para detectar errores de transmisión en los paquetes de datos.

- **GTP-U**

El GTP-U proporciona servicios de transferencia de datos a las capas superiores y permite el túnel de los paquetes de datos, se implementa en las interfases Iu-PS, Gn y Gp. La especificación TS 29.060 define al protocolo GTP-U.

Las principales funciones de GTP-U son:

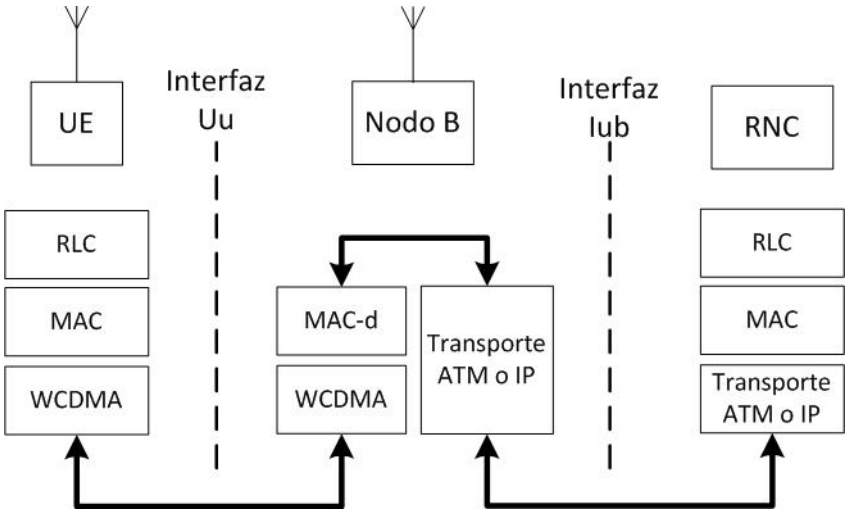
- La transferencia de paquetes de datos.
- La encapsulación y el túnel de datos. La cabecera de GTP-U incluye la información del túnel, esta información incluye un THID Tunnel Endpoint Identifier (Indicador de Punto Extremo del Túnel) de 32 bits que se emplea para direccionar un contexto PDP en un punto extremo del túnel. El túnel permite multiplexar los paquetes de datos de usuario en un sólo trayecto para diferentes usuarios.
- La secuencia de los paquetes de datos: GTP-U puede conservar el orden de los paquetes de datos entre el RNC y el GGSN. La cabecera GTP-U posee un número de secuencia de 16 bits, con la verificación de dicho número se puede determinar si los paquetes de datos están llegando en orden.

- La comprobación de la actividad de los trayectos: GTP-U debe controlar en intervalos regulares si el GTP-U del otro extremo de la interfaz está activo o no y lo hace enviándole un mensaje de solicitud de eco, si el GTP-U del otro extremo está activo le enviará un eco.

- **Protocolos de la Red de Transporte en la Interfaz Uu**

El transporte entre el UE y el Nodo B se realiza a través de la interfaz Uu, utilizando la tecnología de acceso WCDMA.

Figura 2.22 Protocolos de transporte utilizados por la interfaz Uu.



Como se observa en la Figura 2.22, entre el UE y el Nodo B se utiliza WCDMA como interfaz física. Los protocolos MAC y RLC son administrados por el RNC, entonces necesitan ser transportados hasta él, es por ello que en el Nodo B se toman el MAC y el RLC para convertirlos en la carga útil de la pila de transporte IP o ATM con el objetivo de ser transportados hacia el RNC. Una vez en el RNC los protocolos MAC y RLC son extraídos de la pila IP o ATM para uso posterior.

- *MAC*

El protocolo MAC ofrece su servicio como un conjunto de canales lógicos caracterizados por el tipo de datos que transportan. Los canales lógicos son seis: dos de control y cuatro de tráfico. El protocolo MAC busca el control de toda la comunicación de los canales de transporte de WCDMA que pone a disposición de la capa física.

De acuerdo con los tipos de canales de transporte que tiene la capa física, el MAC se divide en tres entidades: el MAC común, el MAC dedicado y el MAC de difusión.

- El MAC Común: reside entre el CRNC y el UE, se encarga del control de los canales de transporte común y compartido.
- El MAC Dedicado: se ubica entre el SRNC y el UE, controla los canales de transporte dedicados.
- El MAC de Difusión: puede encontrarse entre el Nodo B y el UE, gestiona un sólo canal de transporte de difusión en cada célula.

El protocolo MAC también se encarga de recopilar información estadística sobre el tráfico para su uso posterior en la capa del protocolo RRC. Las medidas se toman por un canal lógico e incluyen medidas locales como: el nivel de ocupación del buffer[46] que se utiliza para transmisión, la varianza y la media.

[46] Es un espacio de memoria, en el que se almacenan datos para evitar que el programa o recurso que los requiere, ya sea hardware o software, se quede en algún momento sin datos.

El MAC soporta también HSDPA, como parte de esta extensión se introdujo una nueva entidad denominada «el MAC de alta velocidad». Esta entidad se encarga del control del nuevo canal de transporte (HS-DSCH) utilizado en HSDPA. El MAC de alta velocidad ofrece retransmisión rápida de paquetes que se hayan entregado incorrectamente, cuando el receptor MAC de alta velocidad detecta un error no elimina el paquete recibido, en su lugar, lo almacena en el «Soft buffer» y combina coherentemente el paquete almacenado con las retransmisiones correspondientes hasta que sea posible la decodificación. La capacidad del «Soft buffer» se configura desde la capa RRC y la funcionalidad de retransmisión rápida facilita la entidad HARQ.

- *RLC*

El protocolo RLC se ejecuta tanto en el RNC como en el UE e implementa funcionalidades normales de la capa de enlace de datos. El RLC se hace responsable de la entrega de los PDU Protocol Data Unit (Unidad de Datos de Protocolo) de las capas superiores, además, se encarga de segmentar los SDU Signalling Data Unit (Unidad de Datos de Señalización).

En la especificación TS 25.322 se encuentran más detalles del protocolo RLC.

La transmisión de los PDU por medio del RLC se conoce como «servicio portador de radio» y se han definido tres modos de operación para este servicio:

- Modo Transparente: trasmite las SDU sin añadir ningún tipo de información de protocolos. Este modo se puede utilizar en los servicios del tipo streaming.
- Modo sin Acuse de Recibido: se transmite el SDU pero no se garantiza la entrega. Este modo lo emplean algunos procedimientos de control del RRC en los que el propio RRC se encarga de los acuses de recibido.

- Modo con Acuse de Recibido: El RLC entrega el SDU y garantiza la entrega gracias a un mecanismo de retransmisión. Este modo se utiliza en la transferencia de datos por paquetes.

El RLC realiza las siguientes funciones:

- Segmentación y Reensamblaje: ajusta la longitud variable de las SDU de las capas superiores a la longitud de las PDU RLC.
- Concatenación: cuando el contenido de los SDU no llena un número entero de PDU RLC, se coloca el primer segmento de una SDU RLC en un PDU RLC encadenado al último segmento de la PDU RLC anterior.
- Relleno: cuando no se puede aplicar la concatenación los campos restantes se completan con bits de relleno.
- Corrección de Errores: mientras que la capa física detecta los errores mediante mecanismos CRC, la capa RLC es la encargada de corregirlos.
- Entrega de SDU por Orden: se entregan los SDU de forma ordenada gracias a un mecanismo de acuse de recibido.
- Detección de Duplicaciones: el RLC detecta PDU duplicadas y asegura que las PDU de las capas superiores se entreguen una sola vez gracias a un mecanismo de control de flujo.
- Comprobación del Número de Secuencia: se utiliza para garantizar la integridad de las PDU en aquellos casos en los que no se utilice un mecanismo de acuse de recibido.
- Comprobación y Detección de Errores en los Protocolos: aquí se detectan y se corrigen errores causados por la operación del protocolo RLC. Sí se encuentra un error que no se puede corregir la entidad RLC lo comunica a la capa RRC.

- Suspensión y Reanudación: el RLC puede suspender y reanudar la transferencia de datos cuando lo solicite el RRC.
- Exclusión de SDU: facilita la eliminación del buffer de todas las PDU cuya transmisión ha sido fallida en numerosas ocasiones para evitar el desbordamiento del buffer.
- Cifrado: se utiliza para los portadores de radio que ocupan el acuse de recibido utilizando el algoritmo de cifrado por bloques «Kasumi».

2.4.2 Protocolos de la Red de Radio

Los protocolos de la red de radio son los encargados de controlar el establecimiento de la conexión, el mantenimiento de la conexión y la liberación de los portadores de acceso, los cuales transfieren los datos entre el UE y la CN.

Los protocolos de la red de radio se ejecutan sobre la red de transporte, es decir, las pilas de protocolos ATM o IP y en el caso de la interfaz Uu sobre sus protocolos de transporte.

En la Figura 2.22 y Figura 2.23, los bloques descritos como «ATM o IP» hacen referencia a la pila de protocolos de red de transporte para ATM e IP de la Figura 2.18~Figura 2.21.

- **RANAP**

El protocolo RANAP RAN Application Part (Parte de Aplicaciones de la Red de Acceso a Radio) es un protocolo del plano de control que sirve para transmitir mensajes de señalación sobre la interfaz Iu y es montado sobre el protocolo de transporte de señalización SCCP. También, contribuye a la transmisión de mensajes de señalización del protocolo RRC.

Figura 2.23 Protocolos de la red de radio para el plano de control.

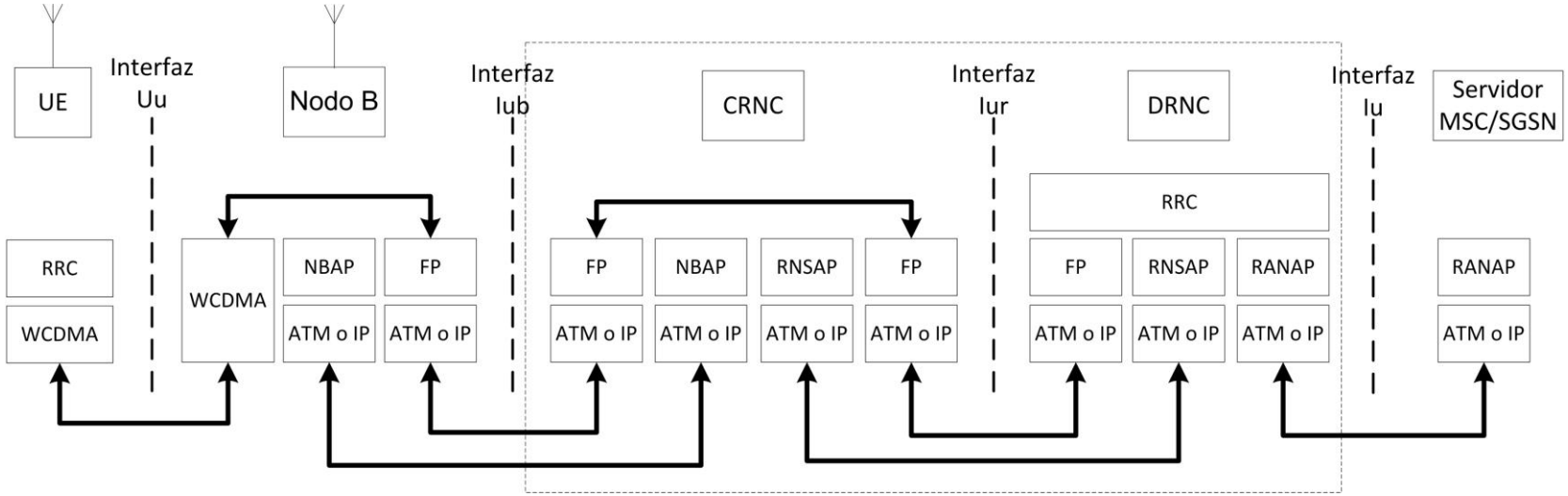
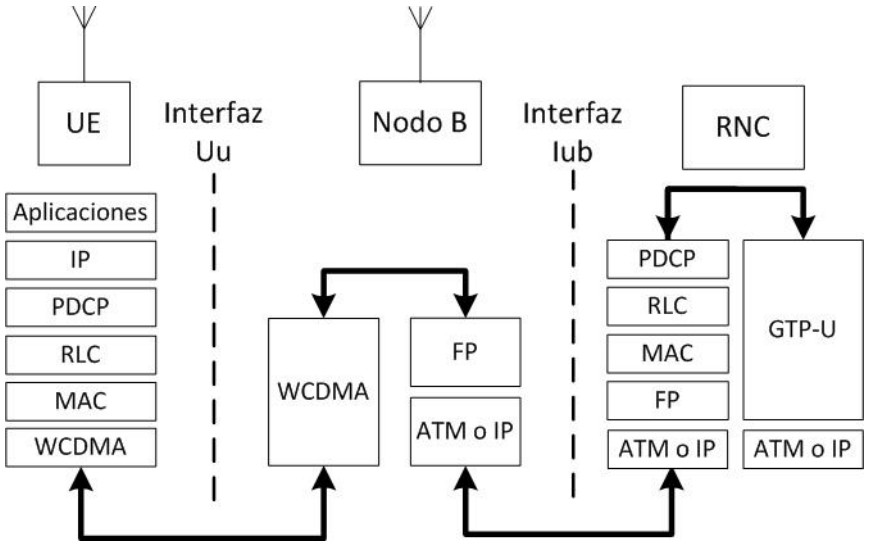


Figura 2.24 Intervención de protocolos de la red de radio para el plano de usuario en el dominio PS.



El protocolo RANAP es el encargado de controlar los recursos de radio de la interfaz Iu. Una entidad RANAP reside en el RNC y su homólogo en el servidor MSC (en el caso del dominio CS) o en el SGSN (en el caso de dominio PS).

Los servicios de RANAP se clasifican en:

- Los Servicios de Control Generales, sólo son necesarios en ocasiones excepcionales, por ejemplo: para el control de la carga de la interfaz Iu, sí el volumen de tráfico de usuario aumenta en exceso o en el caso de un fallo en uno de los extremos de la interfaz RANAP para ofrecer un servicio de restablecimiento para inicializar la interfaz Iu por completo y eliminar todas las conexiones activas.
- Los Servicios de Control Dedicados, se utilizan para diferenciar a cada UE conectado y controlan el modo de seguridad en la UTRAN. RANAP ofrece medios para que el CN pueda controlar el establecimiento, la modificación y la liberación de la conexión, además transfiere una portadora de radio de

un UE hacia un nuevo RNC cuando el UE ha cambiado de posición. Este servicio se llama reubicación de SRNC.

- **RNSAP**

El protocolo RNSAP RNS Application Part (Parte de Aplicación del Subsistema de la Red de Radio) del plano de control, ofrece intercambio de señalización en la interfaz Iur y es montado sobre el protocolo de transporte SCCP. Se ejecuta entre el DRNC y el SRNC. En la especificación TS 25.423 de 3GPP se define al protocolo RNSAP.

Este protocolo se encarga de la señalización de gestión de portadoras de toda la interfaz Iur, del establecimiento de los radioenlaces y permite que el SRNC los controle mediante recursos en un DRNC.

Los mensajes RNSAP facilitan las siguientes funciones:

- La gestión de tráfico de los canales de transporte comunes (por ejemplo: la localización).
- La gestión del tráfico de los canales de transporte dedicado (como: el establecimiento, agregación o eliminación de radioenlaces y la comunicación de mediciones).
- La gestión de tráfico en los canales de trasporte descendentes (como: el establecimiento, agregación o eliminación de radioenlaces y asignación de capacidad).
- Coordinación de las actividades cuando otro RNS se hace cargo de la función SRNC en un procedimiento de handover.
- Las actividades del control de potencia para el enlace descendente.
- Liberación y reestablecimiento de las conexiones RRC siempre que sea necesario realizarlo en la Iur.

- **NBAP**

El protocolo NBAP Nodo B Application Part (Protocolo de Parte de Aplicación del Nodo B) del plano de control, es el encargado de mantener la señalización en la interfaz Iub entre el Nodo B y el RNC. El Nodo B obedece las órdenes del RNC sobre la gestión de recursos radioeléctricos por medio de los mensajes NBAP. En la especificación TS 25.433 de 3GPP se define al protocolo NBAP.

El Nodo B ejecuta procedimientos físicos en la interfaz Uu y debe comunicarlos al RNC, este intercambio de información recibe el nombre de Operación y Mantenimiento (O&M) y constituye una parte integral de la señalización NBAP. Además, el NBAP se encarga del establecimiento y la liberación de una conexión dedicada del plano de usuario en la Iub y el envío de órdenes al Nodo B para activar los recursos para nuevos radioenlaces en la interfaz Uu.

Los procedimientos de NBAP se clasifican en:

- Procedimientos comunes, involucra las actividades de O&M como: procedimientos para la gestión de la configuración de los canales lógicos, procedimientos que permiten informar al RNC del estado de los mismos. También existen procedimientos para permitir al RNC iniciar mediciones específicas y otros para la entrega de la información de difusión que debe transportarse por los canales lógicos.
- Procedimientos dedicados, son los que están relacionados al UE específicamente, dentro de éstos están: la gestión y supervisión de radioenlaces existentes, la reconfiguración en los radioenlaces existentes, la toma de decisiones en los canales dedicados y la configuración del nivel de potencia.

- **RRC**

El protocolo RRC Radio Resource Control (Control de Recursos Radioeléctricos) del plano de control, es el encargado de ofrecer la función de RRM a diferencia de los protocolos de la red de radio anteriores, éste se transporta sobre el protocolo RLC de la red de transporte de la interfaz Uu y opera entre el UE y el RNC. En la especificación TS 25.331 del 3GPP se define al protocolo RRC.

Además, el protocolo RRC se encarga del control de la comunicación para las mediciones de los recursos radioeléctricos.

El RRC posee tres modos:

- TM-SAP Transparent Mode SAP (SAP en Modo Transparente): se utiliza cuando el UE se tiene que comunicar con el RNC antes de establecer una conexión completa (por ejemplo: en el acceso inicial a la red), también se utiliza para los mensajes que se repiten con frecuencia.
- AM-SAP Acknowledge Mode SAP (SAP en Modo con Acuse de Recibido): se emplea para la señalización de control específica de un UE.
- UM-SAP Unacknowledge Mode SAP (SAP en Modo sin Acuse de Recibido): se emplea para evitar posibles retrasos que puedan ocurrir en el modo AM-SAP, como por ejemplo: en la liberación de la conexión.

El RRC posee cuatro entidades lógicas:

- DCFE Dedicated Control Function Entity (Entidad de Función de Control Dedicada): se utiliza para gestionar la señalización específica de un UE y en el SRNC se establece un DCFE por cada UE.
- PNCE Paging Notification Control Entity (Entidad de Control de Notificación y Localización): se utiliza para los mensajes de localización que se envían al UE en estado de reposo.

- BCFE Boadcast Control Function Entity (Entidad de Función de Control de Difusión): se encarga de la informaron de difusión de los canales lógicos BCCH y FACH.
- Entidad de Función de Encaminamiento: se encarga del encaminamiento de los menajes de gestión de movilidad y llamadas (MM / CM).

- **PDCP**

Las aplicaciones de usuario de datos por paquetes se llevan acabo a través de la pila de protocolos TCP/IP, la cual se utiliza para tener acceso a Internet y sus aplicaciones. De esta forma se necesita transportar la pila TCP/IP de las aplicaciones de un UE por la interfaz radioeléctrica, es decir, a través de los protocolos de transporte de la interfaz Uu (WCDMA, MAC y RLC). El protocolo PDCP Packet Data Convergence Protocol (Protocolo de Convergencia de Datos por Paquetes) es el encargado de realizar esta tarea, convirtiendo la pila TCP/IP en carga útil del protocolo asignado para el transporte radioeléctrico (RLC). En la especificación TS 25.323 de 3GPP se define al protocolo PDCP.

El PDCP cumple su función de adaptación comprimiendo las cabeceras IP para que puedan ajustarse al PDU del RLC. Como ya se mencionó, una cabecera IPv4 puede llegar a tener 40 bytes, una cabecera IPv6 tiene 60 bytes, más la carga útil que es demasiado grande para ajustarse en el PDU RLC, con ese objetivo se utiliza la compresión. Además, la capa RLC está provista de un mecanismo de segmentación en caso de que el PDCP no sea suficiente para lograr el transporte.

El primer algoritmo de compresión de cabeceras IP especificado por 3GPP fue el RFC Request For Comments (Petición de Comentario) 2507 de EITF, posteriormente se añadió otro algoritmo de compresión de cabeceras denominado ROHC Robust Header Compression (Compresión Robusta de Cabecera) definido en la RFC 3095 de EITF.

- **FP**

El protocolo FP Frame Protocol (Protocolo de Trama) es el encargado de brindar el soporte adecuado para que los protocolos de transporte radioeléctrico (MAC, RLC y RRC) puedan trasladarse por el Nodo B, RNC y CN a través de la red de transporte ATM o IP.

Este protocolo trabaja tanto en el plano de usuario como el plano de control en las interfaces Iub e Iur. Cuando se trata del plano de usuario, en el Nodo B, FP debe adaptar la estructura de datos de la pila MAC y RLC para llevarla hasta el RNC a través de la pila ATM o IP. Cuando se trata del plano de control, el nodo debe adaptar la estructura de datos de la pila MAC, RLC y RRC para llevarla hasta el RNC a través de la pila ATM o IP. En estas interfaces, FP trabaja sobre los canales de transporte DCH y HS-DSCH.

FP utiliza dos modos de transporte:

- Modo Transparente: los datos se colocan en la pila de transporte sin añadir ninguna cabecera, puede utilizarse para transmitir paquetes en tiempo real en formato GTP-U.
- Modo de Soporte: adopta la forma de un protocolo con la división de datos en tramas y puede transmitir datos de voz codificado en AMR Adaptive Multi Rate (Multivelocidad Adaptable) en el dominio CS, es este caso el FP puede transportarse sobre el AAL2 ó UDP.

2.4.3 Protocolos de Red del Sistema

Los protocolos de red de sistema son los encargados de crear los servicios de comunicaciones para los usuarios y operan sobre los protocolos de red de radio.

El plano de usuario de este nivel esta dado por los codecs de voz como: el AMR para el dominio CS o protocolos que tiene que ver con el flujo de información multimedia como algoritmos MPEG Moving Picture Experts Group (Grupo de

Expertos de Imágenes en Movimiento) para el dominio PS. Por otra parte, los siguientes protocolos de red de sistema pertenecen al plano de control:

- **MM**

El protocolo MM opera entre el UE y el MSC/VLR, es un protocolo de plano de control que ofrece los mecanismos de señalización para el control de la función MM en el CN y de los mecanismos de autenticación entre el UE y el dominio CS.

La especificación TS 24.008 detalla al protocolo MM.

El MM utiliza la conexión de señalización que ofrecen los protocolos de red de radio. Éste se transporta desde el UE hasta el RNC a través del protocolo RRC y del RNC hasta el CN a través del protocolo RANAP.

El protocolo MM posee tres tipos de procedimientos:

- Procedimientos de conexión de MM: se emplean para establecer y liberar una conexión MM.
- Procedimientos comunes de MM: pueden iniciarse en cualquier momento mientras las conexiones MM están activas. Los procedimientos MM obligatorios son:
    - Reasignación de TMSI: en este procedimiento el MSC/VLR asigna una TMSI en lugar del IMSI para que se conserve la confidencialidad de la identidad del usuario.
    - Autenticación: permite al CN confirmar si la identidad que ha facilitado el UE es aceptada o no y proporciona los parámetros para que el USIM calcule nuevas claves de cifrado.
    - Identificación: el CN utiliza este procedimiento para solicitar al UE la IMSI y la IMEI.

  - Desconexión del IMSI: se indica desde el UE cuado éste se desactiva o cuando se extrae el USIM.
  - Cancelación: el CN lo utiliza para cancelar una conexión MM cuando se produce un fallo o cuando encuentra un UE ilegal.

- Procedimientos específicos de MM: se encargan de los mensajes utilizados en la actualización de posición. Estos pueden ser:
  - Actualización Normal de Posición: se utiliza en situaciones en las que el UE descubre que su área de localización ha cambiado, por lo tanto, necesita informar al CN sobre la nueva ubicación. La detección se lleva acabo comparando el valor de LAI difundido por la red con el LAI guardado en el USIM.
  - Actualización Periódica de Posición: se utiliza para notificar al CN la posición del UE.
  - Conexión del IMSI: se lleva acabo cuando el UE se enciende en la misma área de ubicación en la que fue desconectado.

- **GMM**

El protocolo GMM GPRS Mobility Management (Gestión de Movilidad GPRS) opera entre el UE y el SGSN, ofrece los mecanismos de señalización para la MM y las funciones de autenticación entre el UE y el dominio PS del CN. Utiliza la misma conexión de señalización de MM.

La especificación TS 24.008 de 3GPP detalla el protocolo GMM.

Las entidades GMM se pueden ejecutar para los UE que estén trabajando en modo PS/CS, es decir, que tengan conexiones con el MSC/VLR y el SGSN para optimizar recursos y evitar que se generen procedimientos MM y GMM por separado. Estos se conocen como procedimientos combinados.

Los procedimientos GMM para el establecimiento y liberación de la conexión son:

- Conexión GPRS y conexión GPRS combinada: se utiliza para identificar a la P-TMSI y el área actual de encaminamiento hacia la red. Este procedimiento se realiza cuando se enciende el UE.
- Desconexión GPRS y desconexión GPRS combinada: se invoca cuando se apaga el UE o se extrae el USIM.

Los siguientes procedimientos GMM se emplean para la gestión de las posiciones cuando ya existe una conexión GMM:

- La actualización del área de encaminamiento normal y del área de encaminamiento combinada: se lleva acabo cuando el UE advierte que ha cambiado el área de encaminamiento y lo tiene que informar al CN.
- La actualización del área de encaminamiento periódica: notifica al CN periódicamente cual es la posición del UE.

Los siguientes procedimientos comunes de GMM son para fines de seguridad:

- Reasignación de P-TMSI: facilita un P-TMSI para su uso dentro del procedimiento de la interfaz de radio en lugar de la IMSI.
- La autenticación y el cifrado GPRS: este procedimiento lo inicia siempre el CN para comprobar si la identidad que ha facilitado el UE es aceptable.
- La identificación de GPRS: la utiliza el CN para solicitar la IMEI y la IMSI.

El siguiente procedimiento es necesario para proporcionar servicios de conexión al protocolo SM:

- La solicitud de servicios: inicia el procedimiento para establecer una conexión segura y utilizar el protocolo SM.

- **CC**

El protocolo CC pone a disposición los servicios básicos para el establecimiento y la liberación de los servicios de CS. Éste se ejecuta entre el MSC/VLR y los UE, utiliza el servicio de conexión proporcionado por el protocolo MM. La entidad del protocolo CC tiene que estar interconectada con el protocolo ISUP para establecer una conexión de llamada hacia la PSTN externa. Los procedimientos CC crean conexiones entre el UE y el CN, además de activar el codec de voz, multimedia y funciones de interconexión.

- **SM**

El protocolo SM es el homólogo del CC pero en el dominio PS, se utiliza para el establecimiento y liberación de sesiones de paquetes de datos, estas sesiones se les denomina contextos PDP. Se ejecuta entre el UE y el SGSN y utiliza el servicio de conexión proporcionado por el protocolo GMM.

La especificación TS 24.008 de 3GPP detalla el protocolo SM.

La función principal del SM es permitir la gestión del contexto PDP del UE, el cual contienen la información necesaria para encaminar los paquetes de datos del plano de usuario entre el SGSN y el UE.

La gestión del contexto PDP realizada por el SM se notifica al GGSN por medio del protocolo GTP-C.

Los procedimientos SM son los siguientes:

- La activación del contexto PDP: establece un contexto PDP en el UE, en el SGSN y en el GGSN.
- La modificación del contexto PDP: se invoca cuando es necesario un cambio de parámetros de la sesión, como por ejemplo: la QoS.

- Desactivación del contexto PDP: destruye los contextos PDP existentes en el UE y el CN.

- **SS**

El protocolo SS es el encargado de controlar los servicios suplementarios, los cuales son servicios adicionales que ofrece el modo CS y que fueron heredados de GSM (Sección 1.6.3).

- **GTP-C**

El protocolo GTP-C es un protocolo interno del CN y pertenece al dominio PS, se implementa entre SGSN y el GGSN. Este protocolo especifica la gestión de túneles y los procedimientos de control que hacen posible que el SGSN y el GGSN puedan proceder a la transferencia de paquetes de datos de usuario. El GTP-C también se utiliza para transferir mensajes de señalización GMM entre varios SGSN.

El GTP-C opera en la interfaz Gn (entre el SGSN y el GGSN), en la interfaz Gp (entre el SGSN y el BG para la interconexión de otras redes UMTS) y se transporta sobre la pila de protocolos UDP/IP.

2.4.4 Protocolos del Subsistema IMS

En la Tabla 2.8 se presenta la información sobre los protocolos que intervienen en el funcionamiento del IMS y las interfaces que lo utilizan. Todos estos protocolos pertenecen a las capas superiores del modelo OSI que tienen relación con las aplicaciones.

Tabla 2.8 Interfaces del IMS y sus protocolos.

Interfaz	Protocolo	Entidades que Intervienen	Finalidad
Gm	SIP	UE, P-CSCF	Intercambiar mensajes entre el UE y los CSCF
Mw	SIP	P-CSCF, I-CSCF, S-CSCF	Intercambiar mensajes entre los CSCF
ISC	SIP	I-CSCF, S-CSCF, AS	Intercambiar mensajes entre el CSCF y AS
Cx	DIAMETER	I-CSCF, S-CSCF, HSS	Establecer comunicación entre I-CSCF/ S-CSCF y el HSS
Dx	DIAMETER	I-CSCF, S-CSCF, SLF	Los I-CSCF/ S-CSCF la utilizan para encontrar un HSS correcto
Sh	DIAMETER	SIP AS, OSA SCS, HSS	Intercambiar mensajes SIP AS/OSA SCS y HSS
Si	MAP	IMS-SF, HSS	Intercambiar información entre IMS-SF y HSS
Dh	DIAMETER	SIP AS, OSA, SCF. IMS-SF, HSS	Lo emplea un AS para encontrar un HSS correcto
Mm	No especificado	I-CSCF, S-CSCF, red IP externa	Intercambia mensajes IMS a redes externas
Mg	SIP	MGCF, I-CSCF	MGCF convierte la señalización ISUP a SIP y la envía al I-CSCF
Mi	SIP	S-CSCF, BGCF	Intercambiar mensajes entre S-CSCF y BGCF
Mj	SIP	BGCF, MGCF	Intercambiar mensajes entre el BGCF y el MGCF
Mk	SIP	BGCF, MGCF	Intercambiar mensajes entre los BGCF de redes diferentes
Mr	SIP	S-CSCF, MRFC	Intercambiar mensajes entre el S-CSCF y el MRFP

Mp	H.248	MRFC, MRFP	Intercambia mensajes entre MRFC y MRFP
Mn	H.248	MGCF, IMS-MGW	Control de los recursos del plano de usuario
Ut	HTTP	UE, AS (SIP,OSA, SCS, IMS-CF)	Permite al UE gestionar información relacionada con servicios
Go	COPS	PDF, GGSN	Permite al operador controlar el QoS del plano de usuario e intercambiar información relacionada con la tarificación entre el IMS y la Red
Gq	DIAMETER	P-CSCF, PDF	Intercambiar información de políticas entre el P-CSCF y PDF
Ro	DIAMETER	AS, MRCF, S-CSCF, OCS	Tarificación en línea hacia el OCS
Rf	DIAMETER	P-CSCF, S-CSCF, I-CSCF, BGCF, MGCF,AS, MGGF, AS, MRFC, CCF	Lo utilizan las funciones IMS para la tarificación fuera de línea hacia el CCF

- **SIP**

El protocolo SIP es utilizado para establecer, modificar y terminar sesiones multimedia en redes IP. Está definido por la RFC3261 y estandarizado por la IETF.

- **DIAMETER**

Este protocolo se utiliza para la comunicación entre las entidades IMS y el HSS, es un protocolo AAA Authentication, Authorization and Accounting (Autenticación, Autorización y Contabilidad), está basado en el protocolo RADIUS Remote Authentication Dial-In User Service (Servicio de Autenticación Remota de Usuario

por Marcado). DIAMETER incluye un modo que permite la compatibilidad con RADIUS y se transporta sobre SCTP utilizando la pila de transporte TCP/IP. Para proporcionar seguridad a sus conexiones emplea IPSec y TLS Transport Layer Security (Seguridad en la Capa de Transporte) definido en la RFC 2246.

- **COPS**

COPS Common Open Policity Service (Servicio de Políticas Abiertas Comunes) se emplea para la administración y cumplimiento de las políticas. Es un protocolo de consultas y respuestas para el intercambio de información del PDF.

2.5 SERVICIOS PROPORCIONADOS POR UMTS

2.5.1 Servicios Básicos de Telecomunicaciones.

Los servicios básicos de telecomunicaciones se dividen en dos grandes categorías:

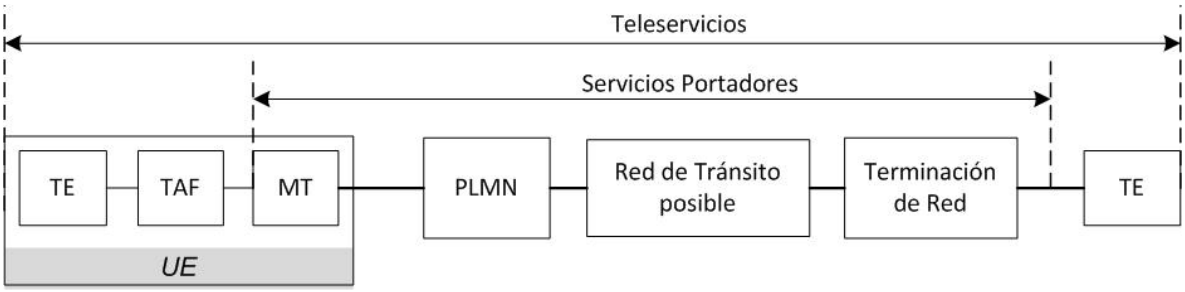
- Servicios Portadores.
- Teleservicios.

El enlace de la comunicación entre los puntos de acceso puede estar formado por una PLMN, una o más redes de tránsito y una red final. Las redes entre los dos puntos de acceso utilizan diferentes métodos para el control de la portadora. En la Figura 2.25 se ilustran dichos servicios.

2.5.2 Servicios Portadores.

Los servicios portadores proporcionan la capacidad de transferir información entre los puntos de acceso e involucran sólo funciones de las capas más bajas (en referencia a las capas del modelo OSI).

Figura 2.25 Servicios básicos soportados por una PLMN.



El enlace de comunicación puede extenderse entre diferentes redes tales como: Internet, Intranets, LAN y ATM basadas en redes de tránsito, teniendo redes específicas como medio para el control portador. Cada red contribuye con la QoS punto a punto percibida por el usuario final.

Los dominios CS y PS proveen un conjunto específico de capacidades portadoras. Los servicios portadores de circuitos están descritos en la TS 22.022 y los servicios de paquetes (GPRS) están descritos en la TS 22.060 del 3GPP.

- **Descripción.**

Los servicios portadores poseen un conjunto de características punto a punto con requerimientos de QoS. La QoS es la calidad de un servicio solicitada y percibida por el cliente (ITU-T M.xxxx).

Los requerimientos de los servicios portadores se pueden dividir en dos grupos:

- Requerimientos de la Transferencia de Información: el cual caracteriza las capacidades de transferencia de la red para intercambiar datos de usuarios entre dos o más puntos de acceso.
- Características de la Calidad de la Información: la cual describe la calidad de la información de usuario transferida entre dos o más puntos de acceso.

- **Transferencia de Información.**

Se pueden soportar tanto los servicios «orientados a la conexión» y «orientados a la no conexión»:

- *Tipo de Tráfico.*

Se requiere que el servicio portador proporcione uno de los siguientes tipos:

- Velocidad de bit constante garantizada.
- Velocidad de bit variable dinámica y no garantizada.
- Velocidad de bit variable dinámica de tiempo real con un mínimo de velocidad de bit garantizada.

Se deben soportar aplicaciones en tiempo real y tiempo diferido:

- Se debe soportar el Video, audio y voz en tiempo real. Esto implica, la habilidad de proveer un stream en tiempo real con velocidad de bit garantizada, retraso punto a punto y variación en el retraso. Así como la habilidad de proveer un servicio de voz en tiempo real de velocidad de bit garantizada, retraso punto a punto y variación en el retraso.
- Se debe soportar el servicio interactivo y de transferencia de archivos en tiempo real. Esto implica, la habilidad de soportar el transporte de mensajes con diferentes peticiones QoS entre distintos usuarios.
- Se debe soportar las aplicaciones multimedia. Esto implica, la habilidad de soportar varios streams de usuarios desde o hacia un usuario que tiene diferentes tipos de tráfico (por ejemplo: tiempo real y tiempo diferido).

- *Características del Tráfico.*

Debe ser posible para una aplicación especificar sus requerimientos de tráfico para la red a través de la petición de un servicio portador con una de las siguientes configuraciones:

- Punto a Punto (Unidireccional y Bidireccional [Simétrico y Asimétrico]).
- Unidireccional Punto a Multi-Punto (Multicast y Broadcast)

- **Calidad de Información.**

La calidad de información caracteriza la integridad de bit y los requerimientos de retraso de las aplicaciones.

Se necesitan además otros parámetros tales como:

- Retraso máximo de transferencia.
- Variación en el retraso.
- BER.
- Velocidad de datos.

- **Soporte de Velocidades de Bits.**

Es posible para una aplicación, especificar sus requerimientos de tráfico a la red a través de la petición de un servicio portador con cualquiera de los tipos de tráfico especificados, características de tráfico, retraso de transferencia máximo, variación en el retraso, BER y velocidad de bit. Es posible para la red, satisfacer estos requerimientos sin gastar recursos en las interfaces de radio y de red debido a las limitaciones de variación en las velocidades de bits.

Será posible para un terminal móvil tener varios servicios portadores activos simultáneamente, cada uno de los cuales podría ser orientado a la conexión o a la no conexión.

El único factor limitante para satisfacer los requerimientos de la aplicación, debe ser la velocidad de bit acumulada por un terminal móvil en un instante dado (ejemplo: cuando se suman las velocidades de bit de un terminal móvil con tráfico simultáneo orientado a la conexión y a la no conexión, independientemente sí el tráfico es en tiempo real o no) en cada ambiente de radio:

- Al menos 144 Kbps en ambiente de radio satelital.
- Al menos 144 Kbps en ambiente de radio rural externo.
- Al menos 384 Kbps en ambientes externos urbano y suburbano.
- Al menos 2048 Kbps en ambientes interno y externo de baja movilidad.

2.5.3 Teleservicios.

Los Teleservicios proporcionan las capacidades completas para las comunicaciones por medio del equipo terminal, funciones de red y posiblemente funciones provistas por centros dedicados.

La referencia básica para la descripción de los Teleservicios es la recomendación ITU-T F.700. La cual proporciona una descripción genérica de los servicios multimedia. La metodología utilizada cubre tanto los servicios de medios simples y los servicios multimedia; los servicios simples son un tipo particular de multimedia y los servicios multimedia están clasificados dentro de categorías con características de funcionamiento similar. Las seis categorías son: servicios de conferencia multimedia, servicios conversacionales multimedia, servicios de distribución de multimedia, servicios de almacenamiento de multimedia, servicios de mensajes multimedia y servicios de colección multimedia.

Los Teleservicios multimedia soportan la transferencia (y en algunos casos almacenamiento, mensajería y distribución) de varios tipos de información (componentes de servicio). Por esta razón, existen atributos de servicio (relacionado con todos los componentes de un teleservicio) y atributos de componentes de servicio (relacionado únicamente a un componente de servicio).

- **Teleservicios Soportados por una PLMN.**

Son el subconjunto de teleservicios estandarizados que pueden ser soportados por el interworking entre teleservicios proporcionados por otras redes. La forma de soportar el siguiente conjunto de teleservicios será estandarizada:

- Voz: debe ser soportado como está definido en los estándares internacionales. Su recomendación es la ITU-T E.105. Las redes deben contener unidades de interworking que permitan recibir llamadas desde o destinadas a usuarios de las redes existentes como lo son: la PSTN e ISDN. Para proporcionar un servicio de voz, se puede especificar un codec de voz estándar. El codec de voz elegido debe tener la capacidad de operar con un mínimo de pérdida de voz sobre el handover entre las redes GERAN y UTRAN.
- Llamada de Emergencia: el servicio debe utilizar un componente de voz. Existen, sin embargo, comparándolo con la telefonía fija requerimientos de autenticación reducidos y requerimientos para el direccionamiento específico. Adicionalmente, las llamadas de emergencia tienen una prioridad más alta que las llamadas normales (más detalles se encuentra en la especificación TS 22.101 de 3GPP).

- Servicios de Mensajes Cortos: existen dos tipos, SMS-PP[47] y SMS-CB[48]. Ambos deben proporcionar continuidad a través de las redes de acceso GERAN y UTRAN.

2.5.4 Acceso a Internet.

Las especificaciones del 3GPP deben proporcionar la forma de interoperar con las redes de datos externas. Se debe satisfacer el interworking junto con las limitaciones introducidas por el ambiente del radio móvil y los requerimientos de QoS para el interworking con redes. El Internet es la red interoperativa más importante, de allí que la especificación de la optimización de acceso a Internet sea parte de las especificaciones del 3GPP. Los beneficios alcanzados más importantes por la definición del acceso a Internet son:

- Transmisión optimizada del tráfico IP sobre la interfaz de radio para minimizar la cantidad de información transmitida.
- El uso optimizado de protocolos y algoritmos de encriptación sobre la interfaz de radio.
- Mecanismos de interoperabilidad de QoS.

Para propósitos de optimización del acceso a Internet se utilizan uno o más servicios portadores genéricos. Los mecanismos de QoS definidos para el modo de acceso de paquetes serán armonizados por aquellos definidos para Internet por el IETF.

[47] SMS-PP Short Message Service - Point to Point (Servicio de Mensajes Cortos – Punto a Punto).
[48] SMS-CB Short Message Service - Cell Broadcast (Servicio de Mensajes Cortos – Difusión Celular).

2.5.5 Servicios Suplementarios

Las interacciones entre los operadores específicamente para servicios suplementarios no están definidas. Un servicio suplementario modifica o complementa un servicio básico de telecomunicaciones. Consecuentemente, no se puede ofrecer al usuario como un servicio aislado. Debe ser ofrecido en conjunto o en asociación con un servicio básico de telecomunicaciones. Los mismos servicios suplementarios pueden ser aplicados a un número de servicios básicos.

Se utilizan dos métodos para caracterizar los servicios suplementarios:

- El primer método es utilizado para la descripción de los servicios suplementarios estandarizados existentes. Estos servicios se especifican a través del detalle de cada una de las operaciones involucradas en la provisión del servicio y el uso del servicio (operaciones como: aprovisionamiento/retiro, registro/borrado, activación/desactivación, invocación e interrogación).
- El segundo método habilita la provisión de servicios suplementarios específicos HE Home Enviroment (Ambiente Local) / SN Serving Network (Red de Servicio). Para hacer posible los servicios, éstos pueden ser construidos utilizando las características de las capacidades de servicio, las cuales son accedidas a través de la interfaz de aplicación estandarizada.

Una PLMN debe ser capaz de manejar múltiples servicios suplementarios junto a una llamada. Las interacciones deben ser manejadas cuando varios servicios suplementarios están activos en la misma llamada. Cuando se pueden activar varios servicios concurrentemente, debe existir una priorización de dichos servicios. Más detalle de los servicios suplementarios se encuentra en la especificación TS 22.004 del 3GPP.

2.5.6 Características de las Capacidades de Servicios.

Las características de las capacidades de los servicios están abiertas, la tecnología diseña bloques accesibles a través de una interfaz de aplicación estandarizada. Esta interfaz puede aplicarse a un número diferente de negocios y dominios de aplicaciones.

Todos los negocios poseen diferentes requerimientos como: la telefonía simple y direccionamiento de llamadas, redes privadas virtuales, multimedia interactiva completa para aplicaciones basadas en UE.

Más detalles se encuentran en la especificación TS 22.121 del 3GPP.

Las características de las capacidades de servicio habilitan aplicaciones para hacer uso de las capacidades de servicio de una red en una forma abierta y segura. Se distinguen dos diferentes tipos de características en las capacidades del servicio:

- Características de capacidades del servicio con Estructura: éstas proporcionan utilidades comunes y necesarias para que las características de las capacidades del servicio no estructurado puedan ser accesibles, seguras, flexibles y manejables.
- Características de capacidades del servicio no estructurado: éstas deben habilitar las aplicaciones para hacer uso de la funcionalidad de las capacidades de red (por ejemplo: características de las capacidades del servicio de localización de usuarios entre otras).

2.5.7 Requerimientos de Desempeño.

- **Conversaciones en Tiempo Real.**

El uso más conocido de este esquema es la telefonía de voz (por ejemplo: GSM), pero con el Internet y la multimedia existe un nuevo número de aplicaciones que

necesitan de este esquema, por ejemplo: la voz sobre IP y las herramientas de video conferencia.

El esquema de conversación en tiempo real está caracterizado porque el tiempo de transferencia debe ser bajo debido a la naturaleza de la conversación del esquema y al mismo tiempo, la relación de variación en tiempo entre las entidades de información del flujo debe ser preservado en la misma forma que lo es para el flujo en tiempo real. El retraso máximo de transferencia viene dado por la percepción humana de las conversaciones de video y audio.

Una aplicación de streaming en tiempo real, es una que entrega información basada en el tiempo, en la cual los datos de usuario poseen un componente de tiempo intrínseco. El video y audio son ejemplos de información basada en el tiempo y consisten de una secuencia continua de bloques de datos que deben ser presentados al usuario en la secuencia correcta a instantes predeterminados.

- *Conversación de Voz.*

Los requerimientos en el retraso de transferencia de audio dependen del nivel de interactividad de los usuarios finales. Para prevenir las dificultades relacionadas a las comunicaciones dinámicas de voz, se han definido los límites generales para el tiempo de transmisión en un sólo sentido, mostrados en la tabla 2.9.

El oído humano es totalmente intolerable a las variaciones en el retraso (jitter[Ψ]) es por ello que los retrasos superiores son reducidos al nivel más bajo como sea posible prácticamente. Un límite tan bajo como 1ms es sugerido como objetivo.

Los requerimientos para la pérdida de información están influenciados por el hecho de que el oído humano es tolerante a cierta cantidad de distorsión en una señal de voz, el desempeño aceptable se obtiene hasta con FER Frame Error Rate (Tasa de Tramas Erróneas) de 3%.

[Ψ] Referirse al glosario

Tabla 2.9 Límites para el tiempo de transmisión.

Rango de retraso	Rango de percepción por el oído humano
0 ~ 150 ms	Rango preferido (< 30 ms, el usuarios no percibe ningún retraso; < 100 ms, el usuario no percibe ningún retraso sí se aplica la cancelación de eco y no existen distorsiones en el enlace).
150 ~ 400 ms	Rango aceptable (pero con incremento en la distorsión).
> 400 ms	Rango inaceptable.

- *Videotelefonía*

Implica un sistema full-duplex que lleva tanto video como audio, pretendido para el uso en un ambiente conversacional. Así como, posee los mismos requerimientos de retraso que una conversación de voz, por ejemplo: cancelación de eco y efecto mínimo sobre conversaciones dinámicas con el requerimiento adicionado que tanto video como audio deben de estar sincronizados con ciertos límites para proporcionar «lip-sync» (sincronización de los labios de los hablantes con las palabras que están siendo escuchadas por el usuario final). El ojo humano es tolerante con algunas pérdidas de información, es por ello que el grado de pérdida de algunos paquetes es aceptable dependiendo del codificador específico de video y la cantidad de protección de errores utilizada.

- *Juegos Interactivos*

Los requerimientos para los juegos interactivos son obviamente muy dependientes del juego en particular, la demanda de aplicaciones requerirá retrasos muy cortos y se propone un valor de 250ms consistente con la demanda de las aplicaciones interactivas.

- *Control de Telemetría en dos Sentidos*

Está incluido como un ejemplo de servicio de datos, el cual requiere un desempeño de streaming en tiempo real. Claramente, el control en dos sentidos implica límites bien ajustados sobre los retrasos permisibles y se propone también un valor de 250ms, pero una diferencia con los servicios de video y voz en esta categoría es la tolerancia cero a la pérdida de información.

- *TELNET*

TELNET Telecommunication Network (Red de Telecomunicaciones) está incluido para un requerimiento corto de retraso con el fin de proporcionar esencialmente una respuesta a los comandos de manera instantánea.

- **Servicios Interactivos.**

Cuando el usuario final, que puede ser una máquina o un humano, está en línea solicitando datos desde un equipo remoto (ejemplo: un servidor) se aplica este esquema. Algunos ejemplos de interacción humana con equipos remotos son: el buscador Web, almacenamiento en base de datos, acceso a servidores. Ejemplos de interacción de máquinas con equipos remotos son: elección para almacenamiento de mediciones e interrogaciones automáticas en base de datos.

El tráfico interactivo es otro esquema de comunicación de datos clásico que a nivel global es caracterizado por la solicitud del patrón de respuesta del usuario final. En el destino del mensaje existe una entidad esperando por el mensaje (respuesta) en cierto tiempo. El retraso del tiempo de viaje es uno de los atributos clave. Otra característica es que el contenido de los paquetes debe ser transferido de forma transparente (con un bajo error de velocidad de bit).

Los requerimientos globales resultantes para este esquema de comunicación son: soportar servicios interactivos en tiempo diferido con un retraso de tiempo de viaje bajo.

Las clases de servicio interactivo son:

- Mensajería y dictado de voz: Los requerimientos para la pérdida de información son esencialmente los mismos que para una conversación de voz, pero una diferencia es que existe más tolerancia para el retraso ya que no está involucrada una conversación directa. El problema principal se convierte, en cuánto retraso puede ser tolerado entre el usuario que emite un comando para repetir el mensaje de voz y el inicio del audio. Un retraso que fluctúe entre unos pocos segundos es razonable para esta aplicación.
- Datos: Aunque existen algunas excepciones, como una regla general se asume que desde el punto de vista del usuario, el primer requerimiento para cualquier aplicación de transferencia de datos es el de garantizar esencialmente cero pérdida de información. Al mismo tiempo, no se aplica una variación en el retraso. Las diferentes aplicaciones por consiguiente, intentan distinguirse sobre la base de un retraso el cual puede ser tolerado por el usuario final desde el momento en que el contenido fuente es solicitado hasta que es presentado al usuario.
- Buscador Web: En esta categoría se hará referencia al almacenamiento y despliegue del contenido HTML de una página Web, otros componentes que están separados bajo diferentes categorías son: las imágenes, los clips de audio y los clips video. Desde el punto de vista del usuario, el principal factor de desempeño es que tan rápida aparece una página después de haber sido solicitada. Se propone un valor de 2 a 4 segundos por página.
- Servicios de Transacción de Alta Prioridad (e-commerce[49]): El principal requerimiento de desempeño en este servicio es el de proveer al usuario un sentido de inmediatez en la transacción. Se sugiere un valor aceptable para los usuarios de 2 a 4 segundos.

[49] Comercio electrónico

- Correo Electrónico (acceso a servidor): El correo electrónico se piensa generalmente como un servicio de almacenamiento y envío, el cual en un principio puede tolerar retrasos de varios minutos o aún horas. Se propone un requerimiento de 2 a 4 segundos.

- **Servicios de Streaming.**

Cuando el usuario está observando video o escuchando audio se aplica el esquema stream. El flujo de datos en tiempo real es siempre entregado a un destino humano y es un transporte en un sólo sentido.

Este esquema es uno de los nuevos servicios dentro de la comunicación de datos, agregando nuevos requerimientos para ambos sistemas, el de telecomunicaciones y el de comunicación de datos. Primero, éste es principalmente un stream unidireccional con una utilización continua muy alta (ejemplo: tiene pocos períodos de silencio o reposo). También se caracteriza porque las relaciones de variación del tiempo entre las entidades de información (ejemplo: muestreo y paquetes) junto con el flujo deben ser preservados, aunque éste no tiene ningún requerimiento sobre el bajo retraso de transferencia.

La variación del retraso del flujo punto a punto debe ser limitada para preservar la relación de tiempo entre las entidades de información del stream. Pero como un stream normalmente está sincronizado en el tiempo para la recepción (equipo de usuario), la mayor variación de retraso aceptable sobre una transmisión de medios viene dada por la capacidad de la función de almacenamiento en el tiempo de la aplicación (buffer). La variación del retraso aceptable es mucho más grande que la variación de retraso dada por los límites de la percepción humana.

Los resultados del requerimiento global para este esquema de comunicación son: soportar servicios de streaming en tiempo real teniendo un flujo de datos unidireccional de utilización continua. (Existen menos requerimientos rigurosos sobre el retraso y la pérdida de paquetes).

Las clases de servicio de streaming son:

- Audio Streaming: Se espera que proporcione mejor calidad que la telefonía convencional y requerimientos para pérdidas de información en términos de paquetes perdidos, el cual será correspondientemente ajustado.
- Video en un sólo Sentido: La característica principal que distingue al video en un solo sentido es que no hay un elemento conversacional involucrado, lo que significa que el requerimiento de retraso no será estricto y puede seguir al del streaming de audio.
- Descarga de Datos: Esta categoría incluye la transferencia de archivos y está influenciada por el tamaño del archivo. También existe una indicación de que la transferencia del archivo está en proceso.
- Imagen Instantánea: Esta categoría incluye una variedad de formatos de codificación algunos de los cuales pueden soportar pérdida de información, ya que éstos son vistos por el ojo humano. Sin embargo, dado que aún los errores de bit simples pueden causar disturbios grandes en otros formatos de imágenes instantáneas, esta categoría debería tener en general cero pérdida de información. Los requerimientos de retraso para la transferencia de imágenes no están restringidos.
- Telemetría: El monitoreo cubre un amplio rango de aplicaciones, pero esta categoría se ha tenido que aplicar a las actividades de baja prioridad, por ejemplo: actualización de estado en un lugar de control.

- **Aplicaciones de Background**

Cuando el terminal final (que típicamente es una computadora) envía y recibe archivos de datos en segundo plano, se aplica este esquema. Algunos ejemplos son: la entrega de correos electrónicos, SMS, descargas de bases de datos y recepción de mediciones almacenadas.

El tráfico de background es uno de los esquemas de comunicación de datos clásico que a nivel global está caracterizado por que el destino no está a la expectativa de los datos en un tiempo dado. El esquema es una entrega más o menos independiente del tiempo. Otra característica es que el contenido de paquetes debe ser transferido transparentemente (con un BER mínimo).

El único requerimiento para las aplicaciones de esta categoría es que la información debe ser entregada al usuario esencialmente libre de errores. Sin embargo, existe aún un límite de retraso ya que los datos son efectivamente inútiles sí éstos se reciben demasiado tarde para cualquier propósito práctico.

Las clases de servicios de Background son:

- Facsímil (fax): Está incluido en esta categoría ya que no está normalmente entendido que sea un acompañamiento de comunicación en tiempo real. No obstante, existe una expectación en la mayoría de los escenarios de negocio que un fax será recibido en alrededor de 30 segundos. Los requerimientos de pérdida de información están basados sobre los requerimientos alámbricos establecidos para el grupo fax 3[50]. Para la simetría, éste deberá proporcionar la velocidad de transferencia requerida en la dirección de envío y el control de señalización en la otra dirección, debido a que se requiere una conexión asimétrica.
- Servicios de transacciones de baja prioridad: Un ejemplo de esta categoría es el SMS y se ha propuesto un tiempo de 30 segundos como valor de retraso en la entrega.
- Correo electrónico (servidor a servidor): El principal interés en el correo electrónico está en el tiempo de acceso. Existe una amplia expectativa con respecto al servicio con un valor medio de algunas horas.

[50] La ITU definió en 1974 una norma mundial, para establecer los periodos de entrega para un FAX, mejor conocida como “Grupos”. El grupo 3 fue creado en 1980, se basa en las recomendaciones UIT-T T.30 y T.4. Tardan entre 6 y 15 segundos en transmitir una sola página (sin incluir el tiempo inicial de sincronizado e identificación de las máquinas), a una velocidad de 14.400 Kbps.

2.6 CALIDAD DE SERVICIO EN UMTS

La QoS es un conjunto de parámetros o atributos establecidos a lo largo de la ruta de transporte de un servicio con el fin de garantizar una buena presentación del servicio al usuario. Estos atributos se encuentran dentro del portador de UMTS, el cual se define como el conjunto de recursos de red asignados que forman un «caudal» de bits con el fin de cumplir con los requisitos de QoS y proporcionar una respuesta a una solicitud de servicios que realiza el usuario final.

Cada servicio impone sus propios requisitos. Los atributos de la QoS son:

- Clases de Tráfico: conversacional, streaming, interactivo y background.
- Velocidad Binaria Máxima: Es el límite superior de velocidad que puede proporcionársele a un usuario final.
- Velocidad Binaria Garantizada: Los atributos de servicio de los portadores de UMTS como el retardo y la fiabilidad, están asegurados hasta dicha velocidad y por encima de este límite no se garantizan los atributos de QoS.
- Orden de Entrega: Este atributo indica si el portador debe o no entregar en orden las SDU.
- Tamaño Máximo de las SDU: Este atributo define el tamaño máximo de las SDU con el que la red debe satisfacer la QoS acordada o negociada.
- Tasa de Error de las SDU: Indica la cantidad de las SDU perdidas o eliminadas por ser erróneas.
- Tasa Residual de Bits Erróneos: Indica la tasa de bits erróneos no detectados en las SDU entregadas.
- Entrega de SDU Erróneas: Indica si se debe entregar o descartar las SDU detectadas como erróneas.

- Retardo de Transferencia: Indica el retardo máximo permitido por el percentil 95 de la distribución del retardo para todas las SDU entregadas durante la vida de un servicio portador.
- Tratamiento Prioritario del Tráfico: Especifica la importancia relativa que debe proporcionarse al tratamiento de todas las SDU para el portador de UMTS frente a las SDU de otros portadores.
- Prioridad de Asignación o Retención: Indica la importancia relativa de asignación y retención de un portador de UMTS en particular, frente a otros portadores.
- Descriptor de Estadísticas de los Recursos de Voz: Especifica las características de las SDU enviadas.
- Indicación de Señalización: Indica la naturaleza de la señalización de las SDU enviadas y únicamente se define para la clase de tráfico interactivo.

Tabla 2.10 Clases de tráfico y sus características

Clases de tráfico	**Características fundamentales**	**Ejemplos de Servicios**
Conversacional	Escaso retardo y escasa variación de retardo.	Voz, VoIP y videoconferencia
Streaming	Retardo y variación moderada (dependiendo de la aplicación del usuario final)	Streaming de video y de audio
Interactivo	El retardo de ida y de vuelta es importante. Variación de retardo moderada. Patrón de petición de respuesta.	Navegación Web

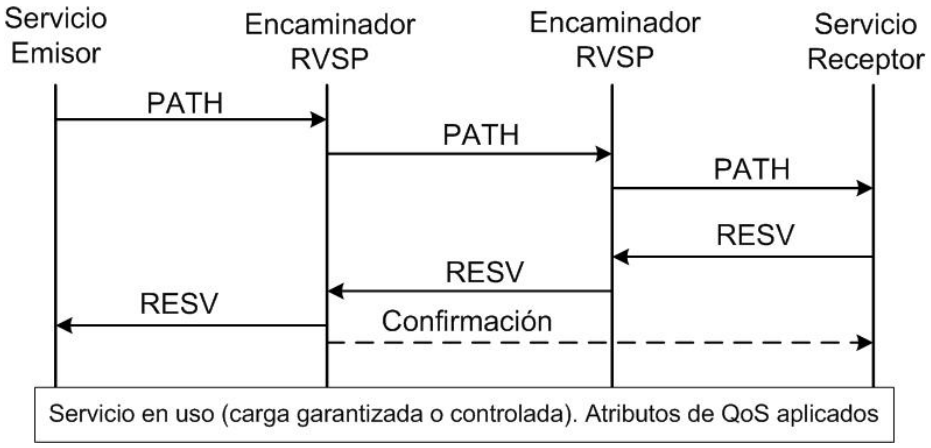
Background	El destino (aplicación del usuario final) no espera respuesta en un período concreto.	Correo electrónico y descarga de archivos

Se debe especificar que la QoS está garantizada dentro de la red UMTS para un servicio extremo a extremo, pero la garantía de la QoS para un servicio que se extiende fuera de los dominios de la red UMTS no se puede asegurar.

2.6.1 Protocolo de Reserva de Recursos

El RSVP Reservation Protocol (Protocolo para Reservación) funciona de la siguiente manera: el emisor describe los atributos de QoS que necesita para la transmisión, esta información la envía el RSVP en un mensaje llamado PATH a la dirección del receptor. Para reservar los recursos requeridos del mensaje PATH el receptor envía un mensaje RESV al emisor, el RESV pasa por una serie de enrutadores con soporte RSVP para llegar al emisor, este mensaje se encarga de reservar los recursos necesarios por cada enrutador por el que pasa. Sí los recursos necesarios son activados correctamente en el enrutador, éste pasa el mensaje RESV hacia el siguiente enrutador de lo contrario devuelve un mensaje de error hacia la dirección de origen. Cuando el último enrutador recibe el mensaje RESV, éste envía un mensaje de confirmación al receptor indicando que el trayecto está preparado para el tráfico y que cumple con las características de QoS especificadas. En la ruta entre el emisor y el receptor pueden existir enrutadores con o sin capacidad RSVP; en el caso de que el enrutador no tenga capacidad RSVP los mensajes del RESV pasan de forma transparente a través de ellos.

Figura 2.26 Funcionamiento del RSVP.



2.6.2 Servicios Diferenciados

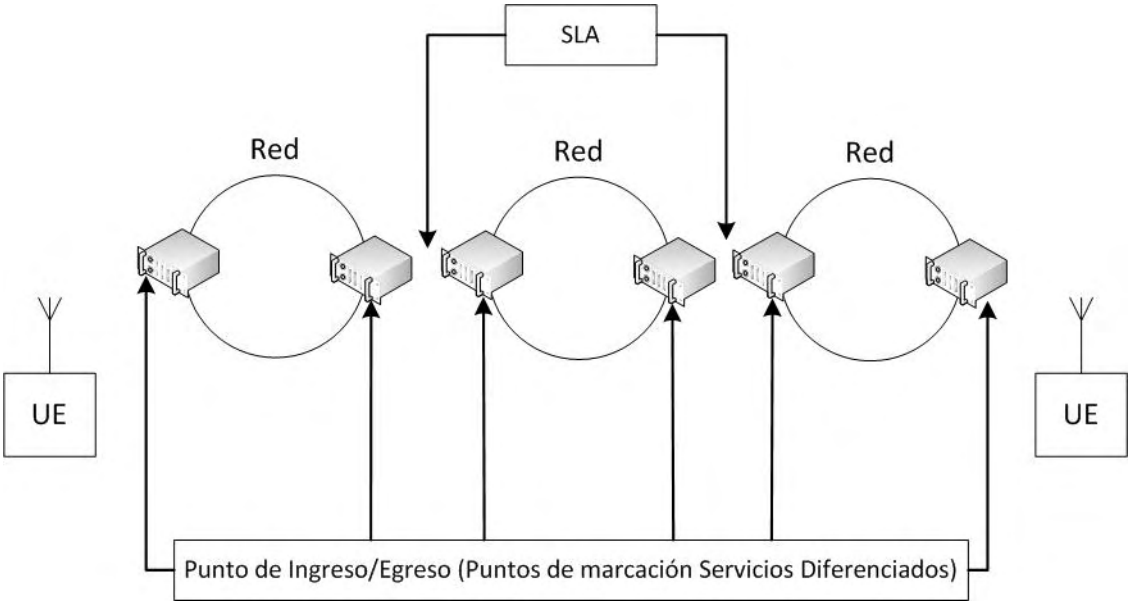
Los DiffServ Diffentiated Service (Servicios Diferenciados) son un método que clasifica los servicios para que puedan tratarse de manera diferente. Con DiffServ es posible tener varias clases de tráfico, pero sólo existen dos niveles de servicio o clases de transporte importantes:

- Envío Preferente (Expedited Forwarding): ésta clase minimiza el retardo y las fluctuaciones proporcionando así el nivel más alto de QoS. El tráfico que no cumple las definiciones de esta clase se descarta. El envió preferente implementa una sola categoría de tráfico de DiffServ.
- Envío Asegurado (Assured Forwarding): esta clase de tráfico puede dividirse en cuatro subclases y cada una en tres categorías para descartar paquetes. Es decir, contiene un total de 12 categorías.

El DiffServ es un protocolo interno de la red transparente a los usuarios finales. Este servicio se aplica a las conexiones del usuario final en los límites o fronteras de la red. En el contexto DiffServ la entrada en la frontera de la red se conoce como «punto de ingreso a la red», del mismo modo que el extremo opuesto de la

red (en donde se desechan las definiciones de DiffServ) se conoce como «punto de egreso de la red». De manera predeterminada DiffServ supone que existe un acuerdo de SLA Service Level Agreement (Acuerdo de Nivel de Servicio) entre las redes. El SLA define los parámetros técnicos que describen la calidad de la conexión entre las redes y en DiffServ se conoce como «criterios de políticas». Al tráfico se le aplica una política u otra, según los criterios de política de los puntos de ingreso y de egreso de la red.

Figura 2.27 Funcionamiento de DiffServ.



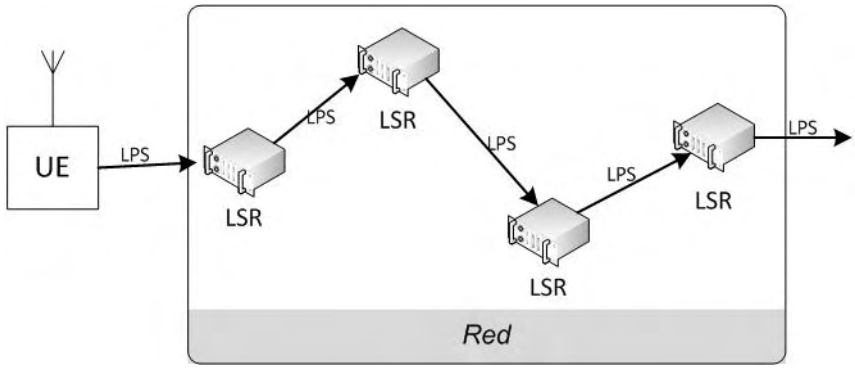
2.6.3 Conmutación de Etiquetas Multiprotocolo

La MPLS Multiprotocol Label Switching (Conmutación de Etiquetes Multiprotocolo) posee varias características en común con DiffServ, por ejemplo, este sistema también marca el tráfico en los puntos de ingreso y egreso a la red, sin embargo, el objetivo de MPLS es clasificar el tráfico del siguiente salto del enrutador. La

MPLS no está controlada por ninguna aplicación, no posee ningún componente de usuario final y se ubica únicamente en los servidores.

MPLS no depende de ningún protocolo y por lo tanto puede utilizar cualquier protocolo de transporte, en donde IP es la primera opción, pero una alternativa es ATM. Los enrutadores habilitados para MPLS reciben el nombre de LSR Label Switching Router (Encaminadores de Conmutación de Etiquetas). El primer LSR de la red recibe los paquetes y toma decisiones del envío de éstos basándose en la dirección de destino del paquete o en cualquier otra información que se incluya en la cabecera del mismo. La información que se utiliza para tomar decisiones depende de las políticas locales, el primer LSR coloca la etiqueta correspondiente al paquete y lo envía al siguiente LSR.

Figura 2.28 Funcionamiento de MPLS



Al recibir la información el siguiente LSR analiza el paquete. Esta etiqueta cumple la función de puntero que señala una tabla en la que incluye por un lado más información indexada sobre el siguiente salto y una nueva etiqueta para el paquete. El LSR coloca esta nueva etiqueta al paquete y lo envía hacia adelante. Este procedimiento se repite las veces que sea necesario, el número de LSR en la cadena a través de la que pasa el paquete es ilimitada y cada etiqueta MLPS es diferente. Esta cadena se denomina LSP Label Switching Path (Ruta Conmutada

por Etiquetas). Sí la información de configuración es correcta y las tablas de encaminamiento son válidas en todos los LSR de la red, el LSP reunirá los requisitos QoS desde el punto de ingreso de la red hasta el punto de egreso.

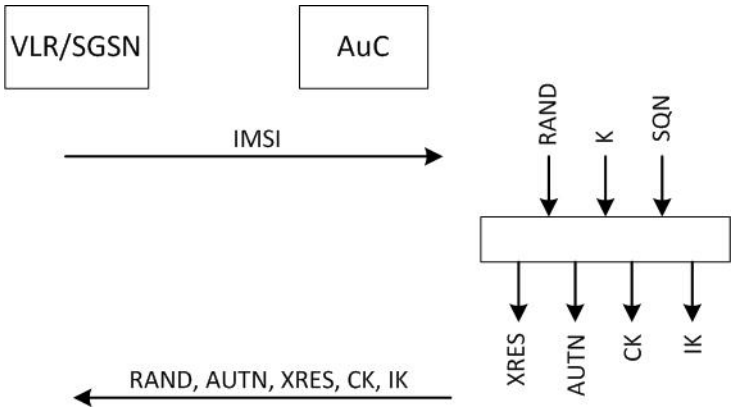
2.7 SEGURIDAD EN UMTS

2.7.1 Seguridad en la Red de Acceso

- **Autenticación Mutua**

En este mecanismo el CN comprueba la identidad del abonado mediante la técnica conocida como «solicitud y respuesta», mientras el terminal comprueba si se está conectando a una red legítima. La esencia del mecanismo de autenticación es una clave maestra «K» que comparte el USIM del usuario y la base de datos de la red. Se trata de una clave permanente y secreta de una longitud de 128 bits. La clave «K» nunca se hace visible entre dos ubicaciones, ni siquiera el usuario conoce su clave maestra.

Figura 2.29 Solicitud y repuesta de los datos de autenticación

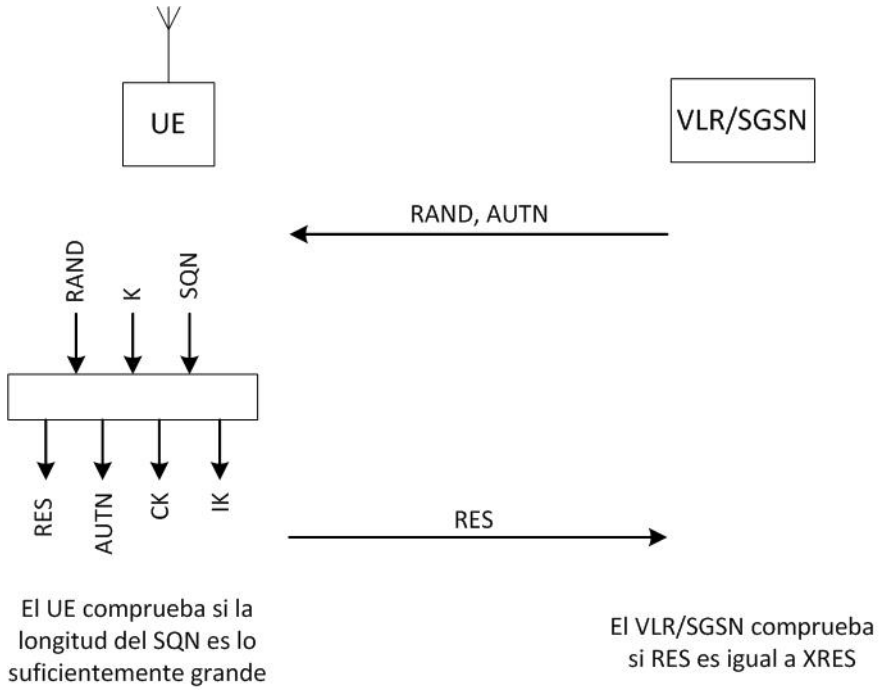


Al mismo tiempo que se realiza la autenticación mutua se obtienen las claves de cifrado y se realiza la comprobación de la integridad. Éstas son claves temporales

con la misma longitud (128 bits). Durante cada autenticación se obtienen nuevas claves a partir de la clave permanente «K». Uno de los principios básicos de la criptografía es reducir al mínimo el uso de la clave permanente «K» y utilizar como alternativa una clave temporal derivada de «K».

A continuación se describe el mecanismo de AKA Authentication and Key Agreement (Autenticación y Acuerdo de Clave). La identificación se realiza cuando se transmite la identidad del usuario (como la IMSI o la TMSI) al VLR/SGSN, después el VLR/SGSN envía la solicitud de datos de autenticación al AuC y éste guarda las claves maestras de los usuarios, basándose en el conocimiento de la IMSI genera los AV Authentication Vector (Vectores de Autenticación) para el usuario. Los vectores generados se envían de vuelta al VLR/SGSN mediante el protocolo MAP.

Figura 2.30 Autenticación de usuario.



El VLR/SGSN envía una solicitud de autenticación de usuario al terminal, este mensaje contiene dos parámetros del AV llamados RAND y AUTN Authentication Token (Ficha de Autenticación) que son transferidos al USIM. El USIM posee la clave maestra «K» y utiliza como parámetros de entrada el RAND y el AUTN, además, realiza el cálculo de forma similar al utilizado para generar los AV en el AuC. Con el resultado del cálculo, el USIM podrá verificar si el parámetro AUTN se generó en el AuC para descartar una falsa red intentando conectarse al terminal. Sí se comprueba que el parámetro se generó en el AuC se envía un parámetro RES Authentication Response (Respuesta de Autenticación) al VLR/SGSN, entonces este último puede comparar las respuestas RES con el XRES Expected RES Value (Valor RES Esperado) esperado que forma parte del AV, sí estas coinciden el proceso concluye correctamente.

Las claves CK Ciphering Key (Clave de Cifrado) para la RAN y la IK Integrity Key (Clave de Integridad) para la protección de la integridad se crean como consecuencia del proceso de autenticación. Estas claves temporales se incluyen en el AV y por lo tanto, se transfieren al VLR/SGSN desde donde se transfiere al RNC cuando comienza el cifrado y el proceso de protección de la integridad. En el otro extremo el USIM también puede calcular la CK e IK para el cifrado y la protección de la integridad.

- **Criptografía para la Autenticación**

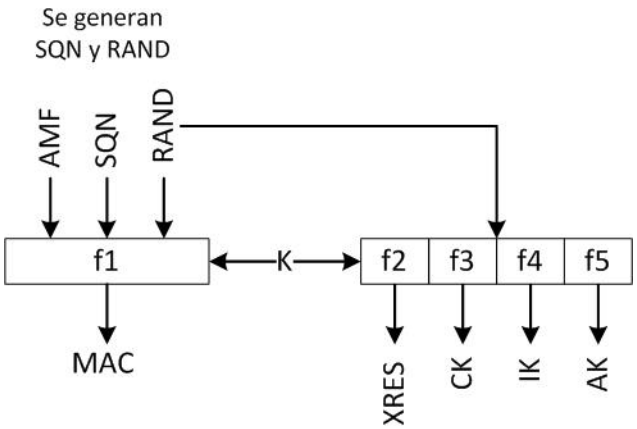
El proceso para generar los AV en el AuC comienzan eligiendo un SQN Sequence Number (Número de Secuencia) correcto. Es necesario que los SQN se seleccionen en orden ascendente, ya que la finalidad de éstos es probar que los vectores de autenticación no han sido utilizados anteriormente. Paralelamente a la elección del SQN se genera una cadena de bits aleatoria RAND de 128 bits.

Para generar los vectores de autenticación se utilizan funciones de un sólo sentido[51]. Con los parámetros de entrada es relativamente fácil cálcular los parámetros de salida, pero teniendo los parámetros de salida es prácticamente imposible averiguar los parámetros de entrada.

En total se emplean cinco funciones de un sólo sentido para calcular el AV (f1, f2, f3, f4 y f5). Es básico que las funciones sean diferentes entre si y que el resultado de una función no conduzca a la deducción de la información de las demás.

La f1 toma como parámetro de entrada a «K», SQN, RAND y AMF Authentication Management Field (Campo de Gestión de Autenticación) y obtiene el MAC Message Authentication Code (Código de Autenticación del Mensaje) de 64 bits como se observa en la Figura 2.31, en donde también se muestra el procedimiento de autenticación en el extremo del USIM.

Figura 2.31 Generación de los vectores de autenticación.



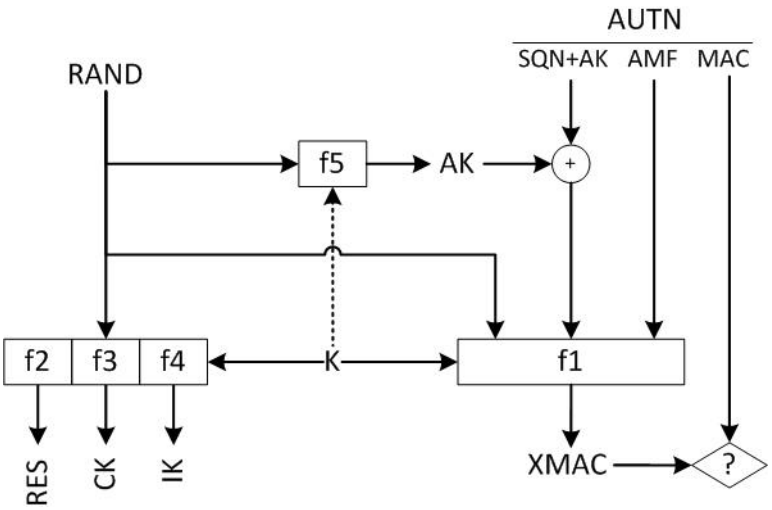
El parámetro AUTN que recibe el USIM de la red contiene a: SQN, AK Anonimity Key (Clave Anónima), AMF y MAC, a través de la f1 se calcula el XMAC Expected MAC Value (Valor MAC Esperado) y se compara con el MAC que se recibió del

[51] Funciones matemáticas sencillas de calcular pero prácticamente imposible de invertir.

parámetro AUTN. Si coinciden significa que RAND y AUTN han sido creados por el AuC de la red del usuario. Sin embargo, cabe la posibilidad de que algún impostor que haya grabado una autenticación anterior pueda reproducir los parámetros RAND y AUTN por lo que el SQN se encarga de neutralizar esta amenaza. La USIM debe comprobar que no se ha utilizado ya el mismo SQN y la forma más sencilla de hacerlo es de exigir que los SQN vayan apareciendo de forma ascendente.

La elección entre los algoritmos f1 a f5 es específica de cada operador, ya que es éste quien controla a las entidades que se emplean (el USIM y el AuC). En la especificación TS 35.206 de 3GPP se incluye un conjunto de algoritmos, como por ejemplo: el llamado «MILENAGE».

Figura 2.32 Procedimiento de autenticación en el USIM.



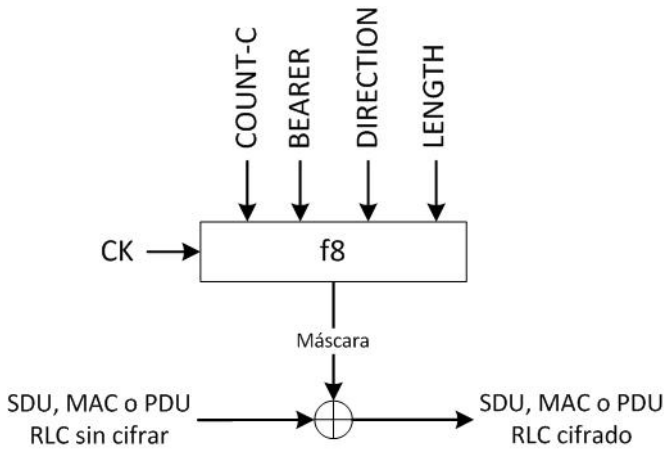
- **Cifrado en la UTRAN**

Una vez que el usuario y la red se han autenticado entre si, pueden comenzar a proteger la comunicación. Como ya se ha visto, se comparte una CK entre el CN y el terminal después de concluir correctamente una autenticación. Antes de

comenzar un cifrado las partes deben acordar un algoritmo de cifrado. El cifrado como el descifrado se realizan en el terminal y en el RNC, lo que significa que la CK debe transferirse del CN a el RNC, para ello se utiliza un mensaje específico del protocolo RANAP conocido como «comando de modo de seguridad».

El mecanismo de cifrado de UMTS se fundamenta en el concepto de cifrado de flujo, lo que significa que los datos de texto no cifrados se añaden bit a bit a unos datos de máscara de apariencia aleatoria generados a partir de la CK y algunos otros parámetros como se ve en la Figura 2.33. El descifrado en la parte que recibe el mensaje se realiza añadiendo la misma máscara a los datos cifrados, ya que añadiendo a los datos la máscara dos veces esta se cancela dejando los datos originales.

Figura 2.33 Cifrado de datos en la interfaz de radio.



Para generar el COUNT-C (que es una entrada dependiente de tramas para f8), se utiliza el HFN Hiper Frame Number (Número de Hipertrama) combinado con un contador dependiendo en donde se realice el cifrado. Si se realiza en la capa MAC el HFN se combina con CFN Conection Frame Number (Número de Trama de

Conexión) y si se realiza en la capa RLC se combina con el RLC-SQN[52]. Esto hace que el COUNT-C siempre varíe, de esta forma las máscaras también serán diferentes para cada cifrado.

La «BEARER» (es la identidad del portador de radio) también es un parámetro de entrada para la generación de la máscara con el fin de generar distintas máscaras en distintos portadores, debido a que el COUNT-C puede repetirse en los portadores.

La esencia del mecanismo de cifrado explicado es el algoritmo f8, el cual se encuentra en la TS 35.201 de 3GPP y se basa en un nuevo cifrado por bloques llamado «KASUMI» el cual se especifica en la TS 35.202 de 3GPP.

2.7.2 Protección de la Integridad de la Señalización RRC

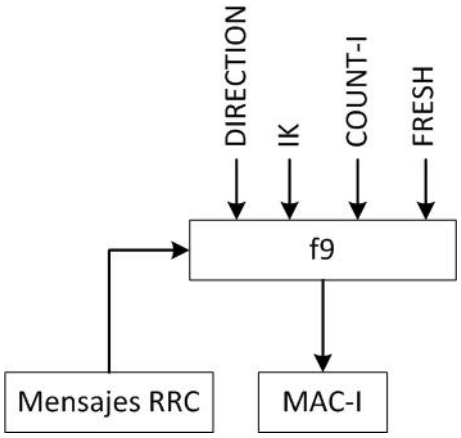
El propósito de esta operación es autenticar individualmente los mensajes de control para evitar que un Nodo B falso se inmiscuya en la conexión del usuario. Un Nodo B falso podría enviar todos los mensajes de forma correcta hasta terminar el proceso de autenticación, luego puede comenzar a manipular los mensajes a su antojo. Esta protección se implementa sobre la capa del RRC con la clave IK, la cual se genera durante el procedimiento AKA y se transmite del CN al RNC a través de un mensaje RANAP.

El algoritmo f9 depende del cifrado por bloques KASUMI y se encuentra en la especificación TS 35.2010 del 3GPP.

En la Figura 2.34 se muestra el procedimiento para proteger la integridad de la señalización RRC.

[52] RLC-SQN Radio Link Control – Sequence Number (Número de Secuencia del Control de Radio Enlace)

Figura 2.34 Cifrado de señalización RRC



El concepto sobre el que se sustenta el mecanismo de protección de integridad, es una función de un sólo sentido controlada por la clave secreta IK y que se representa como f9. El resultado de esta función es la MAC-I[53] que es una cadena de 32 bits de apariencia aleatoria. La cadena MAC-I se añade a cada mensaje RRC y también se genera y se comprueba en el extremo de recepción, se sabe que cualquier cambio que se produzca en los parámetros de entrada de la f9 influye en la MAC-I de manera impredecible.

Como entradas para f9 se emplean: la IK, el propio mensaje RRC, un contador COUNT-I (Entrada dependiente de tramas para f9), el bit de dirección (ascendente o descendente) y el FRESH (Número aleatorio que elige el RNC y que sólo se utiliza una vez). Al igual que en el cifrado, el COUTN-I garantiza valores diferentes de entrada para cada ejecución del f9. El parámetro FRESH se transmite al UE.

Hay algunos mensajes de control de RRC que no se pueden proteger con este mecanismo, como los mensajes enviados antes de que se comience a aplicar la IK, por ejemplo: el mensaje de solicitud de conexión de RRC.

[53] La letra «I» proviene de “Integridad”.

2.7.3 La Seguridad en el CN

- **Seguridad IP**

Ésta se provee a través de IPSec que fue estandarizado por la IETF. Los principales componentes de IPSec son:

- AH Authentication Header (Cabecera de Autenticación).
- ESP Encasulation Security Payload (Carga Útil Encapsulada para Seguridad).
- IKE Internet Key Exchange (Intercambio de Claves de Internet).

La finalidad de IPSec es proteger los paquetes IP y de eso se encarga ESP y AH. ESP ofrece confidencialidad y protección de la integridad, mientras AH únicamente protege la integridad. Tanto ESP como AH necesitan claves. Una SA contiene información sobre el algoritmo utilizado e información de validez de las claves. Las SA deben negociarse para que puedan utilizar ESP y AH, la negociación tiene lugar en modo seguro mediante el protocolo IKE. El IKE se basa en la criptografía de clave pública con la que se pueden intercambiar claves secretas para comunicaciones seguras sobre un canal no seguro.

Existen dos tipos de ESP:

- ESP de Modo de Transporte: aquí se cifra toda la información de los paquetes IP con excepción de la cabecera, entonces se añade una nueva cabecera ESP entre la cabecera IP y la parte cifrada, en las que se incluye el ID y la SA en uso, además, el proceso de cifrado suele añadir algunos bits adicionales. Por último, se calcula un MAC de toda la información excepto de la cabecera IP y se añade al final del paquete. En el extremo de recepción se comprueba la integridad del paquete y para ello se suprime la cabecera IP del principio del paquete y el MAC del final, entonces al paquete restante se le ejecuta un algoritmo utilizando la clave que se

encuentra en la cabecera ESP; el resultado se compara con la MAC del paquete, sí el resultado es positivo se elimina la cabecera ESP y se descifra la parte restante usando la información de la misma.

- ESP en Modo para Túneles: es igual que el modo de transporte, con la diferencia de que la cabecera IP se añade al comienzo para proteger a la cabecera original.

- **MAPSec**

Los mensajes MAP son utilizados como medio de señalización dentro del CN. El objetivo del MAPSec MAP Security (Seguridad MAP) es proteger la integridad de estas operaciones.

La funcionalidad de MAPSec consiste en las operaciones siguientes: se cifra un mensaje MAP de texto no cifrado y se coloca el resultado en un «contenedor» dentro de otro mensaje MAP. Al mismo tiempo se incluye en un nuevo mensaje MAP una suma de control criptográfica, es decir, una MAC que cubre el mensaje original. Para el cifrado y las MAC se necesitan claves. El MAPSec ha copiado el concepto de las SA de IPSec. La SA no solo contiene claves criptográficas sino que incluye también información relevante, como por ejemplo: los períodos de validez de las claves y los identificadores de algoritmos.

2.7.4 Seguridad en el Subsistema IMS de la CN

La especificación de seguridad para el IMS se puede obtener en la especificación TS 33.203 de 3GPP.

- **Autenticación y Acuerdo de Claves**

Cuando el usuario llega a un acuerdo con el operador de IMS se asigna al usuario una IMPI que se guarda en la ISIM y el HSS. El IMPI también guarda una clave maestra criptográfica de 128 bits.

Para que un suscriptor pueda comenzar a utilizar los servicios del IMSI, es necesario activar su registro enviando un mensaje «REGISTER» a una función P-CSCF y ésta envía el REGISTER a una función I-CSCF la cual se pone en contacto con el HSS para que se le asigne una función S-CSCF adecuada. Todas estas comunicaciones y las que tienen lugar a continuación entre los elementos de red son protegidas mediante métodos de seguridad.

Después de seleccionar una S-CSCF, se le envían los mensajes REGISTER y ésta toma los AV del HSS. Estos vectores tienen el mismo formato que los utilizados en el dominio PS y CS. Posteriormente la S-CSCF forma el primer AV y envía tres o cuatro parámetros (excluyendo la XRES y la CK) a la función P-CSCF a través de la I-CSCF. La P-CSCF extrae la IK, pero envía al UE los parámetros RAND y AUTN. Si el mensaje SIP utilizado para transmitir toda esta información es el «401 UNAUTHORIZED», el primer intento de registro es fallido.

Aún así, el ISIM del UE puede comprobar ahora la validez del AUTN y sí el resultado es positivo se calculan los parámetros RES e IK. El parámetro RES se incluye en una nueva solicitud REGISTER, con la integridad protegida en esta ocasión por la IK.

La protección de la integridad se consigue utilizando el protocolo ESP de IPSec. El nuevo REGISTER se dirige primero a la función P-CSCF y desde allí se envía a través del I-CSCF al S-CSCF. Esta función compara el parámetro RES con XRES y sí coincide envía un masaje «OK» devuelta hasta el UE.

Con esto concluye el procedimiento AKA y el resultado es:

- El UE y el P-CSCF comparten la SA y el protocolo IPSec, las cuales se pueden utilizar para proteger las comunicaciones que se establezcan entre ellos.
- En S-CSCF y en HSS, el estado del suscriptor ha pasado de «no registrado» a «registrado».

La función S-CSCF siempre indica un AKA en el momento del registro inicial. En posteriores registros se podría omitir este paso, dependiendo de las opciones elegidas en S-CSCF. También es posible que S-CSCF fuese un nuevo registro del UE en cualquier momento, es decir, S-CSCF puede autenticar al UE siempre que lo crea necesario.

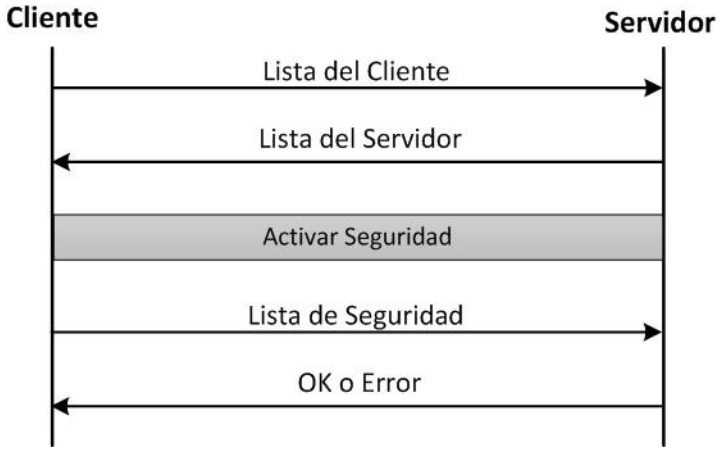
SIP es un protocolo del la IETF sobre el cual el IMS necesita sus propias extensiones. Una de estas extensiones es el uso de AKA de 3GPP para el procedimiento AKA mutuo. Se ha dedicado la RFC 3310 específicamente para este punto.

- **Protección de Mensajes SIP con IPSec**

La autenticación mutua no es suficiente para garantizar que todas las operaciones de tarificación se realicen para la suscripción correcta, por este motivo los mensajes de señalización SIP también se autentican individualmente. Esta medida es especialmente necesaria para los mensajes «INVITE» que son utilizados para establecer sesiones.

La protección de la integridad (autenticación de los mensajes) se lleva a cabo con el protocolo ESP de IPSec. El uso de la protección para la cabecera IP impone algunos requisitos adiciónales.

Figura 2.35 Flujo de mensajes de acuerdo de seguridad



Por un lado, la identidad con la que se compara la autenticación de los mensajes es la dirección IP en el caso de ESP. Por otra parte, la tarificación relacionada con la señalización IMS se basa en las identidades de IMS que sólo están visibles en la capa SIP. Por ello las identidades de esta capa espacialmente la IMPI tiene que estar relacionada de algún modo con la dirección IP. Este problema se solventa en P-CSCF comprobando mensaje por mensaje que la dirección IP utilizada para la protección de la integridad de la capa SIP está permitida para el IMPI en cuestión. El enlace entre la IP y el IMPI se crea originalmente durante el AKA, es decir, al tiempo que se crea el SA ESP.

- **Seguridad de la capa de sesión**

En la capa de sesión referente al modelo OSI se encuentra el protocolo SSL Sockets Security Layer (Capa de Sockets Seguros) o la TLS Transport Layer Security (Seguridad de Capa de Transporte). Un «socket» es una puerta de comunicación utilizada en redes IP, está constituida por una dirección IP y un puerto del protocolo de transporte utilizado.

El SSL fue desarrollado con el objetivo de proporcionar privacidad y fiabilidad en las comunicaciones mantenidas entre dos aplicaciones de la capa de sesión del modelo OSI.

Este protocolo utiliza el cifrado de clave pública para intercambiar las claves de las sesiones entre el cliente y el servidor. Esta clave de sesión se emplea para cifrar las transferencias de HTTP Hypertext Transfer Protocol (Protocolo de Transferencia de Hipertexto). Una sesión se conforma de varias transacciones las que son auntenticadas de forma individual (cada transacción utiliza una clave de sesión diferente) por lo que si alguien consigue descifrar una transacción, la sesión seguirá siendo segura por que únicamente se ha violado la seguridad de una transacción.