



Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

**PROPUESTA DE UN SISTEMA SSH/FTP DE INTERCONEXIÓN ENTRE EMPRESAS
DE TELEFONÍA EN GUATEMALA, PARA EL REPORTE AUTOMÁTICO Y
POSTERIOR BLOQUEO DE IMEI REPORTADOS COMO ROBADOS**

Esteban Mauricio Ortiz Osorio

Asesorado por el Ing. Christian Antonio Orellana López

Guatemala, agosto de 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**PROPUESTA DE UN SISTEMA SSH/FTP DE INTERCONEXIÓN ENTRE EMPRESAS DE
TELEFONÍA EN GUATEMALA, PARA EL REPORTE AUTOMÁTICO Y POSTERIOR
BLOQUEO DE IMEI REPORTADOS COMO ROBADOS**

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

ESTEBAN MAURICIO ORTIZ OSORIO

ASESORADO POR EL ING. CHRISTIAN ANTONIO ORELLANA LÓPEZ

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, AGOSTO DE 2016

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE INGENIERÍA



NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de Leon Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Raúl Eduardo Ticún Córdova
VOCAL V	Br. Henry Fernando Duarte García
SECRETARIA	Ing. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

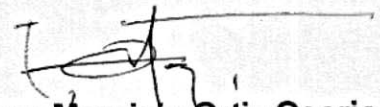
DECANO	Ing. Murphy Olympto Paiz Recinos
EXAMINADORA	Inga. María Magdalena Puente Romero
EXAMINADOR	Ing. Carlos Eduardo Guzmán Salazar
EXAMINADOR	Ing. Armando Alonso Rivera Carrillo
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

PROPUESTA DE UN SISTEMA SSH/FTP DE INTERCONEXIÓN ENTRE EMPRESAS DE TELEFONÍA EN GUATEMALA, PARA EL REPORTE AUTOMÁTICO Y POSTERIOR BLOQUEO DE IMEI REPORTADOS COMO ROBADOS

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 6 de julio de 2016.



Esteban Mauricio Ortiz Osorio

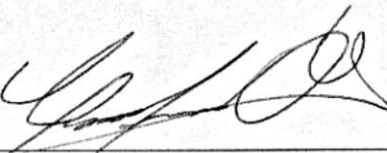
Guatemala, 20 de Julio de 2016

Ingeniero Carlos Guzmán
Coordinador de Área de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería

Señor coordinador,

Tengo el gusto de informar a usted que he concluido con el asesoramiento del trabajo de graduación con título: **"PROPUESTA DE UN SISTEMA SSH/FTP DE INTERCONEXIÓN ENTRE EMPRESAS DE TELEFONÍA EN GUATEMALA, PARA EL REPORTE AUTOMÁTICO Y POSTERIOR BLOQUEO DE IMEI REPORTADOS COMO ROBADOS"**, desarrollado por el estudiante Esteban Mauricio Ortiz Osorio, con carné 200313339. Después de revisar su contenido final, considero que cumple con los requerimientos necesarios y doy mi entera aprobación al mismo.

Atentamente,



Ing. Christian Antonio Orellana Lopez
Colegiado No. 11939





Ref. EIME 37. 2016.
Guatemala, 21 de julio 2016.

Señor Director
Ing. Francisco Javier González López
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado:
**PROPUESTA DE UN SISTEMA SSH/FTP DE INTERCONEXIÓN
ENTRE EMPRESAS DE TELEFONÍA EN GUATEMALA, PARA EL
REPORTE AUTOMÁTICO Y POSTERIOR BLOQUEO DE IMEI
REPORTADOS COMO ROBADOS,** del estudiante Esteban
Mauricio Ortiz Osorio, que cumple con los requisitos establecidos
para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Área Electrónica



sro



REF. EIME 37. 2016.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; ESTEBAN MAURICIO ORTIZ OSORIO, titulado: PROPUESTA DE UN SISTEMA SSH/FTP DE INTERCONEXIÓN ENTRE EMPRESAS DE TELEFONÍA EN GUATEMALA, PARA EL REPORTE AUTOMÁTICO Y POSTERIOR BLOQUEO DE IMEI REPORTADOS COMO ROBADOS, procede a la autorización del mismo.

Ing. Francisco Javier González López



GUATEMALA, 3 DE AGOSTO 2016.



El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica al trabajo de graduación titulado: **PROPUESTA DE UN SISTEMA SSH/FTP DE INTERCONEXIÓN ENTRE EMPRESAS DE TELEFONÍA EN GUATEMALA, PARA EL REPORTE AUTOMÁTICO Y POSTERIOR BLOQUEO DE IMEI REPORTADOS COMO ROBADOS**, presentado por el estudiante universitario: **Esteban Mauricio Ortiz Osorio**, y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano



Guatemala, agosto de 2016

ACTO QUE DEDICO A:

- Dios** Por darme el conocimiento y sabiduría para alcanzar un logro más en mi vida, a él sea la gloria.
- Mis padres** Mario Ortiz López y Loida Osorio de Ortiz, por su apoyo incondicional durante toda mi carrera y por ser mi principal ejemplo de superación, perseverancia y amor a Dios.
- Mi esposa** Mariela Cardozo, por su amor, comprensión y apoyo en todo momento y por compartir conmigo su vida.
- Mi hija** Camila Ortiz Cardozo, por ser una de las partes más importantes de mi vida y una razón más para superarme.
- Mis hermanos y sobrinas** Por sus palabras de ánimo y por estar siempre presentes en los buenos y malos momentos por los que he pasado.

AGRADECIMIENTOS A:

**Universidad de San
Carlos de Guatemala**

Por permitirme formar parte de tan prestigiosa casa de estudios.

Facultad de Ingeniería

Por enseñarme con calidad para ser una persona productiva.

Ing. Christian Orellana

Por su valioso apoyo y asesoría durante la redacción del trabajo de graduación.

**Mis compañeros de
Universidad**

Por compartir tantos momentos durante el transcurso de nuestra carrera.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	III
LISTA DE SÍMBOLOS	V
GLOSARIO	VII
RESUMEN	XI
OBJETIVOS	XIII
INTRODUCCIÓN	XV
1. REDES DE TELEFONÍA CELULAR PARA SERVICIOS DE VOZ Y DATOS	1
1.1. Red 2G para servicios de voz	9
1.1.1. Principales estándares	11
1.1.2. Estándar GSM	18
1.1.3. Estándar GPRS y EDGE	22
1.1.4. Arquitectura de red 2G	30
1.2. Red 3G para servicios de transferencia de datos	39
1.2.1. Estándar UMTS	40
1.2.2. Estándar HSPA	45
1.2.3. Estándar HSDPA	47
1.2.4. Estándar HSUPA	52
1.2.5. Estándar HSPA+	54
1.2.6. Arquitectura de red 3G	55
2. PROTOCOLO DE SEÑALIZACIÓN SS7	61
2.1. Fundamentos básicos y características	61
2.2. Tipos de señalización	63

2.3.	Arquitectura	67
2.3.1.	Enlaces de señalización	68
2.3.2.	Rutas de señalización	74
2.3.3.	Puntos de señalización.....	75
2.3.3.1.	Signalling Point (SP)	75
2.3.3.2.	Service Switching Point SSP.....	75
2.3.3.3.	Signal Transfer Point (STP).....	77
2.3.3.4.	Service Control Point (SCP)	80
3.	SERVIDORES FTP Y SSH	81
3.1.	Sistema operativo Linux	81
3.1.1.	Shell Scripting	84
3.1.2.	Perl Scripting	87
3.2.	Protocolo FTP	88
3.3.	Protocolo SSH.....	90
4.	PROPUESTA DE UN SISTEMA SSH/FTP PARA EL REPORTE AUTOMÁTICO DE UN IMEI REPORTADO COMO ROBADO O EXTRAVIADO	93
4.1.	Creación de Shell Scripts	95
4.2.	Creación de Perl Scripts.....	97
4.3.	Creación rutinas automáticas	99
4.4.	Diagrama final del proceso	101
	CONCLUSIONES	107
	RECOMENDACIONES	109
	BIBLIOGRAFÍA	111

ÍNDICE DE ILUSTRACIONES

FIGURAS

1.	Estructura canal TDMA	17
2.	Bloque estación base	32
3.	Bloque conmutación de red.....	38
4.	Estructura canal HS-DPCCH.....	51
5.	Modo asociado.....	64
6.	Modo cuasi asociado	65
7.	Modo disociado	66
8.	Estructura base protocolo SS7	67
9.	Tipo de enlace de señalización	69
10.	Enlace A.....	70
11.	Enlace B.....	71
12.	Enlace C	71
13.	Enlace D	72
14.	Enlace E.....	73
15.	Enlace F.....	74
16.	Jerarquía STP.....	79
17.	Proceso de bloqueo por IMEI actual.....	94
18.	Formato Crontab	100
19.	Proceso final del reporte y posterior bloqueo por IMEI	104
20.	Arquitectura final	105

TABLAS

I.	Espectro frecuencia GSM	22
II.	Esquemas de codificación y modulación	29
III.	Clases de tráfico UMTS	44
IV.	Clases HSDPA	51
V.	Clases HSUPA	54
VI.	Costos de implementación del sistema.....	106

LISTA DE SÍMBOLOS

Símbolo	Significado
ACK	<i>Acknowledge</i>
ACKM	<i>Acknowledgement</i>
BER	Bit Error Rate
bps	Bit por segundo
f	Frecuencia
GT	<i>Global Tittle</i>
Hz	Hertz
kbps	Kilo bit por segundo
KHz	Kilo Hertz
Mbps	Mega bit por segundo
MHz	Mega Hertz
SMS	Multimedia Message Service
FDM	Multiplexación por división de frecuencia
TDM	Multiplexacion por división de tiempo
E1	Portadora E de nivel 1
E2	Portadora E de nivel 2
QoS	Quality of Service

GLOSARIO

2G	Segunda generación de telecomunicaciones móviles.
3G	Tercera generación de telecomunicaciones móviles.
3GPP	Third Generation Partnership Project, entidad encargada de la estandarización de protocolos de telecomunicaciones.
4G	Cuarta generación de telecomunicaciones móviles.
ANSI	American National Standards Institute.
ATM	Asynchronous Transfer Mode, modo utilizado por los protocolos de telecomunicaciones móviles.
BSC	Base Station Controller.
BSS	Base Station Subsystem.
BTS	Base Transceiver Station.
CDMA	Code Division Multiple Access, método de acceso múltiple que basa su funcionamiento en la división de código y espectro expandido.

EDGE	Enhanced Data rates for GSM Evolution, protocolo de segunda generación para la transferencia de datos.
EIR	Equipment Identity Register.
GPRS	General Packet Radio Service, protocolo de segunda generación para la transferencia de datos.
GGSN	Gateway GPRS Support Node.
GSM	Global System for Mobile Communications, protocolo de segunda generación para servicios de voz.
HLR	Home Location Register.
IMEI	International Mobile Equipment Identity, número de identificación que se asigna a un teléfono y modelo en específico para su identificación en la red.
IMSI	International Mobile Subscriber Identity.
MAP	Mobile Application Part.
MGW	Media Gateway.
MS	Mobile Station, denominación para un teléfono celular.

MSC	Mobile Switching Center.
MSISDN	Mobile Station Integrated Services Digital Network.
MTP	Message Transfer Part.
OSI	Open Systems Interconnection. Modelo de 7 capas utilizado para la transferencia de información por capas.
RAN	Radio Access Network.
RANAP	Radio Access Network Application Protocol.
SCP	Service Control Point.
SCCP	Signaling Connection Control Part.
SIM	Subscriber Identity Module.
SMS	Short Message Service.
SS7	Signaling System No. 7.
SSP	Service Switching Point.
STP	Signal Transfer Point.
SGSN	Serving GPRS Support Node.

RESUMEN

En el presente trabajo de graduación plantea una propuesta de un sistema SSH/FTP de interconexión entre empresas de telefonía en Guatemala, para el reporte automático y posterior bloqueo de IMEI reportados como robados.

En el primer capítulo se estudia a detalle los principales protocolos de segunda generación que se utilizan para los servicios voz, así como los protocolos de tercera generación involucrados en la transferencia de datos. Se presentarán también las arquitecturas base tanto para una red 2G como para una red 3G.

En el segundo capítulo se estudian las características, protocolos y arquitecturas en las cuales se puede soportar el protocolo SS7. Se estudiarán los puntos de señalización que son necesarios para la transmisión de información a lo largo de una red nacional.

En el tercer capítulo se detallan los conceptos de un servidor en Linux, así como la implementación de servicios para la transferencia de información y administración remota, FTP y SSH respectivamente. En este capítulo fundamenta el conocimiento necesario para la creación de Scripts en Shell y Perl.

En el cuarto capítulo se realizará la creación de los Shell Scripts y Perl Scripts necesarios para la verificación de nuevos números de IMEI reportados. En este capítulo se creará la rutina de ejecución automática de los scripts. Al

final de este capítulo se presentará el proceso final para el reporte y posterior bloqueo de los números de IMEI.

OBJETIVOS

General

Realizar una propuesta de un sistema SSH/FTP de interconexión entre empresas de telefonía en Guatemala, para el reporte automático y posterior bloqueo de IMEI reportados como robados.

Específicos

1. Presentar la arquitectura y principales protocolos de las redes de telecomunicaciones 2G para servicios de voz y 3G para servicios de datos.
2. Presentar las características y fundamentos del sistema SS7.
3. Presentar las características y fundamentos de un servidor SSH y un servidor FTP.
4. Formular la propuesta del sistema de reporte automático de IMEI reportados como robados.

INTRODUCCIÓN

A nivel mundial, la telefonía celular se ha convertido en un medio fundamental para el desarrollo humano. De la mano con la telefonía celular, se encuentra el teléfono celular. El uso del teléfono celular fue creciendo de manera exponencial, pero con este crecimiento, también se dio inicio a uno de los problemas más frecuentes del teléfono celular, que es la pérdida o robo del teléfono celular y en muchos casos, su uso inadecuado. En Guatemala, existe la posibilidad de bloquear un número de IMEI con su empresa de telefonía; sin embargo, si el teléfono robado es "liberado" para su uso con otras compañías, el teléfono puede ser utilizado sin ningún problema, esto debido a que el IMEI únicamente es reportado con una empresa y no con las 3 empresas de telefonía existentes en Guatemala.

Las redes de telecomunicaciones cuentan con varios equipos que se encargan de identificar a cada uno de los teléfonos móviles que realizar una conexión hacia una central. Estos equipos reconocen a la terminal móvil mediante una serie de identificadores, uno de ellos es el IMEI, el cual es un identificador internacional de equipos móviles. El IMEI identifica el modelo, serie y marca del teléfono móvil, por ejemplo, un Samsung Galaxy S6.

La señalización utilizada, en la mayor parte del proceso de bloqueo es del tipo SS7, adicional se utilizan señalizaciones especiales para la comunicación entre equipos especiales, esto mediante protocolos propietarios.

Por medio del protocolo SSH se puede obtener un acceso remoto y seguro hacia un servidor que almacena la información de los números de IMEI.

El protocolo FTP permite compartir archivos entre el servidor central y un usuario remoto. La diferencia fundamental entre los protocolos SSH y FTP deriva en que SSH es un acceso remoto seguro que permite la ejecución de tareas y administración remota de un servidor, mientras que FTP únicamente permite la transferencia de archivos.

1. REDES DE TELEFONÍA CELULAR PARA SERVICIOS DE VOZ Y DATOS

La primera generación de redes móviles, también llamada 1G, fue el punto de partida de toda la evolución de las telecomunicaciones. Antes de la 1G, existían medios de comunicación poco eficientes, los cuales dependían de hilos, cables, o eran medios escritos, gracias a esto, los científicos se dieron a la tarea de inventar un sistema de comunicaciones mucho más eficaz, que no dependiera de tantos factores, así fue cómo surgió la idea de las redes de telecomunicaciones móviles.

La primera red móvil comercial fue lanzada en Japón por NTT (Nippon *telegraph and telephone*) en 1979. Inicialmente fue lanzada únicamente para el área metropolitana de Tokio. Cinco años después, la red de NTT había sido ampliada con el objetivo de proporcionar cobertura a toda la población de Japón, con esto se convirtió en la primera red de 1G a nivel nacional.

En 1981, surgió la primera red 1G internacional, el sistema fue el NMT (Nordic Mobile Telephone). Este sistema operaba simultáneamente en Dinamarca, Finlandia, Noruega y Suecia. NMT fue la primera red de telefonía móvil en ofrecer *roaming* internacional.

En 1983, en Estados Unidos surgió la primera red 1G, la cual estaba basada en Chicago Ameritech y usaba para su operación un teléfono móvil Motorola DynaTAC.

La generación 1G, consistía en tecnologías completamente análogas. La característica fundamental de los sistemas 1G era su capacidad de ofrecer servicios de comunicación de voz, sobre la tecnología de conmutación de circuitos. Un dato muy curioso sobre la 1G es que además del servicio de voz, permitían la transmisión de datos empleando módems analógicos convencionales, aunque con velocidades bastantes limitadas que difícilmente superaban los 4 800 bps. La principal desventaja de los sistemas análogos 1G era que la señalización se realizaba por medio de un método de agrupación o envío por banda, por lo que, además de ser perceptible por el usuario, no permitía el uso de telefax y módems. Con la aparición de la red 1G el mercado de teléfonos móviles creció entre un 50 % anualmente, y el número de usuarios a nivel mundial alcanzó, aproximadamente, los 20 millones para 1990.

Hasta 1982, cada uno de los países que contaba con sistemas de telecomunicaciones móviles, desarrollaba su propio sistema para la transmisión y recepción, además, desarrollaban un teléfono móvil compatible únicamente con dicho sistema, esto limitaba grandemente la interacción entre usuarios de diferentes países. En 1982, en Europa se realizó una convención en la cual se conformó una asociación de países europeos. Esta asociación tenía como objetivo primordial desarrollar una tecnología celular que funcionara bajo un servicio común de telefonía móvil. La asociación realizó una serie de pruebas y homologaciones antes de elegir su banda de frecuencia estándar. Los modelos elegidos para la transmisión, fueron la banda estrecha y el modelo de Acceso Múltiple por División de Tiempo (Time División Múltiple Access, TDMA).

Posterior a la elección de la banda y la tecnología a utilizar, surgieron una serie de estándares, entre los cuales se tienen el NMT (Nordic Mobile Telephone), utilizado en los países Nórdicos, Holanda, Europa del Este y Rusia; C-450 utilizado en Alemania Oriental, Portugal y África, TACS (Total Access

Communications System) utilizado en el Reino Unido; Radiocom 2000 utilizado en Francia, TZ-801, TZ-802 y TZ-803 utilizados en Japón y AMPS el cual fue utilizado en los Estados Unidos.

El protocolo de Telefonía Móvil Nórdica (NMT, Nordisk Mobil Telefoni) fue desarrollado durante la década de 1970 y puesto en funcionamiento en 1981, para Suecia y Noruega. En 1982, se unieron Dinamarca y Finlandia, Islandia paso a formar parte en 1986. Desde entonces, la red NMT ha sido usada en Suiza, Noruega, Islandia, Holanda, Hungría, Eslovenia, Croacia, Bosnia, los países bálticos y Rusia. NMT basa su funcionamiento en una tecnología analógica, y según la frecuencia, existen dos variantes, el NMT-450 (el cual funciona bajo la frecuencia de 450 MHz) y el NMT-900 (el cual funciona bajo la frecuencia de 900 MHz). En 1986, se eligió entre estos dos estándares, siendo el ganador el NMT-900 ya que podía utilizar más canales, lo que significaba un aumento en el transporte de llamadas. Las especificaciones eran gratuitas y de código abierto, lo cual permitía a todas las compañías de telecomunicaciones producir equipos basados en NMT.

Dentro de las ventajas de NMT se pueden mencionar que es un sistema *full-duplex*, lo que le permite transmitir y recibir al mismo tiempo, contaba con discado automático, *handover* de celdas, permitía el servicio de *roaming* y contaba con especificaciones para la facturación del servicio. Adicional, contaba con dos métodos para la transmisión de datos, el primero método era llamado denominado DMS (Data and Messaging Service), el cual utilizaba el canal de señalización para transferir datos, las velocidades variaban entre 600 y 1200 bps, el segundo método de transferencia de datos, era denominado NMT Mobidigi, este permitía velocidades de transferencia de 380 bits por segundo y necesitaba equipo externo para su funcionamiento. La principal desventaja de este estándar estaba relacionada con los temas de seguridad, NMT no

realizaba el cifrado de las comunicaciones, esto quiere decir que, cualquier persona equipada de un *scanner* podía escuchar las conversaciones de los diferentes usuarios. Otra desventaja consistía en que, las señales de control transferidas entre la estación de base y la estación móvil utilizaban el mismo canal de audio que la comunicación establecida (la llamada en curso), esto provocaba que, periódicamente, aparecieran pequeñas ráfagas de ruido en la llamada.

El estándar Sistema de Comunicación de Acceso Total (TACS, Total Access Communications System), fue utilizado principalmente en Europa y forma la red de telefonía móvil europea más grande hasta inicios de la década de 1990, cuando fue reemplazado por el estándar GSM. TACS tuvo su apogeo en España, ya que fue el estándar utilizado por la compañía de telecomunicaciones Telefónica; aunque también fue utilizado en Japón bajo el nombre de JTAC. TACS no fue más, que la modificación europea, realizada por Motorola, del estándar AMPS utilizado en Estados Unidos, con la única variante que TACS operaba en la banda de frecuencia de 900 MHz. Posteriormente, se desarrolló el estándar ETAC, el cual únicamente presentaba una extensión del rango de frecuencias utilizado por TAC.

El AMPS (*Advance Mobil Phone System*) es un estándar análogo para la telefonía móvil, desarrollado por los Laboratorios Bell en la década de 1980. El 13 de octubre de 1983, fue introducido en Estados Unidos, posteriormente en 1986, fue introducido en Israel, en Australia en 1987, y en Pakistán en 1990. Fue el estándar análogo más utilizado en Estados Unidos en la década de 1980, hasta principios de la década de los 2000. En el 2000, Australia dejó de utilizar este estándar, en 2004, Pakistán también lo dio de baja y posteriormente en febrero de 2008, el estándar AMPS dejó de ser utilizado en Estados Unidos. AMPS utiliza diferentes frecuencias, denominadas canales, para cada una de

las llamadas o conversaciones establecidas. Por esta razón, si existe una cantidad considerable de usuarios, el sistema AMPS requiere un gran ancho de banda.

En términos generales, AMPS fue muy similar al estándar IMTS (Improved Mobile Telephone Service), con la diferencia que utiliza más potencia para realizar los cálculos y procesos necesarios para el seleccionamiento de las frecuencias, realizar *handoff* o realizar las configuraciones de la llamada. *handoff* consiste en que si el usuario cambia de celda mientras está hablando, AMPS logra mantener la comunicación activa siempre y cuando haya canales disponibles en la celda en la que se entra. *Handoff* basa su funcionamiento en el análisis de la potencia de la señal emitida por el teléfono móvil y la recibida en las distintas estaciones base. Depende del modo en el que se haga puede cortarse la comunicación unos 300 ms para reanudarse inmediatamente después o puede ser completamente inapreciable para el usuario.

El sistema AMPS se distingue de los antiguos sistemas de telecomunicaciones móviles, debido a su capacidad de establecer llamadas del tipo *back-end*. En AMPS, los conjuntos de celdas pueden asignar, de manera ordenada y flexible, canales a los teléfonos móviles, basados en la intensidad de la señal. Con esta función, los conjuntos de celdas tienen la posibilidad de que una misma frecuencia pueda ser reutilizada en varios lugares sin interferencias. Esto permitió que un mayor número de teléfonos pudieran ser utilizados en una misma área geográfica.

Debido a que AMPS es un estándar análogo era muy susceptible a la estática y el ruido, adicional presentaba severas fallas de seguridad ya que no incluía en sus configuraciones protección contra "espionaje" o sabotaje de llamadas. En la década de 1990, surgió una epidemia de "clonación" de

números telefónicos, la cual derivó en pérdidas millonarias para las empresas que prestaban el servicio de telefonía móvil. La vulnerabilidad consistía en que un intruso, con ayuda de equipo especializado, podía interceptar información del usuario tal como el Número de Serie Electrónico (Electronic Serial Number, ESN), el Número de Directorio Móvil (Mobile Directory Number, MDN) o el Número de Teléfono Celular (Cellular Telephone Number, CTN).

El número de serie electrónico, es una trama que consta de 12 dígitos enviado por el teléfono móvil a la red de telecomunicaciones, esto con fines de cobro y tarificación de las llamadas o servicios; una vez, la red de telecomunicaciones verifica el número de serie electrónico, procede a habilitar las llamadas o servicios. Si el intruso logra interceptar un número de serie electrónico y un número de directorio podría clonar la combinación en un teléfono móvil diferente, y entonces poder usarlo en otras áreas geográficas para realizar llamadas o utilizar servicios sin tener que pagar ni un solo centavo.

Para poder abusar de esta vulnerabilidad del sistema AMPS, los intrusos necesitaban tres elementos especiales:

- Un receptor de radio, por ejemplo, el PCR-1000, el cual podía ser sintonizado en canales inversos (la frecuencia o el canal por el cual los teléfonos móviles le envía datos a la antena celular).
- Una computadora que tuviera instalada una tarjeta de audio y un programa llamado Bampaia.
- Un teléfono móvil el cual sería utilizado con los datos clonados.

Si el intruso contaba con estos requisitos el proceso consistía en lo siguiente: cuando el radio receptor era sintonizado en la frecuencia adecuada, recibiría la señal transmitida por el teléfono móvil (el cual posteriormente sería

clonado). La información captada contenía los datos del ESN y MDN. Esta señal se conecta a la computadora mediante la tarjeta de sonido (siendo la señal que alimenta la entrada de la misma), posteriormente el programa Banpaia sería el encargado de decodificar el ESN y el MDN, contenidos en la señal, y lo desplegaba en el monitor. Después de obtener esta información, el intruso únicamente debía copiar esos datos en el teléfono móvil clon y reiniciarlo, después de lo cual la red de telefonía no podía distinguir el teléfono móvil clon era el teléfono original o no. Esto daba al intruso la capacidad de utilizar el servicio de telefonía móvil del abonado legítimo como si ese teléfono hubiera sido robado físicamente, con la única diferencia que el suscriptor no perdió físicamente su teléfono. En la mayoría de casos, el abonado legítimo no se daba cuenta de la clonación, sino hasta que su factura del servicio era emitida.

La vulnerabilidad en la seguridad llegó a ser tan grande, que algunas compañías de telefonía se vieron en la necesidad de solicitar un número de PIN antes de realizar una llamada. Con el tiempo, las compañías de telefonía móvil comenzaron a utilizar un sistema llamado RF Fingerprint, mediante este sistema de seguridad, la red podía determinar algunas sutiles diferencias en la señal de un teléfono legítimo y el clonado, y con esto podían restringir el servicio para los teléfonos clonados. El sistema logro reducir en un 90 % los casos de clonación, sin embargo, uno de los problemas más frecuentes consistía en que, si un usuario legítimo realizaba un cambio en el hardware de su teléfono móvil (batería, antena, entre otros), la red lo reconocía como un clon y le denegaba el servicio.

El estándar AMPS opera en la banda de frecuencia de 850 MHz. Para cada área, la Comisión Federal de Comunicaciones de Estados Unidos (Federal Communications Commission, FCC) permitió dos licencias, mejor conocidas

como redes. Estas licencias son conocidas como portadoras de tipo A y de tipo B. Cada compañía telefónica utiliza un bloque determinado de frecuencias, el cual consta de 21 canales de control y 395 canales de voz. Originalmente, las portadoras de tipo B fueron, generalmente, propiedad de la compañía telefónica local, y las portadoras de tipo A fueron asignadas a las compañías de telefonía inalámbrica.

En 1983, la FCC otorgó a cada una de las compañías de telefonía 333 pares de canales (666 canales en total) ya que, a fines de 1980, la base de usuarios activos, de la industria de telefonía móvil, había crecido hasta alcanzar cifras millonarias. En 1989, la FCC concedió más canales a cada empresa de telefonía móvil, se expandió la cantidad de canales hasta 416 pares (832 contando cada portadora). Estos canales adicionales, fueron utilizados bajo frecuencias que eran de la banda reservada para futuras expansiones. Estas frecuencias son adyacentes a la banda celular existente y antes de ser utilizadas para la telefonía móvil, eran utilizadas para la transmisión de canales de televisión UHF 70-83.

Dentro del estándar AMPS, cada canal dúplex se compone de 2 frecuencias, 416 de estos se encontraban en el rango de frecuencia de 824 a 849 MHz, y eran utilizados para las transmisiones de los teléfonos móviles hacia las estaciones base. Los otros 416 canales restantes se encontraban en el rango de frecuencia de 869 a 894 MHz, y eran utilizados para las transmisiones de las estaciones base hacia los teléfonos móviles. Cada sitio celular utilizaba un subconjunto de canales diferente a los canales que utilizan sus sitios vecinos, esto con la finalidad de evitar interferencias, aunque esto redujo significativamente el número de canales disponibles. Dentro del sistema AMPS, cada uno de los canales tenía un ancho de banda de 30 kHz, para hacer un total de 60 kHz para cada canal dúplex.

El estándar Radio y Teléfono Móvil Integrados (RTMI por sus siglas en italiano) fue el primer servicio de telecomunicaciones móviles implementado en Italia. Este sistema entró en funcionamiento 1973. RTMI operaba en la banda de frecuencia de 160 MHz y era utilizado básicamente para fines gubernamentales y algunas personas que ocupaban puestos dentro de los ministerios de finanzas y defensa. Durante la década de 1970, este sistema tuvo muy poca popularidad, hasta que, en 1980, surgió un estándar RTMI que operaba bajo la banda de frecuencia de 450 MHz, este sistema fue abierto al público en general y consiguió aumentar su cantidad de usuarios por encima de 150 000.

1.1. Red 2G para servicios de voz

En 1949, la compañía AT&T inicia con la comercialización del servicio telefónico móvil, denominado Servicio de Teléfono Móvil (*Mobile Telephone Service*, MTS). AT&T prestó su servicio telefónico móvil a cien ciudades y corredores viales, aunque su total de usuarios era de apenas 5 000 clientes los cuales realizaban alrededor de 30 000 llamadas cada semana. Las llamadas eran configuradas de forma manual por un operador, por lo cual el usuario únicamente tenía que presionar un botón en el auricular para hablar y soltarlo para para iniciar la conversación. El crecimiento de suscriptores y la generación de ingresos se vieron obstaculizados por las limitaciones de la tecnología, debido a únicamente existían 3 canales de radio disponibles, esto significaba que solo tres usuarios en cualquier ciudad podían hacer llamadas desde su teléfono móvil al mismo tiempo. Por esta razón el servicio MTS tuvo que evolucionar al servicio IMTS (Improved Mobile Telephone Service).

El servicio IMTS utiliza canales adicionales, con lo cual se permite que más llamadas de voz puedan ser realizadas de manera simultánea en un área

geográfica determinada. Además, se incorporó la función de marcación cliente, eliminando así el establecimiento manual de las llamadas. Durante la primera generación de redes móviles, únicamente se pudo lograr una mejora de los servicios de voz, ya que todos los estándares contaban con la limitante de ser análogos. Esta generación abrió camino para su sucesora, la cual dio una revolución al establecer sistemas digitales.

Durante la década de 1980, los servicios de telefonía móvil eran suficientes para la cantidad de usuarios existentes, pero conforme la popularidad de este servicio fue creciendo, los desarrolladores de tecnologías se vieron en la necesidad de realizar cambios a sus estructuras, sistemas y estándares, esto con la finalidad de dar abasto al creciente número de nuevos usuarios; pero, con el creciente número suscriptores, también crecía la demanda por más, mejores y nuevos servicios, de esa necesidad se dio un cambio al rumbo de las tecnologías, este cambio de rumbo fue dirigido hacia las tecnologías digitales. En 1991, con el lanzamiento del estándar GSM en Finlandia, se inicia oficialmente la segunda generación de redes móviles.

Los estándares 2G ofrecían tres características fundamentales que sus antecesores no ofrecían, estas son la codificación digital de todas las conversaciones de voz, los estándares 2G ofrecen un uso más eficiente del espectro electromagnético y dio inicio con la transferencia de datos móviles. Uno de los beneficios más interesantes que se logra con la utilización de estándares digitales es el mejor comportamiento en ambientes de elevada interferencia, que les proporciona una capacidad superior a los estándares analógicos. Adicionalmente, la tecnología digital tenía la ventaja de estar situada en una senda de avances constantes en aspectos como la miniaturización e integración de dispositivos a un costo cada vez menor.

Las tecnologías 2G ofrecían servicios tales como mensajes de texto, mensajes multimedia y mensajes de voz. Todos los mensajes de texto y multimedia enviados están codificados digitalmente, lo que garantiza que únicamente el receptor podrá revisar el contenido de dicho mensaje.

Los estándares 2G se caracterizan por el multiplexado temporal que realizan sobre la portadora utilizada para la transferencia de información. No realizan una transmisión o recepción continua y pueden dedicar ciertos intervalos de tiempo a sintonizar las frecuencias guía de celdas vecinas. Esto permite el mecanismo de toma de medidas, esto supone una importante descarga computacional para la red. Sin embargo, la decisión de un traspaso de llamada de una celda a otra sigue siendo de la red, por ello esta técnica de traspaso se denomina MAHO (Mobile Assisted Hand Over).

Uno de los servicios que más llamo la atención fue la transferencia de datos, esto dio un plus adicional al estándar GSM, aunque con el paso del tiempo surgió la necesidad de mejores tasas de transmisión y recepción de datos; esto abrió las puertas a las generaciones 2,5G y 2,75G.

1.1.1. Principales estándares

Entre los estándares más importantes de la 2G, se encuentran el GSM, IS-95, PDC, iDEN y D-AMPS. Adicionalmente existieron servicios 2G como el GPRS y EDGE, los cuales eran una mejora de los estándares antiguos, con la diferencia de una mejor tasa de transferencia.

El protocolo IS-95, también conocido como CDMA One, fue desarrollado por la compañía Qualcomm; basa su funcionamiento en la tecnología CDMA. IS-95 fue publicado bajo las Normas TIA/EIA/IS-95. En sus inicios este estándar

compitió fuertemente con la versión digital de AMPS, en la actualidad este estándar fue sustituido por el IS-2000.

IS-95 consiste en un conjunto de 5 protocolos, el primero es el P_REV = 1. Este fue basado en los estándares ANSI; solo se definió para la banda de frecuencia de 1 900 MHz. El segundo protocolo es el P_REV = 2, a este protocolo también se le denomina Interim Standard 95A (IS-95A), fue desarrollado para Banda Clase 0 únicamente. El tercer protocolo es el P_REV = 3, también conocido como TSB-74. El cuarto protocolo es el P_REV = 4 también conocido como IS-95B Fase I, este estándar proporciona las Normas IS-95B que establecen los parámetros necesarios para realizar la fusión de estándares TIA y ANSI, adicional fue el primer estándar que especificaba la interoperabilidad de teléfonos móviles en dos bandas de frecuencias. El estándar P_REV = 4 fue la variante del IS-95 más popular. El quinto estándar fue el P_REV = 5 al que también se le denomina IS-95B Fase II, este estándar no fue tan popular como su antecesor y únicamente fue utilizado en una pequeña parte de Corea del Sur.

Las Normas IS-95 describen una interfaz de aire como un conjunto de protocolos utilizados para la comunicación entre los teléfonos móviles y la red de telefonía. *IS-95* fue descrito como un protocolo de tres capas, donde la capa uno (L1, Layer 1) corresponde a la capa física, la capa 2 (L2, Layer 2) se refiere a las subcapas de Control de Acceso al Media (Media Access Control) y Control de Acceso al Enlace, MAC (Link Access Control, LAC), y la capa 3 (L3, Layer 3) hace referencia a la llamada en curso.

IS-95 define la transmisión de información en ambos sentidos, tanto de bajada (la red de telefonía enviando información al teléfono móvil) como de subida (el teléfono móvil enviando información a la red de telefonía). Para la

transmisión de información de bajada, las señales de radio se transmiten por medio de la BTS. Cada BTS esta sincronizada con un receptor GPS por lo que las transmisiones están siendo controladas todo el tiempo. En bajada, todas las transmisiones se modulan con QPSK con una velocidad de 1 228 800 bps.

Cada señal es transmitida con un código de Walsh de longitud 64 caracteres. Si la información es transmitida en sentido de subida, las señales son transmitidas por el teléfono móvil. La información es modulada con OQPSK, esto con la finalidad de operar en el rango óptimo del amplificador de potencia del teléfono móvil. La información es transmitida con una velocidad de 1 228 800 bps y las señales se ensanchan con códigos de Walsh. Cada BTS dedica una cantidad de su potencia de salida a un canal piloto, el cual consiste en una trama PN no modulada. Cada sector de una BTS tiene asignado un código de desplazamiento de 64 caracteres. No hay datos consignados en el piloto hacia adelante.

Con su fuerte función de auto correlación, el piloto hacia adelante permite móviles para determinar la temporización del sistema y distinguir diferentes de BTS de traspaso. Con la ayuda de la función de auto correlación, el canal piloto permite a los teléfonos móviles determinar la hora del sistema y distinguir las diferentes BTS de la red de telefonía. Cuando el teléfono móvil se encuentra "buscando" señal, quiere decir que está tratando de encontrar las señales del canal piloto de la red mediante la sintonización de frecuencias particulares y la realización de una correlación cruzada de todas las posibles faces del código PN.

Generalmente, los datos transmitidos son divididos en tramas de bits, cada trama de bits es pasada por un codificador convolucional, el cual añade los bits de redundancia para la detección y corrección de errores. Adicional, se

transmite un canal de sincronización, el cual transmite continuamente un único mensaje, el mensaje del canal de sincronización, este mensaje transmite 32 bits por cada trama con una codificación de 128 símbolos.

Una BTS puede transmitir de uno a siete canales de búsqueda, cada canal contiene los mensajes de señalización transmitidos desde la red de telefonía para todos los teléfonos móviles inactivos. El canal de búsqueda también transmite los mensajes de mayor prioridad dedicados a la inicialización de las llamadas hacia y desde los teléfonos móviles. Cuando un teléfono móvil está inactivo, siempre se encuentra recibiendo información del canal de búsqueda.

El espacio de Walsh que no es utilizado para transmitir los canales utilizados por la BTS, está disponible para los canales de tráfico. Estos canales transmiten las llamadas de voz y de datos individuales. Al igual que los canales de búsqueda, los canales de tráfico tienen un tiempo de trama de 20 ms. Dado que los datos de voz son intermitentes, los canales de tráfico soportan la función de operación a velocidad variable, es decir que cada trama de 20 ms se puede transmitir a una velocidad diferente, según lo determinado por el servicio en uso (voz o datos). El teléfono móvil que recibe una trama de velocidad variable, no conoce la velocidad a la que fue transmitida la trama. Típicamente, la trama se decodifica a la máxima velocidad posible y utilizando las métricas de calidad del decodificador Viterbi, se escoge el resultado correcto.

Una de las ventajas de utilizar un protocolo de velocidad variable es que por naturaleza proporciona a las tramas una potencia de transmisión bajas, lo que se traduce en una mejora en cuanto a la interferencia causada a otras señales. El control activo de potencia, se utiliza en los canales de tráfico que transmiten una llamada cuando el teléfono móvil envía mensajes de señalización a la red indicando una baja calidad de la señal, entonces la red

modifica la potencia, para mantener la calidad de la señal lo suficiente buena. Una vez que se establece una llamada de voz, el teléfono móvil se limita a utilizar únicamente el canal de tráfico.

El estándar IS-95, permite que los canales de tráfico también puedan realizar llamadas de datos usando la conmutación de circuitos. Las tramas de velocidad variable se generan utilizando el Protocolo de Enlace Radio IS-95 (Radio Link Protocol, RLP). RLP proporciona un mecanismo para mejorar el rendimiento del enlace inalámbrico (para la transmisión de datos). IS-95, como cualquier otro protocolo de comunicación, tienen un rendimiento limitado de acuerdo con el teorema de Shannon, de acuerdo con la capacidad de mejorar el SNR y ancho de banda. IS-95 tiene un ancho de banda fijo.

El estándar PDC (Personal Digital Cellular) es un estándar 2G utilizado en Japón. PDC basa su funcionamiento en la tecnología TDMA. El estándar PDC ofrece un uso mucho eficiente comparado con otros estándares TDMA, esto debido a que divide cada canal en varias ranuras de tiempo y por lo tanto permite que varios usuarios puedan utilizar un mismo canal. Cada canal puede soportar un máximo de 3 usuarios bajo condiciones normales. Adicionalmente, puede proporcionar 6 canales de tipo *half rate* o 3 canales de tipo *full rate*.

Para la codificación de voz, PDC utiliza un codificador distinto que el de IS54/IS136. La tasa de transferencia de este estándar es de 9,6 kbps en modo *full rate*, y de 5,6 kbps en modo *half rate*. Utilizando sus capacidades de Red Inteligente, PDC también soporta llamadas de tipo prepago, Números de Acceso Universal y Redes Privadas Virtuales inalámbricas, VPN.

PDC ha sido diseñado para reducir el problema ocasionado por la congestión en lugares como centros comerciales y oficina. Una red de

estaciones base del tipo micro y nano puede ser desplegada en interiores, con sistemas de antenas distribuidos y repetidores. Para la transmisión de datos se introdujo el estándar PDC-P, el cual utiliza un sistema basado en la transmisión de paquetes permitiendo a varios usuarios utilizar un mismo canal de manera simultánea. La transmisión de datos por conmutación de paquetes, permite que el usuario está conectado permanentemente y únicamente paga por la cantidad de datos transferidos.

El estándar iDEN (Integrated Digital Enhanced Network), fue desarrollado por Motorola, ofrece a sus usuarios los beneficios de acceso de radio troncal. iDEN utiliza la técnica de acceso TDMA., en comparación con los sistemas celulares de radio y de dos vías analógicas, mediante el uso de compresión de voz y Time Division Multiple Access (TDMA). iDEN fue diseñado para operar en frecuencias individuales, las cuales pueden, o no, ser contiguas. iDEN opera en canales de 25 KHz, pero solo ocupa 20 kHz con el fin de proporcionar protección contra la interferencia, esto mediante las bandas de guarda; puede soportar 3 o 6 usuarios por cada canal. Los intervalos de tiempo de transmisión y recepción asignados a cada usuario se compensan con el tiempo que un usuario no necesita transmitir y recibir al mismo tiempo. En la figura 1 se observa la estructura de un canal utilizando TMDA.

Figura 1. Estructura canal TDMA



Fuente: *Comunicaciones móviles*. <http://www.ComUMoviles.com/TDAM+Canal+voz%3>.

Consulta: julio de 2016.

Dentro de las características más importantes de TDMA se encuentran:

- Debido a que las transmisiones no son continuas, la función *handoff* se vuelve más sencilla.
- Un solo canal de frecuencia puede ser utilizado por varios usuarios de manera simultánea.
- Los intervalos de tiempo son asignados de forma dinámica.
- Menor interferencia a señales ajenas.
- Controles de potencia flexibles.

1.1.2. Estándar GSM

El Sistema Global las Comunicaciones Móviles (Global System for Mobile Communications, GSM) es un estándar de segunda generación que fue desarrollado por el Instituto Europeo de Normas de Telecomunicaciones (European Telecommunications Standards Institute, ETSI).

En 1982, se da inicio con la creación de GSM, cuando fue creado el grupo GSM cuya tarea era crear un estándar de telefonía móvil para ser utilizado en toda Europa. En 1990 finalizó el desarrollo del primer estándar llamado GSM-900, luego en 1991 se finalizó el segundo estándar llamado DCS-180. Este año también fueron presentados los primeros prototipos de teléfonos móviles con soporte para GSM. Un año más tarde, en 1992, el estándar GSM-900 entró en funcionamiento y conjuntamente se presentó el primer teléfono móvil que soporta este estándar, siendo este el Nokia 1011. GSM tuvo tanto éxito en Europa, que rápidamente fue introducido para América en los años posteriores.

El estándar GSM se compone de 4 sistemas, siendo estos el GSM-900, GSM-1800, GSM-1900 y EGSM, adicionalmente existe un quinto y sexto sistemas, el GSM-80 utilizado en algunos países de América y el GSM-450 utilizado en algunos países europeos, especialmente de la región nórdica y este de Europa. GSM utiliza las tecnologías de Acceso Múltiple por División de Frecuencia (Frequency Division Multiple Access, FDMA) y Acceso Múltiple por división de Tiempo (Time Division Multiple Access, TDMA), por esta razón GSM utilizan dos bandas de frecuencias de manera simultánea, la primera banda de frecuencia se utiliza para la transferencia de información desde el teléfono móvil hacia la estación base y la otra para la transferencia de información desde la estación base hacia el teléfono móvil.

En cuanto a canales de transferencia se refiere, con el método TDMA, se proporcionan ocho canales dentro de una portadora única con una codificación de voz de 13 Kbps, de esta manera se consigue un ancho de banda efectivo de 25 KHz. Actualmente, se agregó una nueva tecnología denominada Adaptación Multi-Tasa (Adaptive Multi-Rate, AMR), este método permite duplicar la cantidad toda de llamadas activas dentro de un canal de voz.

GSM-900 es el sistema original, está diseñado para trabajar en la banda de frecuencia de 900 MHz. Utiliza las frecuencias 890-915 MHz para el envío de información desde el teléfono móvil hacia la estación base y las frecuencias 935- 960 MHz para la transferencia de información desde la estación base hacia el teléfono móvil. Contiene 124 canales, que van del canal 1 al 124, los canales están espaciados 200 kHz uno del otro. Se utiliza el tipo de espaciado dúplex de 45 MHz. Las bandas de guarda de 100 kHz de ancho están situadas en cada extremo del rango de frecuencias.

GSM-1800 es el sistema más utilizado en Europa (conjuntamente con GSM-900) utiliza las frecuencias 1710-1785 MHz para enviar información desde el teléfono móvil hacia la estación base y las frecuencias 1805-1880 MHz él envió de información desde la estación base hacia el teléfono móvil. Contiene un total de 374 canales que van desde el 512 hasta el 885. Utiliza un tipo de espaciado dúplex de 95 MHz. En el Reino Unido, GSM-1800 también recibe el nombre de Servicio Digital de Celulares (Digital Cellular Service, DCS), mientras que en Hong Kong se llama PCS.3

GSM-1900 es utilizado, en su mayoría, para países americanos, siendo estos Argentina, Bolivia, Brasil, Canadá, Chile, Colombia, Ecuador, Estados Unidos, Panamá, Perú, Venezuela, México, Paraguay, El Salvador y Guatemala. Utiliza las frecuencias 1 850-1 910 MHz para el envío de

información desde el teléfono móvil hacia la estación base, y las frecuencias 1 930-1 990 MHz para el envío de información desde la estación base hacia el teléfono móvil. Contiene un total de 298 canales que van numerados del 512 al 810. Al estándar GSM-1900 también se le conoce como Servicio Personal de Comunicaciones (Personal Communications Service, PCS).

El sistema GSM Extendido (EGSM, Extended GSM), es una ampliación del sistema GSM-900, ya que en algunos países de Europa era necesaria la ampliación de las bandas de frecuencia utilizadas. Utiliza las frecuencias 880-915 MHz para el envío de información desde el teléfono móvil hacia la estación base y las frecuencias 925-960 para el envío de información desde la estación base hacia el teléfono móvil. EGSM cuenta con 50 canales más que GSM-900, que van desde el 975 hasta el 1 023, adicionalmente también se incluye el canal 0. Cuando EGSM entró en funcionamiento, se dio el inconveniente que los teléfonos no lo soportaban, por lo que fue necesario un cambio de la mayoría de teléfonos móviles pertenecientes a usuarios de este estándar. EGSM, está diseñado para cubrir un área menor, por lo cual ya no requiere cantidades elevadas de potencia para la transmisión.

GSM-850 fue implementado para su uso en América Latina, funciona bajo la banda de 850 MHz, incluido Guatemala. GSM-850 utiliza las frecuencias 824-849 MHz para el envío de información desde el teléfono móvil hacia la estación base y las frecuencias 869-894 para el envío de información desde la estación base hacia el teléfono móvil. Contiene un total de 123 canales que van desde el 128 hasta el 251. A este sistema también se le conoce como GSM-800, ya que anteriormente este rango de frecuencias fue asignado al estándar AMPS.

GSM-450 es el sistema menos utilizado. Fue implementado para su uso en los países nórdicos, Rusia, Benelux y el este de Europa. Este sistema, fue

implementado en la misma banda de frecuencia que el sistema NMT. Puede utilizar las frecuencias 450,4-457,6 MHz y 478,8-486 MHz para el envío de información desde el teléfono móvil hacia la estación base y las frecuencias 460,4-467,6 MHz y 488,8-496 MHz para el envío de información desde la estación base hacia el teléfono móvil. Las frecuencias están agrupadas en 2 grupos, el primer grupo contiene las frecuencias 450,4-457,6 MHz y 460,4-467,6 MHz, mientras que el segundo grupo contiene las frecuencias 478,8-486 MHz y 488,8-496 MHz. Para el primer grupo contiene un total de 34 canales que van del 259 al 293. Para el segundo grupo también contiene 34 canales que van del 306 al 340. En la tabla I se observa la banda de frecuencia asignada para cada estándar GSM.

El estándar GSM, permitió la inclusión de nuevos servicios y el mejoramiento de los existentes. Los servicios de voz que ofrece son el identificador de llamada entrante, buzón de voz, Transferencia de llamadas entrantes a un teléfono móvil o fijo, restricción de llamadas entrantes y salientes, llamada en espera y el servicio *push to talk*. Los servicios multimedia son mensajes de texto corto, mensajes multimedia, video llamada, mensajería instantánea IM, navegación en internet, correo electrónico, juegos *online*, reproductores digitales, entre otros. De todos los servicios multimedia los que mayor impacto tuvieron sobre los usuarios fueron el mensaje de texto corto y el servicio de navegación en internet, por esa razón en la actualidad aún son servicios vigentes y de bastante demanda.

Tabla I. **Espectro frecuencia GSM**

Sistema	Banda	Uplink (MHz)	Downlink (MHz)
T-GSM-380	380	380.2–389.8	390.2–399.8
T-GSM-410	410	410.2–419.8	420.2–429.8
GSM-450	450	450.4–457.6	460.4–467.6
GSM-480	480	478.8–486.0	488.8–496.0
GSM-710	710	698.0–716.0	728.0–746.0
GSM-750	750	747.0–762.0	777.0–792.0
T-GSM-810	810	806.0–821.0	851.0–866.0
GSM-850	850	824.0–849.0	869.0–894.0
P-GSM-900	900	890.2–914.8	935.2–959.8
E-GSM-900	900	880.0–914.8	925.0–959.8
R-GSM-900	900	876.0–914.8	921.0–959.8
T-GSM-900	900	870.4–876.0	915.4–921.0
DCS-1800	1800	1710.2–1784.8	1805.2–1879.8
PCS-1900	1900	1850.0–1910.0	1930.0–1990.0

Fuente: *Eve U.* <http://eve-ingsistemas-u.blogspot.com/2012/04/el-sistema-global-para.html>.

Consulta: julio de 2016.

1.1.3. Estándar GPRS y EDGE

Debido a la creciente demanda por una mayor velocidad para la transferencia de datos, se originó una sub-generación de redes móviles denominada 2,5G. Esta generación tuvo como estándar principal al estándar GPRS (General Packet Radio Service), el cual es una extensión del estándar GSM para la transmisión de datos mediante la conmutación por paquetes. Una de las novedades de GPRS consiste en que la cantidad de tráfico cursado está ligada con el volumen de datos transferidos, mientras que protocolos anteriores

ligaban la cantidad de tráfico con el tiempo de uso de la conexión, esto se transforma en una reducción de costo del servicio para el usuario ya que la tarificación se realiza con base en la cantidad de megabytes descargados y la velocidad utilizada.

El rendimiento del estándar GPRS es variable, ya que depende de gran manera del de usuarios que utilizan el servicio al mismo tiempo. GPRS proporciona velocidades de transferencia de datos de 56 a 114 Kbps. Los servicios que ofrece GPRS son mensajería SMS, mensajería de difusión, mensajería multimedia, servicio *push to talk*, mensajería instantánea, servicio de navegación en internet mediante el Protocolo de Aplicaciones Inalámbricas (Wireless Application Protocol, WAP), servicio Punto a Punto (*Point to Point*, P2P) y el servicio Punto a Multipunto (*Point to Multi-Point*, P2M). En referencia al servicio de mensajería SMS, el servicio fue introducido en GSM, pero con una velocidad de 10 mensajes por minuto, mientras que en GPRS se aumentó la velocidad máxima a 30 mensajes por minuto.

GPRS soporta una gran cantidad de protocolos, entre los cuales se encuentran el Protocolo de Internet (Internet Protocol, IP) el cual es el protocolo de comunicaciones más importante y basa su funcionamiento en el direccionamiento y establecimiento de rutas; Protocolo Punto-Punto (Point-to-Point Protocol, PPP), este protocolo, a pesar de ser estándar, muchas veces no es soportado por la red de telefonía local. PPP sirve para utilizar el teléfono móvil como un modem de internet mediante el establecimiento de un túnel IP; protocolo X,25, el cual es utilizado generalmente por equipos de cobro inalámbricos.

Las velocidades de carga y descarga que se pueden lograr en GPRS dependen del número de intervalos de tiempo TDMA asignado por el operador,

la codificación de canal utilizada, la capacidad máxima del teléfono móvil, esto depende de la clase del teléfono. Los teléfonos que soportan GPRS están divididos en clase A, clase B y clase C.

Los teléfonos móviles de clase A, pueden utilizar el servicio GPRS y el servicio de voz, de manera simultánea. En la actualidad aún existen estos dispositivos.

Los teléfonos móviles de clase B, pueden utilizar el servicio GPRS y el servicio voz, pero no de manera simultánea. Si el usuario utiliza el servicio de voz, el servicio GPRS está suspendido y luego, cuando la llamada de voz finaliza, se reanuda automáticamente. La mayoría de los teléfonos móviles GPRS son de clase B.

Los teléfonos móviles de clase C, pueden utilizar el servicio GPRS o de llamadas de voz, pero no de manera simultánea. Adicionalmente en esta clase de dispositivos, el usuario debe realizar un cambio manual entre cualquiera de los servicios.

La conexión GPRS se establece mediante un conjunto de parámetros configurados en el Nombre del Punto de Acceso (Access Point Name, APN). Un APN define las configuraciones de los servicios como WAP, SMS, MMS y para los servicios de comunicación mediante internet como el correo electrónico y acceso a internet. Con el fin de configurar una conexión GPRS para un módem inalámbrico, el usuario debe especificar un APN, opcionalmente, un nombre de usuario y contraseña, y muy rara vez una dirección IP, todos estos datos son proporcionados por el operador de red local.

Un teléfono móvil de clase A tiene la característica de que, si la red de telefonía lo solicita, puede transmitir en dos frecuencias diferentes al mismo tiempo, por lo tanto, tendrá dos frecuencias de radio, pero esta característica representa costos de operación elevados, por esta razón si el teléfono móvil se ve obligado a transmitir en dos frecuencias diferentes puede utilizar la función Modo de Transferencia Dual (Dual Transfer Mode, DTM). DTM permite la utilización simultánea de los servicios de datos y de voz.

Los métodos de acceso utilizados en GPRS se basan en FDD y TDMA. Durante una sesión, un usuario tiene asignado un canal para el tráfico de subida y un canal para el tráfico de bajada. Esto combinado con la multiplexación en el dominio del tiempo, hace posible que varios usuarios compartan el mismo canal de frecuencia. Los paquetes de datos tienen una longitud constante, que corresponde a un intervalo de tiempo. El enlace de bajada utiliza el esquema de primero en entrar es el primero en salir.

El proceso de codificación del canal GPRS consta de dos pasos. Primero, mediante un código cíclico se agregan bits de paridad a la trama (esta función es realizada por el bloque de verificación); posterior a esto, se realiza la codificación del mensaje mediante un código convolucional. GPRS utiliza los esquemas de codificación CS-1, CS-2, CS-3 y CS-4. Estos esquemas especifican el número de bits de paridad generados por el código cíclico y la tasa de punción del código convolucional. En los esquemas de codificación CS-1, CS-2 y CS-3 la tasa del código convolucional es de $1/2$, esto quiere decir que cada bit de entrada se convierte en dos bits codificados. En los esquemas de codificación CS-2 y CS-3, la salida del código convolucional es modificada hasta lograr la tasa de código deseada. En el esquema CS-4 no se aplica ninguna codificación convolucional.

CS-4 es el esquema de codificación menos robusto, por esta razón se utiliza cuando el teléfono móvil se encuentra cerca de la BTS, mientras que CS-1 que es el esquema más robusto es usado cuando el teléfono móvil se encuentra lejos de la BTS. Utilizando CS-4 es posible lograr una velocidad de transmisión de 20 Kbps por cada intervalo de tiempo. Ahora bien, usando este esquema la cobertura de cada celda es únicamente el 25 % de lo normal. CS-1 permite lograr una velocidad de transmisión de 0,8 Kbps, pero la cobertura de cada celda es el 98 % de la cobertura normal.

Los intervalos de tiempo múltiples determinan la velocidad de transferencia de datos disponible para los enlaces de subida y bajada. Puede tomar un valor de 1 a 45, el cual sirve para asignar los canales a los enlaces. En un intervalo múltiple, la asignación del canal se representa por la suma de dos dígitos (por ejemplo, 5 + 2). El primer dígito representa al número de intervalos de tiempo para el enlace de bajada y el segundo dígito representa el número de intervalos de tiempo para el enlace de subida. Generalmente, para los teléfonos móviles de clase 10 se utilizan 4 intervalos de tiempo para el enlace de bajada y 2 para el enlace de bajada.

Con la utilización del esquema de intervalos de tiempo múltiples se identifica información del enlace tal como el número máximo de intervalos de tiempo que pueden ser asignados al enlace de subida, el número máximo de intervalos de tiempo que pueden ser asignados al enlace de bajada, el número total de intervalos de tiempo que pueden ser asignados a un solo teléfono móvil, el tiempo necesario para que el teléfono móvil esté disponible para transmitir información y el tiempo necesario para que el teléfono móvil esté disponible para recibir información.

La demanda por una mejor velocidad de transferencia de datos fue creciendo, hasta que la velocidad máxima de GPRS fue insuficiente, por esta razón, en 2003, fue necesario hacer una mejora de GPRS, esta mejora recibe el nombre de Tasa de Datos Mejorada para la Evolución de GSM (EDGE, Enhanced Data Rates for GSM Evolution), este protocolo también fue conocido como EGPRS (Enhanced GPRS). EDGE, debido a sus velocidades máximas para la transferencia de datos, es considerado como un protocolo pre-3G.

Debido a que el estándar EDGE fue implementado como una mejora de GPRS, para los operadores de telefonía fue fácil la adaptación a este nuevo estándar. EDGE puede funcionar en cualquier red de telefonía con soporte para GPRS, ya que, a excepción de la BTS, no requiere cambios de hardware o software. En cuanto a la BTS, se deben instalar nuevos transceptores e instalar nuevo software para los nuevos esquemas de modulación y codificación.

Para la modulación de la información transmitida, el estándar EDGE utiliza la Modulación por Desplazamiento mínimo Gaussiano (Gaussian Minimum-Shift Keying, GMSK), en otros casos, también puede utilizar la EDGE utiliza la Modulación por Desplazamiento de Fase PSK8 (8 Phase Shift Keying, 8PSK) para la parte superior de sus esquemas de modulación y codificación. EDGE produce una palabra de 3 bits por cada cambio de fase de la portadora, esto triplica la velocidad de transferencia de datos que ofrece GSM. EDGE utiliza un algoritmo de adaptación de velocidad de transferencia de datos, el cual se adapta al esquema de modulación y codificación, de acuerdo con la calidad del canal.

EDGE introduce una nueva tecnología denominada Redundancia Incremental (IM, Incremental Redundancy), la cual, en lugar de retransmitir

paquetes alterados, envía más información de redundancia para combinarse en el receptor. Esto aumenta la probabilidad de una correcta decodificación.

EDGE puede lograr una velocidad de transferencia de información de 500 Kbps (con una latencia extremo-extremo de menos de 150 ms) para 4 intervalos de tiempo en el modo de conmutación de paquetes. Esto significa que puede manejar cuatro veces más tráfico que el estándar GPRS. EDGE satisface los requerimientos de la Unión Internacional de Telecomunicaciones para una red 3G, y ha sido aceptado por la UIT como parte de la familia IMT-2000 de estándares 3G. En la actualidad con el estándar EDGE se puede alcanzar una velocidad de transferencia para la experiencia del usuario de hasta 384 Kbps.

El proceso de codificación consta de dos pasos. Primero, se agregan bits de paridad mediante un código cíclico. Segundo, se realiza la codificación de la información mediante un código convolucional. En GPRS, los Esquemas de codificación de CS-1 a CS-4 especifican el número de bits de paridad generados por el código cíclico y la tasa de punción del código convolucional. A diferencia de GPRS, en EDGE se utilizan los siguientes esquemas de codificación y modulación:

- MCS-1
- MCS-2
- MCS-3
- MCS-4
- MCS-5
- MCS-6
- MCS-7
- MCS-8
- MCS-9

Los esquemas MCS-1, MCS-2, MCS-3 y MCS-4 utilizan la modulación GMSK y tienen un rendimiento similar a los estándares CS-1, CS-2, CS-3 y CS-4 en GPRS. Los esquemas MCS-5, MCS-6, MCS-7, MCS-8 y MCS-9 utilizan 8PSK. Todos los esquemas de codificación y modulación, en EDGE, utilizan un código convolucional de tasa 1/3. Otra diferencia con el estándar GPRS, consiste en que en EDGE todos los encabezados son codificados más robustamente. En la tabla II se muestran las especificaciones de cada uno de los esquemas de codificación y modulación.

Existe una versión mejorada denominada EDGE Mejorado (Evolved Enhanced Data Rates for GSM Evolution, E-EDGE). Con E-EDGE se consigue reducir al mínimo la latencia por intervalo de tiempo (en el rango de 20 ms a 10 ms). La velocidad de transferencia de información se incrementa hasta 1 Mbps pico, adicionalmente se cambia la modulación de orden superior por la Modulación de Amplitud en Cuadratura (Quadrature Amplitude Modulation, QAM) y se escogen los tipos 32QAM y 16QMA. Finalmente, la calidad de la señal se mejora con el uso de antenas duales, las cuales mejoran la tasa promedio de bits y la eficiencia del espectro.

Tabla II. **Esquemas de codificación y modulación**

Esquema de codificación y modulación	Velocidad de transferencia por intervalo de tiempo <Kbps/intervalo>	Tipo de Modulación	Tasa del Código para datos	Tasa del Código para encabezados
MCS-1	9,20	GMSK	0,53	0,53
MCS-2	11,60	GMSK	0,66	0,53
MCS-3	15,20	GMSK	0,85	0,53
MCS-4	18,00	GMSK	1,00	0,53
MCS-5	22,80	8PSK	0,36	0,33
MCS-6	30,00	8PSK	0,49	0,33
MCS-7	45,20	8PSK	0,76	0,39
MCS-8	54,80	8PSK	0,92	0,39
MCS-9	59,60	8PSK	1,00	0,39

Fuente: elaboración propia.

1.1.4. Arquitectura de red 2G

Como se estudió anteriormente, el estándar 2G más utilizado actualmente es el GSM, por esta razón se analizará la arquitectura de una red 2G GSM. La arquitectura GSM se puede dividir en tres bloques principales, estos son la estación base, conmutación de red y administración de red. Cada uno de estos bloques contiene subsistemas. La estación móvil se refiere al equipo que transmite y recibe las señales de información, en términos generales, se refiere al teléfono móvil del usuario y la tarjeta SIM.

El Modulo de Identificación del suscriptor (Subscriber Identity Module, SIM) es una tarjeta que permite a la red identificar al usuario por medio de información como identificación, autenticación y servicios prestados. Al principio únicamente existía SIM permanente, la cual era instalada dentro del teléfono móvil y no podía ser movilizada, con el pasar del tiempo, la movilidad e interoperabilidad fue un requisito crítico, por lo que se desarrolló una nueva SIM, la cual puede ser retirada de un teléfono móvil para luego instalarla en uno diferente.

Una tarjeta SIM almacena el número de serie, estado de la SIM, algoritmo de autenticación, algoritmo y número de secuencia de cifrado de señalización, algoritmo de cifrado de datos, clave de seguridad administrada por el usuario, identificador temporal de usuario móvil y el Identificador Internacional de usuario móvil (International Mobile Subscriber Identity, IMSI). La IMSI es un código único de identificación internacional para cada uno de los teléfonos móviles, está conformado por tres códigos, el Código de País Móvil (Mobile Country Code, MCC), Código de Red Móvil (Mobile Network Code, MNC) y MSIN. MCC contiene la información del país en servicio, MNC la información de la empresa

de telecomunicaciones que ofrece el servicio y MSIN es el identificador del teléfono móvil.

El bloque estación base es el encargado de la transferencia de información con el teléfono móvil. Se compone de la Estación Base Transceptora (Base Station Transceiver, BTS), Controlador de Estación Base (Base Station Controller, BSC) y Unidad de Transcodificación (Transcodification Unit, TRAU).

La BTS es la encargada de mantener toda la información con el teléfono móvil por medio de la interfaz de aire. Sus atribuciones son encriptar la señalización de tráfico, monitoreo de los canales libres, enviar información de canales libres al BSC, direccionamiento de acceso de los teléfonos móviles que solicitan red, codificación para protección contra errores, medición de la intensidad de campo, medición de la calidad de señal recibida en cada teléfono móvil y envío de alarmas y advertencias en caso de que un teléfono móvil presente un comportamiento erróneo.

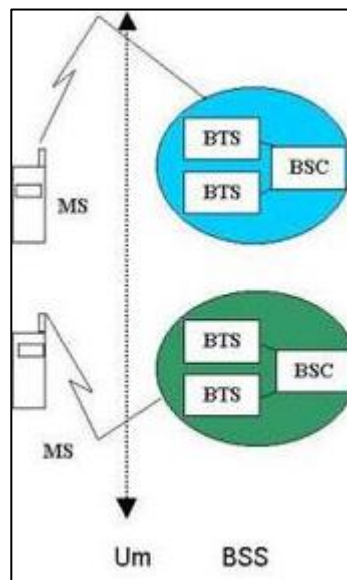
La BSC es el elemento principal del bloque BSS, entre sus funciones se encuentran establecer la comunicación entre el teléfono móvil y el bloque de conmutación de red, administrar los canales, control de potencia de la BTS, control de potencia del teléfono móvil, soportar la señalización de la interfaz de aire y control sobre llamada de voz (inicio y finalización). Es parte fundamental para el proceso de *handover* (un teléfono móvil cambia de BTS sin perder la llamada activa) ya que se encarga de realizar la comunicación entre las BTS vecinas. Adicional, BSC se encarga de la función de tarificación del servicio.

TRAU se encarga de la codificación y posterior decodificación de toda la información de la llamada de voz, también se ocupa de la adaptación de la

velocidad para la transferencia de datos. En la figura 2 se puede observar la estructura del bloque estación base.

El bloque de conmutación de red es la parte fundamental dentro de una arquitectura GSM, ya que es el encargado de iniciar, enrutar, controlar y finalizar un servicio (puede ser voz o datos). También almacenan datos de cada uno de los suscriptores. Los elementos que conforman este bloque son el Centro de Conmutación Móvil (Mobile Switching Center, MSC), Registro de Ubicación Local (Home Location Register, HLR), Registro de Ubicación de Visitantes (Visitor Location Register, VLR), Centro de Mensajes de Texto Corto (Short Message Service Center, SMSC), Registro de Identificación de Equipos (Equipment Identification Register, EIR) y el Centro de Autenticación de Usuario (Authentication User Center, AUC).

Figura 2. **Bloque estación base**



Fuente: *Rayan Sple*. <http://www.rayansple.com/Redes+en+telefon%C3%ADa+celular>.

Consulta: julio de 2016.

La MSC es el elemento principal del bloque de conmutación de red, su función principal es el control y administración de una llamada de voz. La MSC debe conocer el origen y destino de cada una de las llamadas. Otras de las funciones de la MSC incluyen la actualización geográfica del teléfono móvil, administración de canales disponibles, administración de los recursos disponibles, coordinación del proceso de traspaso de llamada *Handover*, administración de las frecuencias utilizadas por cada estación base, codificación, supresión de ruido y coordinación de toda la información manejada por todos los equipos adyacentes por medio de los enlaces de comunicación.

Para intercomunicarse con la red pública la MSC utiliza el protocolo de comunicación denominado Sistema de Señalización No.7 (Signalling System No. 7, SS7). SS7 consiste en un conjunto de protocolos de señalización telefónica empleados en las redes de telefonía móvil, basa su funcionamiento en el sistema de conmutación por paquetes. SS7 permite que diferentes conmutadores intercambien mensajes de señalización de los circuitos establecidos entre ellos.

Por medio del protocolo SS7 se obtiene un estándar para la señalización dentro de la arquitectura de red. Las características más importantes de este protocolo se encuentran la capacidad que tiene un solo enlace para soportar decenas de troncales, alta velocidad para la transferencia del tráfico de señalización, su arquitectura es de fácil implementación, costos de implementación bajos, alta adaptabilidad a las redes externas y cambios dentro de la red. Las rutas de señalización se asignan de forma estática, las rutas que ya se encuentran configuradas son denominadas *RouteSet*. Dentro del sistema SS7 existen 3 tipos de nodos, el primero llamado Punto de Transferencia de Señal (Signal Transfer Point, STP), Punto de Conmutación de Servicios

(Service Switching Point, SCP) y el Punto de Control de servicios (Service Control Point, SSP).

Un STP es utilizado para la transferencia de información entre los nodos de la red SS7, en la mayoría de los casos, los mensajes son recibidos sobre un *link* de señalización y transferidos hacia otro enlace. Los STP pueden ser independientes o integrados. Para los STP independientes pueden ser internacionales, nacionales, regionales o locales.

Un SSP es considerado como un interruptor de voz, lleva a cabo la administración del tráfico en la banda de voz la señalización SS7. Un SSP puede ser el origen o destino de los mensajes, pero no puede realizar la función de transferencia.

El SCP básicamente es una interfaz de comunicación entre las bases de datos y la red SS7. Cuando se recibe una llamada, el SCP realiza una consulta al SDP y este devuelve información con la cual se puede identificar geográficamente a donde se debe enviar la llamada.

El HLR es una base de datos, la cual almacena información sobre todos los suscriptores de la red de telefonía móvil. Para realizar una distribución de carga, es posible integrar más de un HLR en la red. Los identificadores de cada uno de los suscriptores son el código MSISDN e IMSI. Con el objetivo de enrutar correctamente una llamada de voz, dentro del HLR se almacenan los siguientes 2 tipos de información:

- Información general sobre el suscriptor, tal como el identificador internacional, servicios a los cuales está suscrito el usuario (pueden ser

gratuitos o servicios de paga), servicios suplementarios activos, servicios restringidos y estado actual del suscriptor.

- Información de la ubicación geográfica del suscriptor, tal como VLR utilizado, número de estación móvil y MSC.

El VLR, al igual que el HLR, es una base de datos, con la diferencia que el VLR es una base de datos que contiene información sobre suscriptores temporales dentro de la red de telefonía. Cada teléfono móvil es controlado por un VLR asociado con la MSC que le presta el servicio al teléfono. Cada vez que un teléfono móvil ingresa a una nueva zona de automáticamente se inicia un proceso de registro, la MSC envía una actualización de posición al VLR, y este a su vez envía una actualización de datos al HLR. Los datos temporales que se almacenan en el VLR son el MSISDN, IMSI, TMSI, MSRN y LAI.

Para el caso de un usuario haciendo *roaming*, el VLR de la red visitante se pone en contacto con el HLR de la red origen del usuario, y le solicita información de los servicios que el usuario tiene autorizados. Posterior a esto, ya se comunica con su MSC para permitir o no el uso de los servicios de la red visitante.

El AUC es el equipo encargado de la seguridad de los usuarios, su control de acceso al servicio de llamadas lo realiza mediante la autenticación de cada usuario que desea utilizar el servicio, Si la autenticación del usuario no es exitosa, el abonado no podrá acceder a ningún servicio dentro de la red. El proceso de autenticación se realiza mediante la verificación de una clave de identificación propia de cada usuario, la cual es llamada Ki. La clave Ki es utilizada para generar los datos que son utilizados para la autenticación de la IMSI y para generar otra llave que se utiliza para cifrar toda la comunicación existente entre la estación móvil y la red del operador.

Cada tarjeta SIM tiene almacenada una clave Ki, la cual también es almacenada dentro del AUC. Ki no es transmitida desde la tarjeta SIM hacia el AUC, pero se combina con la IMSI con fines de generar la clave de cifrado. Gracias a este sistema de autenticación han disminuido de manera considerable los robos o fraudes derivados de la clonación de tarjetas SIM.

El EIR consiste en una base de datos donde se almacenan los IMEI de cada uno de los teléfonos móviles registrados alguna vez en la red móvil. El EIR es el encargado de controlar el acceso a la red. Esta función la realiza mediante la inclusión de los IMEI en 3 diferentes listas de acceso, que son:

- Lista blanca. los IMEI que se encuentran dentro de esta lista tienen permitido establecer una conexión con la red de telefonía.
- Lista gris: los IMEI que se encuentran dentro de esta lista tiene permitido establecer conexión con la red de telefonía, pero estarán siendo vigilados con el objetivo de evitar usos indebidos del mismo.
- Lista negra. los IMEI que se encuentran dentro de esta lista tienen bloqueada la conexión con la red de telefonía, esto se debe a que fueron reportados como robados, perdidos, han sido utilizados para actividades criminales o la marca y el modelo no son permitidos dentro de la red.

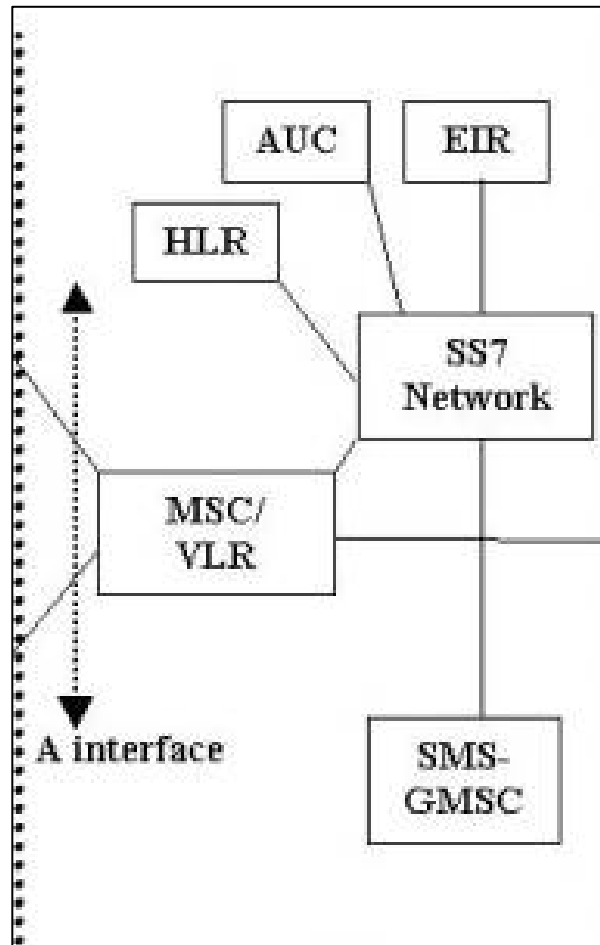
En SMSC es el encargado de todo el procesamiento y enrutamiento de todos los mensajes SMS. El SMSC se encarga de almacenar cada uno de los mensajes SMS hasta que son enviados o descartados. Dentro de las principales funciones del SMSC se encuentran recibir y almacenar todos los SMS enviados por usuarios, recibir y almacenar los SMS originados por cuentas propias del operador o servicios de valor agregado, comunicarse con el HLR para verificar los permisos de cada usuario, verificar en conjunto con el

HLR el estado actual del usuario de destino y generar registros de cada SMS recibido con fines de facturación y estadísticas.

El bloque de administración de red es el encargado de la parte de operación y mantenimiento de la red. Se encarga del monitoreo constante y simultaneo de todas las funciones y equipos que conforman la red de telefonía. Adicionalmente realiza las funciones de gestión, monitoreo y asignación de parámetros de configuración. Este bloque se encuentra conformado por el Centro de Administración de Red (Network Management Center, NMC), el Centro de administración y supervisión (SMC, Supervision Management Center) y el Centro de operación y mantenimiento (Operation and Maintenance Center, OMC).

En la figura 3 se observa la arquitectura de red del bloque de conmutación de red.

Figura 3. **Bloque conmutación de red**



Fuente: *Rayan Sple*. <http://www.rayansple.com/Redes+en+telefon%C3%ADa+celular>.

Consulta: julio de 2016.

Adicional a todos los equipos que conforman una red de telefonía GSM, se encuentran las interfaces las cuales son las encargadas de la comunicación entre los diferentes equipos y servidores. Dentro de las principales interfaces se encuentran la interfaz A, Abis, B, C, D, E, F, G, I y Um. La interfaz A transporta toda la información relacionada con las BSS, el control del tráfico de llamadas de voz y la movilidad de los usuarios. También se encarga de controlar los

circuitos que serán utilizados entre la BSS y la MSC. La interfaz Abis realiza el control del equipo de radiofrecuencia. La interfaz B se encarga de la comunicación entre la MSC y el VLR.

La interfaz C se encarga de la comunicación entre la MSC y el HLR (en caso exista más de un HLR, también se encarga de intercomunicar a la MSC con este otro HLR). La interfaz D se encarga de la comunicación entre el HLR y el VLR. La interfaz E se encarga de la comunicación entre las diferentes MSC dentro de la red de telefonía local. La interfaz F se encarga de la comunicación entre la MSC y el EIR. La interfaz G se encarga de la comunicación entre los VLR, ya sean de la red local o una red visitante. La interfaz H se encarga de la comunicación entre el HLR y el AUC. La interfaz I permite la comunicación entre la MSC y el teléfono móvil. La interfaz Um se encuentra ubicada entre la estación móvil y la BSS, esta interfaz tiene una tasa de transmisión de 13 Kbps para voz y 9,6 Kbps para datos.

1.2. Red 3G para servicios de transferencia de datos

En 1980, la ITU (International Telecommunications Union) inicio con el desarrollo de las normas técnicas para la creación de los estándares 3G. Una de las medidas que tomó la ITU fue reservar bandas frecuencias para sistemas 3G. Para la creación de los estándares 3G, la ITU se planteó los siguientes objetivos: tener una mayor capacidad de canal, así con un uso más eficiente del mismo, mayor flexibilidad en el uso de las bandas de frecuencia, ancho de banda ajustable, mejoras en la velocidad de acceso a las bases, itinerancia de datos entre redes de diferentes operadores e implementación de servicios multimedia.

En cuanto a los requisitos para cada estándar 3G, la IUT publicó los siguientes: alta velocidad para la transferencia de datos (para el enlace descendente la tasa de transferencia teórica es de 384 Kbps), transmisión de datos de forma simétrica y asimétrica, mantener la calidad de los servicios de voz ya existentes, mejorar la eficiencia del uso del canal para la transferencia de datos, ejecución simultánea de varios servicios, soporte para técnica de conmutación por paquetes, soporte para Emails y *roaming*. Los estándares 3G deben utilizar seguridad por medio de cifrado de bloques, el cifrado utilizado es Kasumi. Durante la conferencia WRC 2000 se asignaron, para los estándares 3G, los anchos de banda 850 - 960 MHz, 1 710 -1 980 MHz, 2 010-2 025 MHz, 2 110-2 200 MHz y 2 500-2 690 MHz.

1.2.1. Estándar UMTS

El estándar UMTS (Universal Mobile Partnership *Project*) es un estándar que cumple con los requisitos 3G. Fue desarrollado por la institución 3GPP (Third Generation Partnership Project). Para el acceso a radio, UMTS utiliza la técnica W-CDMA (Wideband Code Division Multiple Access), esta técnica ofrece una mayor eficiencia espectral y ancho de banda para los operadores de redes móviles. W-CDMA utiliza los métodos de operación TDD (Time Division Duplex) y FDD (Frequency Division Duplex). UMTS permite una mayor cantidad de usuarios en la red de acceso local, adicional brinda una mejor tasa de transferencia de datos. Las principales características del estándar UMTS son compatibilidad con los estándares 2G, reducción de costo en los servicios ofrecidos, tasa de transferencia de datos de hasta 2 Mbps, mayor cantidad de servicios multimedia, simetría y asimetría de servicios, punto central para redes móviles y fijas, 5 MHz de ancho de banda para cualquier tipo de celda, asignación dinámica del ancho de banda, mayor cantidad de usuarios soportados de manera simultánea, implementación del protocolo IP, utilización

de un perfil único de usuario para la asignación de servicios, VHE (Virtual Home Environment) el cual permite ofrecer los mismos servicios a un usuario sin importar su localización y utilización de la tecnología de conmutación por paquetes como base para su funcionamiento.

UMTS utiliza los siguientes tipos de celdas:

- Pico celda: esta celda trabaja en un ancho de banda de 5 MHz y su tasa de transferencia de datos es de 2 Mbps. Son utilizadas para cubrir áreas pequeñas (hasta 45 metros). Normalmente este tipo de celdas son implementadas dentro de centros comerciales y edificios.
- Micro celda: esta celda trabaja en un ancho de banda de 5 MHz y su tasa de transferencia de datos es de 384 Kbps. Son utilizadas para cubrir áreas medianas (hasta 1 000 metros). Normalmente este tipo de celdas son implementadas en áreas urbanas.
- Macro celda: esta celda trabaja en un ancho de banda de 5 MHz y su tasa de transferencia de datos es de 114 kbps. Son utilizadas para cubrir áreas medianas (hasta 35 Km). Normalmente este tipo de celdas son implementadas en áreas urbanas y rurales.

UMTS también utiliza la técnica UTRAN (Universal Terrestrial Radio Access Network) la cual está compuesta de múltiples estaciones base, que utilizan diferentes interfaces de radio, así como bandas de frecuencia. Sus fronteras son de la interfaz Iu al núcleo de red, y de la interfaz Uu al equipo de usuario.

Los servicios que ofrece UMTS se basan en capacidades comunes en todos los entornos de usuarios y radioeléctricos. Esto mediante el uso del servicio *roaming*, el cual se orienta desde la red local hacia la de otros operadores que trabajen bajo UMTS, por esta razón el usuario no nota cambio alguno al estar fuera de su red local. VHE también permite la gestión de las funcionalidades con la red visitada.

El estándar UMTS, permite a los operadores de red la asignación de estándares de más bajo nivel en escenarios específicos, es decir, permite la asignación de canales de EDGE a los usuarios de bajo ancho de banda y canales WCDMA a otros usuarios, con esto se logra una optimización de ancho de banda y con esto se mejora la eficiencia de la red local. Lo anterior también permite que los usuarios puedan tener acceso a una mayor cantidad de servicios de manera simultánea. En cuanto a la calidad del servicio de transferencia de datos, se contempla las siguientes clases de tráfico:

- **Conversacional:** transferencia de datos en tiempo real. Los usuarios finales son personas, por esta razón sus características están impuestas por la percepción del usuario. El retardo extremo a extremo debe ser bajo (menor a 400 ms). El tráfico suele ser bastante simétrico. En esta clase se tiene el tráfico de voz sobre IP, videoconferencia y videojuegos.
- **Interactiva:** transferencia de datos de forma bidireccional sin control de ancho de banda. En esta clase uno de los extremos solicita información a un equipo remoto. El tráfico suele ser muy poco simétrico. En esta clase tienen las solicitudes de localización geográfica y navegación por internet.

- *Streaming*: transferencia de datos de manera continua con un ancho de banda controlado. Esta clase es aquella en la cual la información es procesada y presentada al usuario final conforme van llegando los paquetes del flujo de información. El tráfico es totalmente asimétrico. En esta clase se tiene todo el tráfico multimedia.
- Subordinado: en esta clase los datos no son transferidos en tiempo real, esto debido a que los datos no son catalogados como de “alta importancia”.

La principal diferencia entre las diferentes clases de tráfico es la sensibilidad que poseen frente al retardo, que va desde la clase más sensible a retardos (conversacional) hasta la menos sensible (subordinado). En la tabla III se muestran una comparación entre las 4 clases de tráfico.

La siguiente tabla muestra un resumen de cada una de las clases anteriores con sus características generales y algunos ejemplos de aplicaciones

Tabla III. **Clases de tráfico UMTS**

Clases "UMTS Qos"	Características	Ejemplo de aplicación
Conversacional	Necesidad de retardo temporal corto y fijo entre unidades de información.	Voz, video telefonía y video juegos
Flujo continuo	Necesidad de retardo temporal fijo.	Multimedia de flujo continuo (TV, radio, etc.)
interactivo	Integridad de los datos (sin errores) y de respuesta del usuario (respuesta temporal no muy alta).	Aplicaciones de navegación web o juegos de red.
No crítico	Integridad de los datos, sin respuesta inmediata del usuario.	Correo electrónico, mensajes cortos.

Fuente: *Comunicaciones Móviles*. [http://www.ComUMoviles.com/Trafico+UMTS%](http://www.ComUMoviles.com/Trafico+UMTS%20). Consulta: julio de 2016.

Adicional a la clasificación por el tipo de tráfico, UMTS también se puede clasificar por el tipo de servicios ofrecidos, la clasificación es la siguiente:

- Mensajes
- Voz
- Datos
- Multimedia de velocidad media
- Multimedia de alta velocidad
- Multimedia de alta interactividad

1.2.2. Estándar HSPA

El estándar HSPA (High Speed Packet Access) es una fusión de dos estándares, el HSDPA (High Speed Downlink Packet Access) y HSUPA (High Speed Uplink Packet Access). En teoría, HSPA tiene tasas de transferencia máximas de 14,4 Mbps para el enlace descendente y 2 Mbps para el enlace ascendente. HSPA utiliza el tipo de modulación 16 QAM para el enlace ascendente y la modulación 64QAM para el enlace descendente.

Como se observa, con HSPA se duplica la tasa de transferencia máxima para el enlace ascendente y se quintuplica la tasa de transferencia máxima para el enlace descendente. Esto se logra mediante la utilización de uno de los siguientes métodos:

- Compartir el canal de transmisión. Con la utilización de este método se logra una mayor eficiencia en el uso de los códigos disponibles y de la potencia.
- Intervalos de tiempo más cortos. La utilización de este método conlleva una reducción en los tiempos de subida y bajada.

Una de las características más importantes de HSPA es que no requiere la utilización de portadoras adicionales, esto quiere decir que HSPA puede compartir la misma portadora con WCDMA. HSPA utiliza la técnica de acceso móvil WCDMA (Wideband Code Division Multiple Access), esta técnica proporciona mayor eficiencia en cuanto a la utilización del espectro. WCDMA puede utilizar uno de los siguientes tipos de multiplexación: multiplexación por división de frecuencia (FDD) y multiplexación división de tiempo (TDD). HSPA utiliza WCDMA FDD, entre sus características más importantes se encuentran:

- Tasa de transferencia de códigos de hasta 3,84 Mcps
- Ancho de banda de 5 MHz
- Longitud de trama de 10 ms
- Control de potencia de lazo cerrado de 1 500 Hz
- Para la codificación de voz se utiliza el protocolo AMR (Adaptative Multi Rate)
- Soporte para *handover* tipo *soft* y *hard*
- Diversidad en los modos de transmisión

En cuanto a la codificación de voz, se utiliza el protocolo AMR con 8 diferentes tasas de transferencia. Con esto se consigue que cuando la carga de una celda se incrementa, el sistema disminuye automáticamente la tasa de transferencia de algunos usuarios para poder soportar más usuarios. Adicional a esto, AMR ofrece la posibilidad técnica de adaptar el esquema de codificación utilizado a las diferentes condiciones del canal de radio. La codificación más robusta es utilizada bajo condiciones de mala propagación, mientras que la codificación con tasa de transferencia más alta, es utilizada bajo condiciones de propagación buenas. Durante la comunicación, el receptor mide la calidad del enlace de radio y debe regresar al transmisor la medición de la calidad del enlace o la codificación que debe utilizar en la próxima trama.

Mediante la codificación del canal, se puede mejorar la correlación entre símbolos con el fin de que, si existe una interferencia se pueda recuperar la señal. Dependiendo del tipo de servicio se pueden utilizar los siguientes dos tipos de codificación: código de convolucional para los servicios de voz y turbocódigo para los servicios de datos. La convolución es utilizada para contrarrestar la interferencia, mediante la introducción de varios bits de redundancia en la trama de información original. La comunicación sobre un canal de radio está caracterizada por un desvanecimiento rápido, lo que puede

ocasionar un gran número de errores consecutivos; la mayoría de los esquemas de codificación funcionan mejor con errores aleatorios que con bloques completos de errores. Mediante el intercalado de datos, no se transmiten dos bits adyacentes juntos, por lo que los errores son aleatorizados.

Otro aspecto importante es el control de potencia en particular para el enlace ascendente, ya que, sin un control adecuado, un solo teléfono puede bloquear una celda completa, ya que se trabaja en la misma frecuencia, y dos móviles están separados del nodo B solo por sus respectivos códigos de esparcimiento. Existen dos tipos de control de potencia: de lazo abierto y de lazo cerrado.

Para el control de potencia de lazo abierto, básicamente se realiza una medición superficial de las pérdidas por trayectoria mediante un mecanismo que consiste en enviar el primer mensaje de señalización con la mínima cantidad de potencia, en el caso que no haya respuesta de parte del Nodo B, se comienza a incrementar la potencia hasta que se tenga una respuesta del Nodo B. En el control de potencia de lazo cerrado la estación base hace mediciones de la relación señal – interferencia recibida, y la compara con una medición estándar. Si la medición es mayor que la estándar, la estación base mandará un aviso para que se disminuya la potencia, en el caso que la medición sea menor que la estándar, se mandará una notificación para aumentar la potencia. Cada medición y envío de notificaciones se realiza 1 500 veces por segundo.

1.2.3. Estándar HSDPA

El estándar HSDPA (High Speed Downlink Packet Access) es un estándar de tercera generación, también conocido como 3,5G. HSDPA fue publicado en el Release 5 de 3GPP; este estándar provee una mejora en la tasa de

transferencia en el enlace ascendente, dicha velocidad es de hasta 384kbps. HSDPA se basa en la transmisión de canal compartido y sus principales características son:

- Uso compartido del canal.
- Transmisión múltiple de códigos.
- Modulación de orden superior.
- Intervalos de tiempo de transmisión cortos.
- Rápida adaptación al enlace.
- Soporte de la técnica HARQ (Hybrid Automatic Repeat Request)
- Alta velocidad del canal compartido para el enlace descendente.
- Modulaciones QPSK y 16 QAM.
- Soporte para el protocolo MAC-HS (High Speed Medium Access Protocol).
- Rápida programación y diversidad de usuarios.

Para el enlace descendente se utilizan canales de alta velocidad llamados High Speed Physical Downlink Shared (HS-PDSCH). En un mismo canal de radio pueden operar más de 15 canales HS-PDSCH, con un ancho de banda de 5 MHz y un factor de extendido de 16. Las transmisiones de datos de los usuarios son asignadas a uno o más canales por intervalos de tiempo de transmisión de 2 ms, con esto se consigue una red más dinámica. La característica fundamental de HSDPA es su capacidad de combinar modulaciones y codificaciones; a esta técnica se le denomina AMC (Adaptive Modulation and Coding); dicha técnica permite disponer de las modulaciones QAM y QPSK, cada una de estas modulaciones se utilizan dependiendo de la calidad de recepción de la señal por parte del usuario.

HSDPA introduce un canal rápido compartido para el enlace de bajada denominado HS-DSCH (High Speed Downlink Shared Channel), el cual está utiliza un SF constante de 16. Dentro de las principales características de este canal se pueden mencionar la capacidad de asignar hasta 15 canales a un solo usuario, soporte de la modulación 16QAM, uso de retransmisiones a nivel físico, utilización de turbo códigos, a nivel de *slot* no se utilizan retransmisiones continuas. Adicionalmente, se introduce el canal HS-SCCH, conocido como el canal de control, es un canal físico para el enlace de bajada que se encarga de la transmitir la información de control, la cual es necesaria para el proceso de demodulación y decodificación por parte del equipo móvil. Cada vez que un usuario utilice HS-DSCH se debe enviar un HS-SCCH con un SF de 128 y estructura basada en un TTI de 2 ms. Este canal está dividido en dos partes: la primera parte contiene información sobre la modulación y canalización utilizada, la segunda parte consiste en el tamaño de bloque de transporte y la información del ARQH. El canal HS-SCCH transporta la siguiente información del canal HS-DSCH:

- Información del tipo de canalización utilizada
- Información del tamaño de bloque
- Información sobre el ARQH
- Tipo de modulación utilizada
- Tipo de codificación utilizada
- Identificador del equipo móvil

La técnica ARQH es una variación del método para la detección y corrección de errores llamado ARQ. ARQH aún continúa utilizando los códigos de redundancia cíclica, pero a diferencia de ARQ se añade la utilización de los FEC (Forward Error Correction). ARQH se caracteriza por tener una rápida respuesta ante los errores. En el caso que se detecte un error, se solicitará la

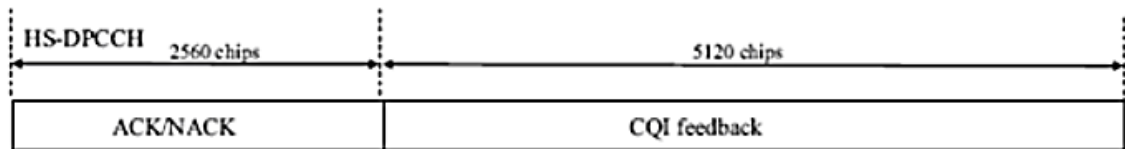
retransmisión, posteriormente se combinara con las transmisiones anteriores (esto se realiza antes del proceso de decodificación del mensaje). Si toda la información es correcta, es decir, no se detectaron errores, se procede a enviar, por el canal HS-DPCCH, una notificación conocida como ACK.

Existen dos técnicas para el uso del ARQH: IR (Incremental Redundancy) y el CC (Chase Combining). En la técnica IR se aplica un código convolucional a los datos transmitidos, esto genera un nuevo bloque de datos. A este nuevo bloque se le aplica una perforación, la cual consiste en quitar algunos bits y se dividir dicho bloque en bloques más pequeños, los cuales tienen la misma cantidad de datos que tenía antes de pasar por el código convolucional, posteriormente a estos bloques se les añade un código CRC y posteriormente se transmite la información. Si el primer bloque es recibido con errores, se envía el segundo y se combina con el primero y así sucesivamente hasta que los datos sean recibidos sin errores.

Si se utiliza la técnica CC, los datos se transmiten de forma normal con el CRC ya añadido. Si los datos son recibidos con errores, el retransmisor solicitará una retransmisión, este receptor almacenará todas las retransmisiones y las combina hasta conseguir que la información llegue sin errores. Ambos canales se envían en los tres *slots* que contiene el canal HS-DPCCH con un TTI de 2 ms.

En la figura 4 se observa la estructura de un canal HS-DPCCH.

Figura 4. Estructura canal HS-DPCCH



Fuente: GSM Arena. http://www.gsmarena.com/HSDPA_canal_HSDPCCH.jpg.

Consulta: julio de 2016.

Para el enlace de subida se utiliza el canal dedicado DCH, el cual es mapeado en el canal físico DP-DCH, su SF puede tomar valores de entre 4 y 256, con 7 posibles tramas y un valor tasa de transferencia máxima de 384 Kbps. Para el caso de las llamadas de voz o video se continúan utilizando los canales y protocolos especificados en el release 99.

En la tabla IV, se observan las características de las diferentes clases del protocolo HSDPA existentes.

Tabla IV. Clases HSDPA

Categoría HSDPA	Número máximo de códigos HS-DSCH por celda	Tipo de modulación utilizada	Tasa de transferencia máxima para el enlace descendente en Mbps
1	5	16-QAM	1,2
2	5	16-QAM	1,2
3	5	16-QAM	1,8
4	5	16-QAM	1,8
5	5	16-QAM	3,6
6	5	16-QAM	3,6
7	10	16-QAM	7,2
8	10	16-QAM	7,2
9	15	16-QAM	10,1
10	15	16-QAM	14
11	5	QPSK	0,9
12	5	QPSK	1,8

Fuente: elaboración propia.

1.2.4. Estándar HSUPA

El protocolo HSUPA fue introducido en el Release 6 de 3GPP. HSUPA agrega un nuevo canal de transporte llamado E-DCH (Enhanced Dedicated Channel). Con HSUPA se consigue mejorar el desempeño del enlace ascendente, con esto se logra una reducción de la latencia, un aumento de las tasas de transferencia de datos y la capacidad. La transferencia de datos en HSUPA ofrece una gran cantidad de nuevas y mejores características, tales como nuevos medios de control de acceso, nodos B y RNC.

Adicionalmente, se pueden mencionar las transmisiones *multi code*, reducción del TTI, soporte de Fast Hybrid Automatic Repeat ReQuest y soporte para *Fast Scheduling*. El nuevo canal E-DCH no puede ser compartido entre diferentes usuarios, es decir es dedicado a un solo usuario, por esta razón puede ser usados hasta cuatro códigos para aumentar las tasas de transferencia de datos del enlace de subida. En el protocolo FHARQ el nodo B puede requerir una rápida retransmisión de la información (si esta es recibida con errores), lo que hace que el sistema sea más robusto contra los errores. HSUPA logra mejorar el *soft handover*, esto se logra mediante la unificación de todas las estaciones base y sectores involucrados en la decodificar la información.

Para el enlace ascendente, la característica más importante es la capacidad para tolerar cierta cantidad de interferencia, la cual es igual a la potencia recibida por la estación base. Por lo general, mientras mayor sea la tasa de datos, mayor es la potencia de transmisión requerida y mayor es el consumo de recursos. El protocolo *fast scheduling* permite una reubicación dinámica de los recursos, adicionalmente permite que el sistema soporte un mayor número de usuarios, así como rápidas adaptaciones ante variaciones de

interferencia. Como el algoritmo de *scheduling* no se encuentra estandarizado, diferentes estrategias pueden ser implementadas, lo cual es útil ya que diferentes ambientes y distintos tipos de tráfico pueden requerir diferentes requerimientos en la estrategia de *scheduling*.

Adicional al este modo de transmisión, HSUPA también permite un modo de transmisión auto iniciado desde las estaciones móviles, este modo de transmisión es denominado *non-Schedule*, este modo se utiliza para los servicios VoIP, ya que para estos servicios la reducción del TTI y el planificador basado Nodo B no son capaces de proporcionar el tiempo de retardo y ancho de banda constante necesarios.

Cada flujo de datos MAC-d (es decir, el QoS) está configurado para utilizar ambos modos de transmisión, Schedule y Non-Schedule. La estación móvil ajusta la tasa de transferencia de datos, independiente de cual sea el modo de transmisión utilizado. La tasa máxima de transferencia de datos, para ambos modos de transmisión, está configurada en el establecimiento de la llamada, y por lo general no cambian con frecuencia. La energía utilizada es controlada dinámicamente por el Nodo B a través de la concesión absoluta (que consiste en un valor real) y la concesión relativa mensajes.

HSUPA, a nivel de capa física, introduce los siguientes canales: E-AGCH (Absolute Grant Channel), E-RGCH (Relative Grant Channel), F-DPCH (Fractional-DPCH), E-Hich (E-DCH Hybrid ARQ Channel Indicator), E-DPCCH (E-DCH Dedicated Physical Control Channel) y E-DPDCH (e-DCH Dedicated Physical Data Channel). El canal E-DPDCH es utilizado para transportar la información del canal E-DCH, y el canal E-DPCCH es utilizado para transportar la información de control asociada con el canal E-DCH.

En la tabla V, se observan las características de las diferentes clases del protocolo HSUPA existentes.

Tabla V. **Clases HSUPA**

Categoría HSUPA	Tasa de transferencia máxima para el enlace ascendente en Mbps	Tipo de modulación utilizada
1	0,73	QPSK
2	1,46	QPSK
3	1,46	QPSK
4	2,93	QPSK
5	2,10	QPSK
6	5,76	QPSK

Fuente: elaboración propia.

1.2.5. Estándar HSPA+

El estándar HSPA+, también denominado E-HSPA (Evolved HSPA), fue definido en el Release 7 de 3GPP. Este estándar provee tasas de transferencia de datos de hasta 84 Mbps para el enlace ascendente y 22 Mbps para el enlace descendente. Estas tasas de transferencia son logradas mediante la utilización de una técnica multi antena llamada MIMO 2x2 (Multiple-Input Multiple-Output) y el tipo de modulación 64-QAM. Las versiones más recientes del estándar HSPA+ soportarán tasas de transferencia máximas de hasta 168 Mbps para el enlace ascendente, y hasta 672 Mbps para el enlace descendente, esto mediante la utilización de múltiples portadoras y técnicas avanzadas de antena. Las características más importantes del estándar HSPA+ son:

- Aumento de la tasa máxima de transferencia de datos para el enlace ascendente y descendente.
- Compatibilidad con UMTS.
- Reducción de latencia.
- Soporte a servicios de voz y datos dentro de la misma portadora.
- Soporte simultaneo de servicios de voz y datos.
- Mejora en la eficiencia de los servicios de banda ancha.
- Reducción del consumo de potencia.

HSPA+ ofrece los servicios de voz sobre IP (VoIP), videoconferencias, juegos en línea, *streaming*, televisión, y el denominado *triple play* el cual incluye televisión, internet y telefonía.

1.2.6. Arquitectura de red 3G

La arquitectura de una red 3G, es fundamentalmente una red GSM más un *core* de datos conocido como Packet Core. Básicamente una arquitectura 3G se encuentra conformada por el dominio de equipo de usuario, dominio de núcleo de red y el dominio de red de acceso.

El dominio de equipo de usuario se encuentra conformado por los módulos de identidad, tarjeta SIM y estación móvil. Los dominios de núcleo de red y red de acceso unificados conforman el dominio de infraestructura. El dominio de núcleo de red está conformado por los subdominios red de servicio (SN), red local (HN) y red de tránsito (TN). El subdominio red de servicio representa la red de acceso local a la cual pertenece el usuario. El subdominio red local representa la red a la cual se encuentra registrado el usuario. El sub-dominio red de tránsito representan a la red en la cual se encuentra registrado el usuario

receptor. El dominio de red de acceso, a diferencia del dominio de núcleo de red, depende directamente de la técnica de acceso utilizada.

Dentro del dominio de infraestructura, los elementos de red 2G que se mantienen son BTS, BSC, MSC, HLR, EIR, VLR, AuC y OSS. Los nuevos elementos que se incorporan son SGSN, GGSN, MGW, RNC, Nodos B.

El SGSN (Serving GPRS Support Node) es un elemento del bloque denominado Packet Core, el cual tiene como función principal proporcionar a las estaciones móviles el acceso a la red de datos. Entre las funciones principales del SGSN se encuentran realizar la autenticación de la estación móvil, realizar enrutamientos, transferencia de los paquetes de información, control de la ubicación de las estaciones móviles, control de la información del suscriptor e interconexión con el GGSN. Para llevar a cabo todas estas funciones el SGSN se apoya en una serie de servicios anteriormente configurados, entre los cuales se encuentran el SGSN Service, el MAP Service, el SGTP Service y el GTPP Service.

El SGSN Service se utiliza para establecer una conexión hacia la RNC. El MAP Service se utiliza para establecer una conexión con el HLR. El SGTP Service se utiliza para establecer una conexión con el GGSN, el SGSN y GGSN son elementos que dependen uno del otro, es decir sin la debida autenticación y enrutamiento del SGSN, un usuario jamás podrá registrarse en el GGSN. El GTPP Service el cual se utiliza para soportar todos los procesos de tarificación y facturación. Dentro de la información de usuario que almacena el SGSN se encuentra el VLR y HLR a los cuales se encuentra registrado el usuario, información de ubicación, identificadores temporales e IMSI, información de suscripción y servicios y su dirección PDP.

El GGSN (Gateway GPRS Support Node) es el elemento del Packet Core que le permite al usuario poder acceder a la nube, esto se cumple debido a que el GGSN cumple con las funciones de ruteo, modem y seguridad. Básicamente, se puede decir que es la puerta de salida hacia la PDN de una red de telefonía local, estas redes externas pueden ser Internet o una red corporativa (Intranet); dependiendo de la configuración de la red local, puede, o no, controlar (mediante los APNs) una parte de autenticación o autorización de navegación denominada Radius/Diameter.

Los APN (Access Point Name) son puntos de accesos con diferentes configuraciones que son usados con diferentes usuarios. Dentro de sus configuraciones se puede establecer la forma en que los usuarios acceden a la red. La información que puede indicar un APN es:

- Tipo de usuario (prepago, pospago o híbrido).
- Nombre y claves de usuario.
- Punto de conexión.
- Tipo de autenticación.
- En caso de usar Proxy, la dirección IP del mismo.
- La tasa de transferencia de datos máxima (para el enlace ascendente y descendente).
- MCC (Mobile Country Coder) y MNC (Mobile Network Code) de la red local.
- Tipo de protocolo IP.

El MGW (Media Gateway) es un elemento físico/lógico, cuya función principal es servir de puente o conexión entre dos o más elementos de la red que utilizan diferentes tipos de señalización, para hacer posible esta conexión, el MGW traduce los diferentes tipos de señalización a lenguaje de *switch*.

Adicional el MGW se encarga de controlar la señalización de todos los Gateways que transportan el control de señalización de las llamadas.

Los Nodos B tienen como función principal realizar la administración de los protocolos de todas las interfaces de aire pertenecientes a la red local. Por esta razón, las funciones realizadas por un Nodo B están ligadas al método de acceso al canal de aire. Un solo Nodo B puede soportar más de una celda, aunque compartiendo el recurso disponible con cada una de ellas. Un Nodo B se encuentra conformado por dos elementos lógicos: el de transporte común y los TTP. La función de transporte común se realiza a través de los canales de transporte común que son utilizados por la estación móvil para el acceso inicial a la red. Entre las funciones de un Nodo B se encuentran las siguientes:

- Administración de los protocolos de la interfaz de aire
- Mapeo de recursos lógicos
- Transmisión de información del Sistema
- Coordinación con la RNC
- Administración del control de potencia de lado cerrado
- Realización de combinación para la diversidad
- Generación de códigos para el acceso a la red
- División de las tramas de datos internos
- Monitoreo y reporte de interferencias para el enlace de subida

Debido a que un Nodo B es un elemento transceptor (que recibe y envía información), un modulador debe ser configurado para modular toda la información. Las modulaciones utilizadas son QPSK y 16QAM.

El último nuevo elemento incorporado por una arquitectura 3G es la RNC (Radio Network Controller), la cual tiene como función principal realizar la

administración de los Nodos B que se encuentren conectados a la RNC. Una RNC puede ser de tipo de transferencia, control o servicio. Una RNC de transferencia es la que realiza las funciones de transferencia de usuarios entre celdas (*handover*). Una RNC de control es aquella que tiene como función principal la administración de todos los elementos de transporte común. La RNC de servicio tiene como función principal establecer, mantener y finalizar las conexiones de radio.

Entre las funciones principales de una RNC se encuentran la administración de los recursos de transporte de la interfaz lu, administración de la información del sistema, realización de los *handover*, administración de los recursos lógicos del Nodo B, administración de tráfico de todos los canales comunes, administración de los horarios de la información del sistema, control de potencias para los enlaces ascendentes y descendentes, división de las tramas de datos transferidas sobre varios Nodos B, generación y administración de reportes de tráfico, control de acceso y asignación de códigos de canalización.

2. PROTOCOLO DE SEÑALIZACIÓN SS7

El protocolo de señalización SS7 es un conjunto de protocolos de señalización de telefonía desarrollado en 1975. Este protocolo es utilizado para la traducción de números, portabilidad de números locales, facturación de usuarios prepago, servicio de mensajes cortos (SMS), y comunicación entre elementos de la arquitectura de la red local. El protocolo de señalización SS7 funciona mediante la conmutación de paquetes. Está conformado por STP (Signaling Transfer Point) y equipos de finalización (conmutadores, bases de datos o servidores). Por medio del protocolo de señalización SS7 dos conmutadores telefónicos pueden intercambiar en todo momento mensajes de señalización independientemente de los circuitos establecidos entre ellos.

SS7 fue diseñado para cumplir con los siguientes propósitos: soportar su uso en redes de telecomunicaciones digitales relacionadas con el intercambio de programas controlados digitalmente, usando canales digitales de 64 Kbps, proveer un medio confiable para la transferencia de información, cumplir con los requisitos de transferencia de llamada, control remoto, administración y mantenimiento, capacidad de adaptación para el uso de conexiones punto a punto.

2.1. Fundamentos básicos y características

Como se mencionó, SS7 está conformado por una serie de protocolos de canal común. El primer protocolo de canal común conocido como SS6 (Signalling System No. 6) fue publicado en 1977. Debido a que SS6 únicamente soportaba señalización de 28 bits, no contaba con una alta capacidad de

adaptación e integración con los sistemas digitales. Por esta razón en 1980, se definió el protocolo SS7 como un estándar internacional.

Entre las funciones principales del protocolo SS7 se encuentran establecimiento y enrutamiento de una llamada, transferencia de información de usuario, proveer los recursos necesarios para que diferentes equipos de conmutación distantes entre sí puedan comunicarse, soportar servicios inalámbricos tales como servicios PCS, *roaming* inalámbrico, autenticación de usuarios, portabilidad de números telefónicos locales, soporte de servicios extras de telefonía tales como llamada tripartita, llamada en espera y retorno de llamada.

SS7 utiliza la función de señalización de canal-común para el enrutamiento de los mensajes de control, estos mensajes son pequeños paquetes que contienen información del sistema. El sistema SS7 define cada una de las funciones que deben ser realizadas en la parte de conmutación de paquetes, este método es conocido como Modo de Señalización Asociado. Adicional existe el Modo de Señalización No Asociado en el cual algunos elementos de la red de conmutación transportan únicamente los paquetes de control.

A los nodos de señalización se les conoce como puntos de señalización. Un punto de señalización tiene la capacidad de realizar la discriminación de mensajes, esto quiere decir que los puntos de señalización son capaces de leer la dirección del encabezado de cada mensaje y posteriormente determinar si el mensaje es destinado a ese nodo. Entre las principales características del protocolo SS7 se tienen: confiabilidad y robustez, utilización de un solo enlace de señalización para brindar soporte a cientos de troncales, adaptabilidad a diferentes tipos de arquitectura de red, alta velocidad de transferencia,

reducción de costo de implementación, así como menor cantidad de elementos físicos.

2.2. Tipos de señalización

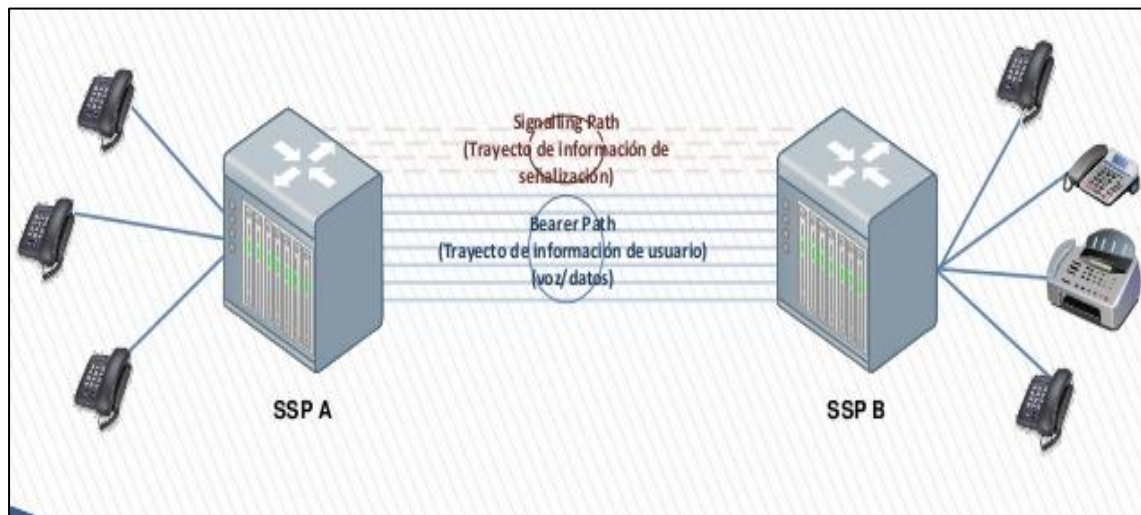
El protocolo de señalización SS7 puede utilizar 3 diferentes tipos de señalización conocidos como modo asociado, modo cuasi asociado y modo disociado. El modo a utilizar se define mediante el estudio de la relación entre el elemento/entidad y el canal.

El tipo de señalización más utilizado es el modo asociado. En el modo asociado, el canal de señalización es paralelo al circuito de voz, permitiendo el intercambio de la información de señalización; en otras palabras, en este modo los canales que transportan la información del usuario siguen la misma ruta directa entre puntos de señalización adyacentes. Siguiendo los conceptos del protocolo SS7, se concluye que entre dos puntos de señalización se debe utilizar el modo asociado mandatoriamente.

El modo asociado requiere de un canal de señalización entre un SP en particular y todos los otros SP, esto quiere decir que los mensajes de señalización siguen la misma ruta; por esta razón el modo asociado no es ideal para todos los tipos de red. En este caso el diseño de confiabilidad para los enlaces de señalización es simple, ya que todos los enlaces comparten el mismo método de transmisión. Las redes que emplean únicamente señalización en modo asociado son más fáciles de diseñar; sin embargo, estas son menos económicas excepto para redes pequeñas. El modo asociado requiere que cada conmutador en la red tenga enlaces de señalización con cada uno de los conmutadores con los que está interconectado.

En el modo asociado dos enlaces de señalización, como mínimo, son utilizados para redundancia. En la figura 5 se muestra la estructura del modo asociado.

Figura 5. **Modo asociado**

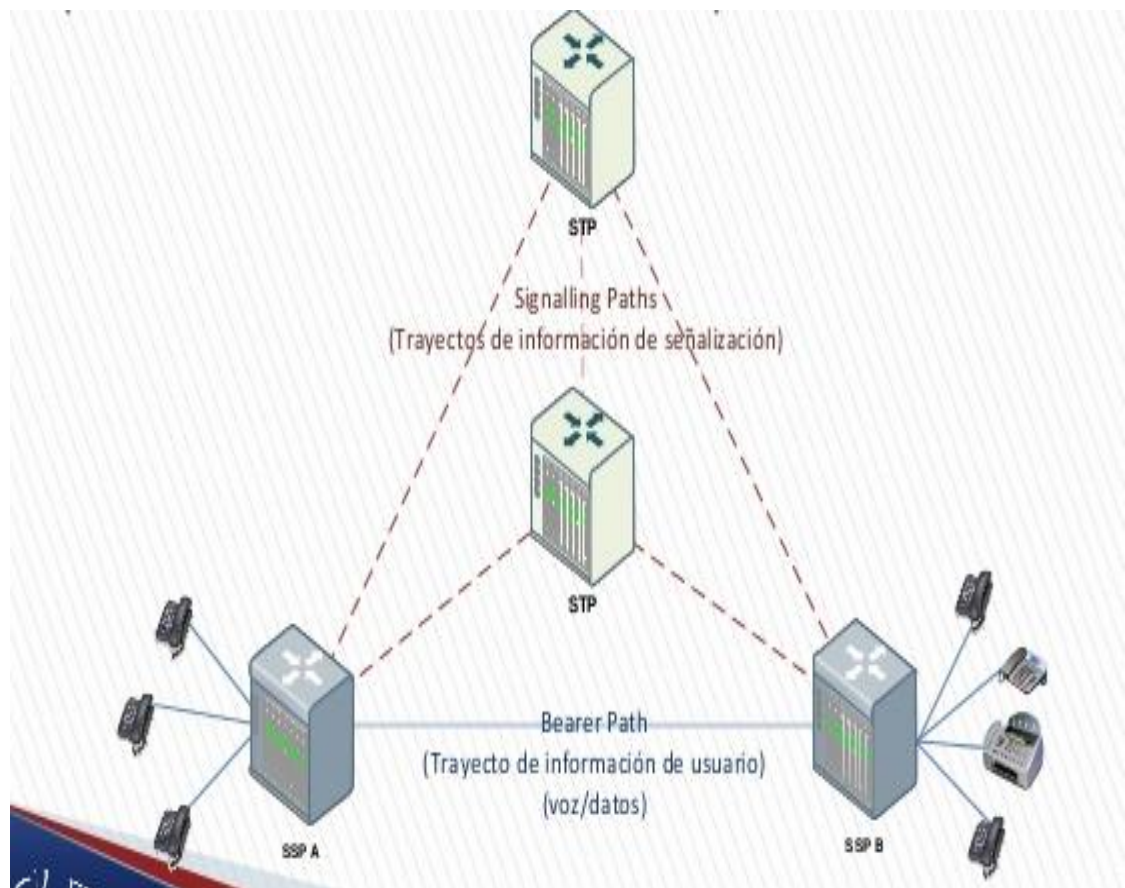


Fuente: NTPU. http://www.ntpu-es.com/SS7/Asoc_Mode.jpg. Consulta: julio de 2015.

En el modo cuasi asociado, los paquetes de información requieren de un número mínimo de STP para poder llegar a su destino final. De los tres modos, este es el modo más utilizado cuando se minimiza el tiempo necesario para el enrutamiento de los paquetes de información. Todos los paquetes de información que son enrutados a un mismo destino final, deben tomar la misma ruta. En otras palabras, en este modo la información de toda la señalización es enrutada entre dos puntos de señalización no adyacentes o distantes, conectados al mismo par de STP, mediante una ruta ya establecida con anterioridad.

Las redes que utilizan el modo cuasi asociado hacen un mejor uso de los recursos de los enlaces de señalización. Pero en contraparte, tienden a crear redes más complejas y grandes. El modo de cuasi asociado es la opción más económica para rutas con poca carga en cuanto a la transferencia de paquetes, debido a que, en este modo se evita la necesidad de enlaces directos. La señalización es enrutada a través de uno o más nodos intermedios. En la figura 6 se observa la estructura del modo cuasi asociado.

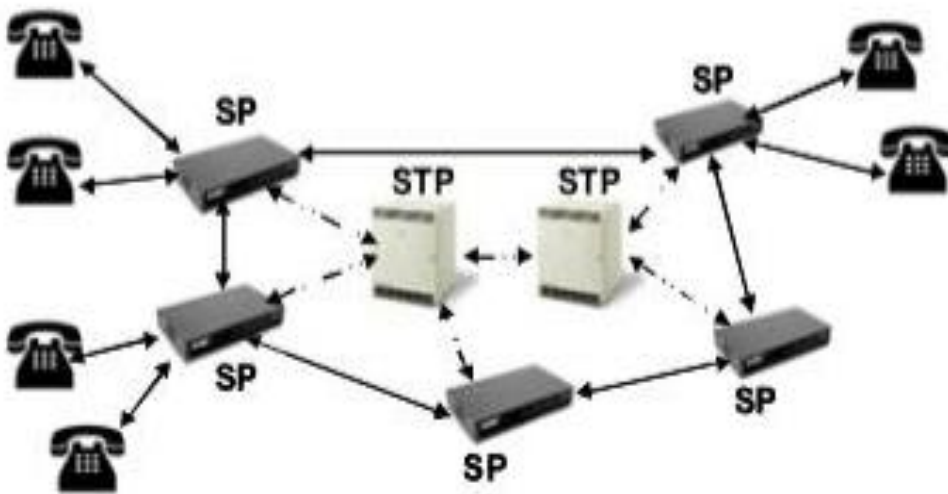
Figura 6. **Modo cuasi asociado**



Fuente: NTPU. http://www.ntpu-es.com/SS7/Asoc_QMode.jpg. Consulta: julio de 2015.

En el modo disociado todos los paquetes de información son enrutados a su destino final por rutas diferentes, para ello es necesaria la utilización de un gran número de nodos intermediarios, los cuales son conocidos como puntos de transferencia de señalización. Los STP son utilizados para dirigir los datos de señalización entre los SP. En el modo disociado, si dos paquetes de información independientes tienen un mismo destino final, pueden ser enrutados por dos distintas rutas, el cual es el funcionamiento del método de enrutamiento en el protocolo IP. En la figura 7 se muestra la estructura del modo disociado.

Figura 7. **Modo disociado**



Fuente: *NTPU*. http://www.ntpu-es.com/SS7/Asoc_QMode.jpg. Consulta: julio de 2015.

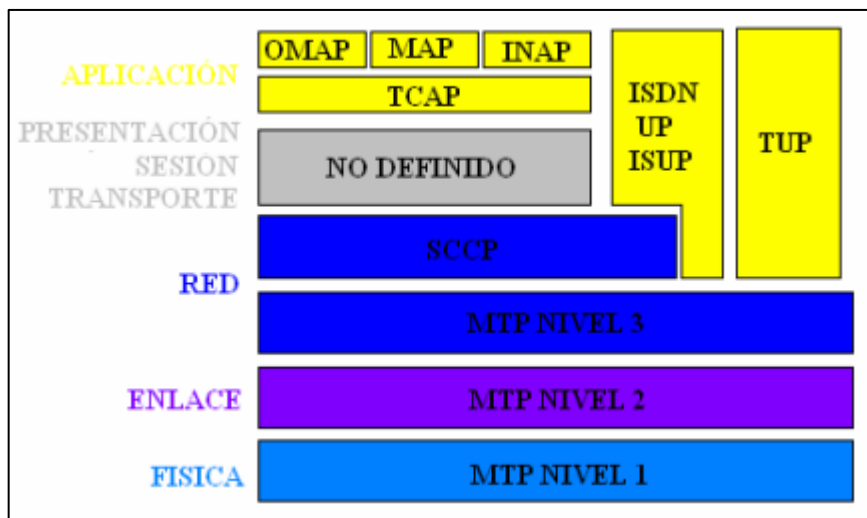
Los modos de señalización asociado y cuasi asociado, poseen la característica de asegurar una entrega secuencial de los paquetes de

información, esto los aventaja sobre el modo disociado ya que este no cuenta con esta característica.

2.3. Arquitectura

Una de las características, a nivel de arquitectura, es que el protocolo SS7 puede optar por más de una arquitectura base, esto depende básicamente de la elección que realice el administrador de la red local. La arquitectura SS7 está conformada por enlaces de señalización, rutas, nodos de señalización, puntos de señalización. En la figura 8 se muestra la estructura base del protocolo SS7.

Figura 8. Estructura base protocolo SS7



Fuente: NTPU. <http://www.ntpu-es.com/SS7/Structure%33.jpg>. Consulta: julio de 2015.

Como se observa en la figura, el protocolo SS7 basa su funcionamiento en el modelo OSI. OMAP (Operation, Maintenance and Administration Part) es el encargado de las funciones de operación y mantenimiento. MAP (Mobile Application Part) es la parte de la aplicación móvil. INAP (Intelligent Network

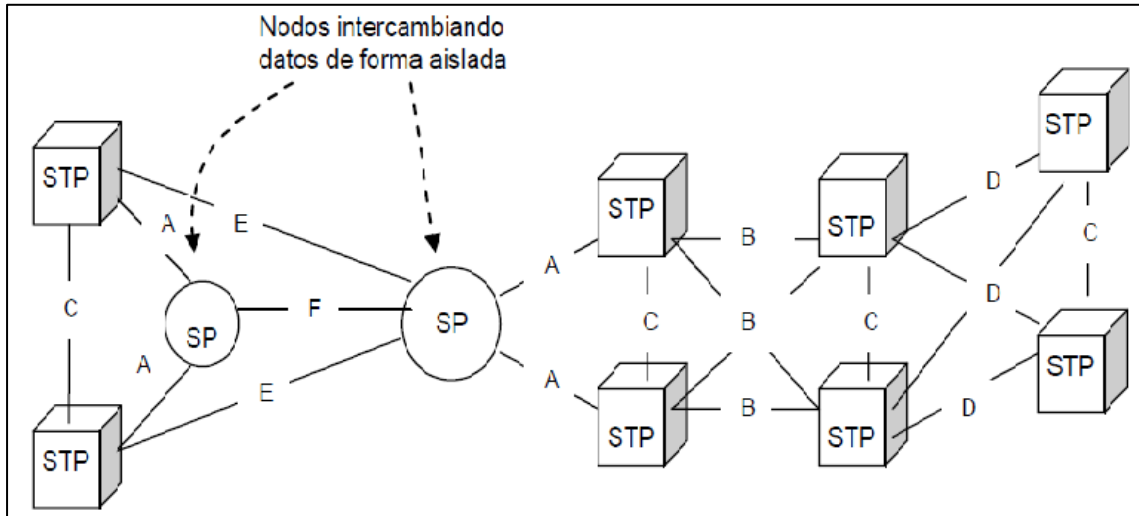
Application Part) es la parte encargada de las aplicaciones de red inteligente. TCAP (Transaction Capabilities Application Part) es la parte de aplicación de capacidades de transacción. ISDN UP (ISDN user Part) es la parte ISDN del usuario. TUP (Telephone User Part) es la parte de usuario telefónico. SSCP (Signalling Connection Part) es la parte de conexión de señalización. MTP (Message Transfer Part) es la parte de transferencia de mensajes.

2.3.1. Enlaces de señalización

Los enlaces de señalización SS7 son organizados según su función en la señalización de la red local. Todos los enlaces de señalización son bidireccionales y tienen tasas de transferencia de información de 56 o 64 Kbps. Los enlaces de señalización son interconectados mediante los elementos llamados Signaling Links, cuya tasa de transferencia máxima puede ser de 1,544 MHz. Con el objetivo de obtener mayor ancho de banda y robustez ante errores, el administrador de red puede utilizar más de 16 *links* entre cada par de SP, adicional con esto se consigue balancear cargas de tráfico. A este arreglo de *links* se le conoce como Linkset. Dentro de un linkset, todos los *links* poseen las mismas características.

Los enlaces de señalización están organizados lógicamente por tipos de conectores; los tipos de enlace de señalización pueden ser enlace A, enlace B, enlace C, enlace D, enlace E y enlace F. En la figura 9 se observan las configuraciones de los tipos de enlace.

Figura 10. **Enlace A**

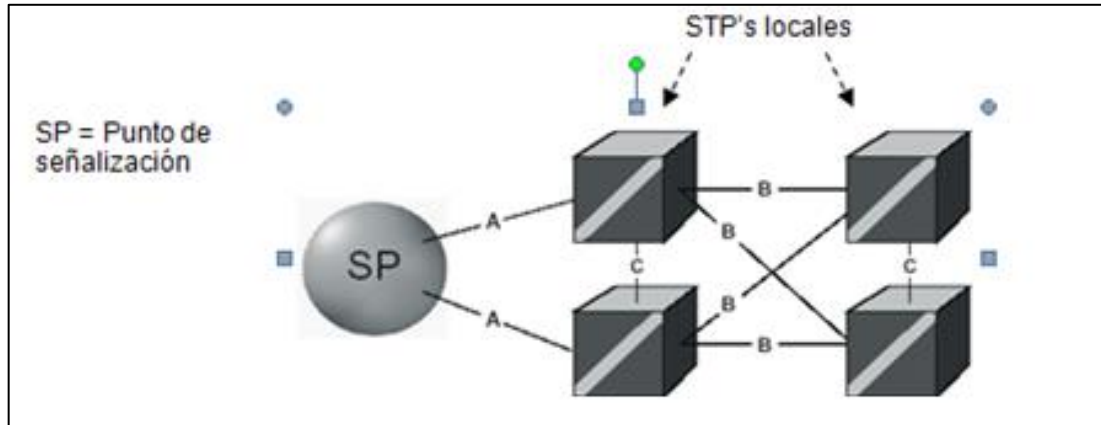


Fuente: *Transmisión y Datos*. <http://www.transmisiondatos-unidad3y4.blogspot.com/2014/03/ss7-y-rdsi.html>. Consulta: julio de 2016.

Un enlace B (Bridge Link) sirve para conectar pares de STP (locales o regionales) que tengan la misma jerarquía, ya sea, o no, que se encuentren en redes diferentes. Se pueden utilizar hasta 8 enlaces para conectar dos pares STP, dentro de una misma red denominada malla STP. En la figura 11 se muestra la estructura de un enlace B.

Un enlace C (Cross Link) tiene como función la conexión de dos STP que se encuentren en la misma red. Normalmente, un enlace C se utiliza para transferir información únicamente si la red está presentando congestión. La imagen 12 muestra la estructura de un enlace C.

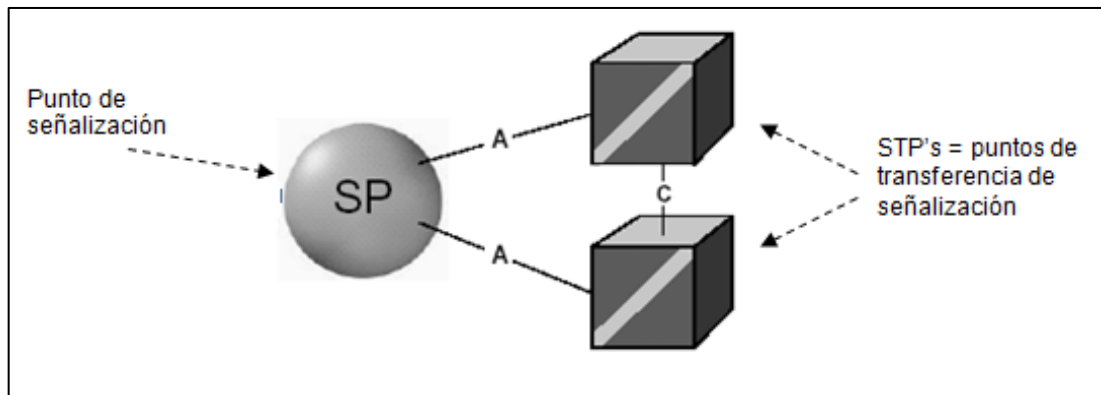
Figura 11. **Enlace B**



Fuente: *TX de Datos*. <http://1.bp.blogspot.com/-yawL7RzkEKw/URLQXx4QqEI/AAAAAAAAABA/AUCaPM6beeY/s1600/enlace+b.png>.

Consulta: julio de 2016.

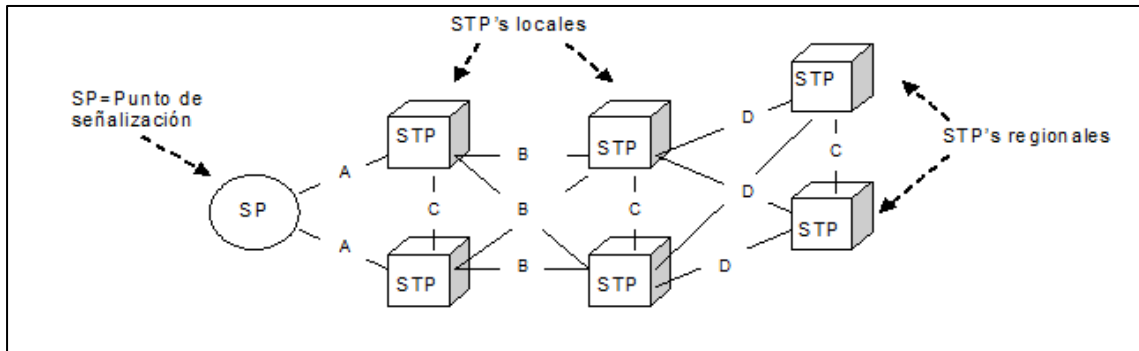
Figura 12. **Enlace C**



Fuente: *TX de Datos*. <http://4.bp.blogspot.com/-ToLW2E2nXZg/URLPuAbF0-/AAAAAAAAA4/zjE3zUYoXIU/s1600/enlaces+a+y+c.png>. Consulta: julio de 2016.

Un enlace D (Diagonal Link) son utilizados para pares de STP los cuales tienen diferentes jerarquías, por ejemplo, un STP regional con un STP local. Los enlaces D no son utilizados comúnmente, a menos que la red de telefonía local cuente con varios niveles de jerarquía. En la figura 13 se muestra la estructura de un enlace D.

Figura 13. **Enlace D**



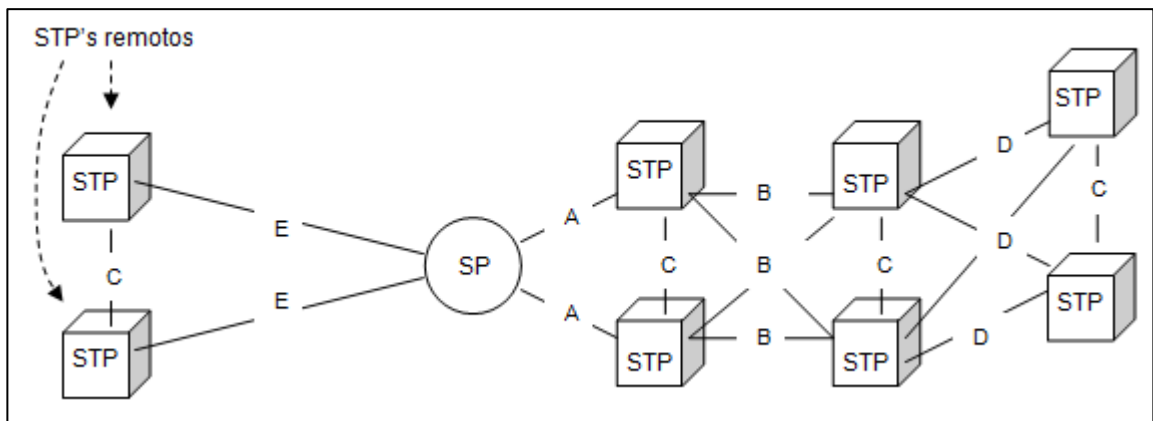
Fuente: *TX de Datos*. http://4.bp.blogspot.com/-8jaKghOiwHk/URLQu1VB7I/AAAAAAAAAABI/w83N-m-G_PQ/s1600/enlac+e.png. Consulta: julio

de 2016.

Un enlace E (Extended Link) se utiliza para conectar un SP con un par STP remoto, que no forma parte del de los STP locales, esto se realiza para mejorar la flexibilidad mediante la extensión de su conexión. En otras palabras, un enlace E puede ser el camino que seguirán los mensajes emitidos por el SP si el par STP local presenta sobrecarga. Para enlazar un SP con un par STP se pueden utilizar hasta 16 enlaces E. Debido a la confiabilidad de este tipo de enlaces, son utilizados para servicios de emergencia. En la figura 14 se observa la estructura de un enlace E.

Un enlace F (Fully Associated Link) se utiliza para enlazar dos SP, que quieren compartir información entre ellos, sin sobrecargar la red local; es decir, enlazan 2 SP sin necesidad de que un STP intervenga. Un enlace F únicamente puede ser configurado en el modo asociado. Un ejemplo de un enlace F es la conexión entre dos *switch* de una misma red. En la figura 15 se observa la estructura de un enlace F.

Figura 14. **Enlace E**

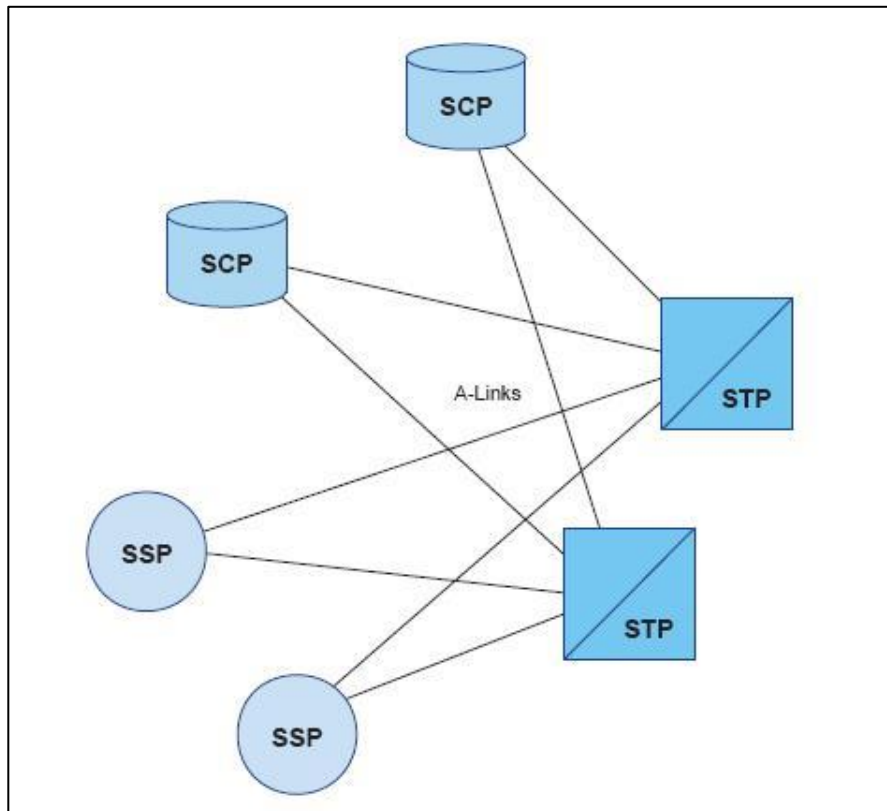


Fuente: *TX de Datos*. [http://4.bp.blogspot.com/-](http://4.bp.blogspot.com/-0IkBly3tTms/URLosv1NT5I/AAAAAAAAABY/mfrCx-1B8fE/s1600/enlac+ee.png)

[0IkBly3tTms/URLosv1NT5I/AAAAAAAAABY/mfrCx-1B8fE/s1600/enlac+ee.png](http://4.bp.blogspot.com/-0IkBly3tTms/URLosv1NT5I/AAAAAAAAABY/mfrCx-1B8fE/s1600/enlac+ee.png).

Consulta: julio de 2016.

Figura 15. **Enlace F**



Fuente: *Learn SS7*. <http://learns7.blogspot.com/2010/04/ss7-links.html>. Consulta: julio de 2016.

2.3.2. Rutas de señalización

En el protocolo SS7, una ruta de señalización se define como la trayectoria que debe tomar un mensaje para llegar a su destino final, partiendo de su origen.

Una ruta de señalización se configura de manera estática en cada SP y STP, esto quiere decir que no se soporta la asignación dinámica de nuevas rutas.

2.3.3. Puntos de señalización

Los puntos de señalización son nodos cuya función principal es servir de puntos de conexión para el establecimiento de rutas, en las cuales pueden pasar paquetes de información. Los puntos de señalización están divididos en SP (Signalling Point), SSP (Service Switching Point), STP (Signal Transfer Point) y SCP (Service Control Point).

2.3.3.1. Signalling Point (SP)

Los SP, son nodos que se utilizan para originar o recibir información de señalización específicamente. Los SP pueden ser adyacentes o no adyacentes. Los SP adyacentes son aquellos que se conectan directamente por medio de un conjunto de enlaces de señalización. Los SP no adyacentes son aquellos que no se conectan directamente por medio de conjunto de enlaces de señalización.

Para realizar el direccionamiento de un nodo SP, es necesario identificarlo mediante un código único, este código único recibe el nombre de Código de Punto o PC (Point Code). Para poder realizar la identificación de un nodo, PC funciona en la capa 3 (MTP). Por tal razón, cada paquete de información contiene la información del PC de origen y del PC de destino. En el caso de mensajes de información en *roaming* se utilizan PC con una longitud de 14 bits.

2.3.3.2. Service Switching Point SSP

Los SSP son nodos finales que pueden ser interconectados entre sí. Los SSP realizan el procesamiento de las llamadas, los SSP pueden generar o recibir mensajes de información relacionados con la gestión de llamadas, los SSP también pueden enviar solicitudes a otros SCP para permitir el

enrutamiento de los mensajes de información. Adicionalmente, los SSP realizan el control de en la banda de voz y de señalización. Un SSP puede fungir como origen o destino de los mensajes de información, pero no puede realizar la función de transferencia, esto implica que, si un mensaje llega a un SSP incorrecto, el mensaje no será reenviado y por lo tanto será eliminado.

La mayoría de las funciones de los SSP son ejecutadas mediante la vinculación de un ordenador a los interruptores existentes. A través del conmutador de voz, el ordenador recibe las señales para activar la comunicación de mensajes de señalización SS7. Los SSP se puede utilizar para una gran cantidad de funciones, tales como servicios de enrutamiento mejoradas, redes privadas virtuales (VPN), portabilidad numérica, filtrado de llamadas, servicio de número personal, tele-voto y de gestión de llamadas por internet. Las ventajas de incorporar SSP a la arquitectura de red son:

- Alta eficiencia de conmutación en la multiplexación por división de tiempo.
- Densidad de empaquetamiento que se combina con una lista de aplicaciones pre configuradas.
- Soporte para interfaces VoIP y TDM que funcionan como un enlace entre dominios. Esto proporciona una transición sencilla entre redes tradicionales y de próxima generación.
- Servicios de red inteligente y funciones de gestión de llamadas, lo que contribuye al uso productivo de los recursos de la red.

2.3.3.3. Signal Transfer Point (STP)

Los STP son nodos SS7 que realizan la transferencia de mensajes de señalización entre los nodos de la red local. Si un SSP es análogo a un *switch*, se puede decir que el STP es el análogo de un *router*; esto quiere decir que un STP es un *router* que transmite mensajes SS7 entre puntos finales (SEP, Signaling End Points) y otros STP. Los SEP están formados por los SSP y los SCP. El STP está conectado a los SEP y STP adyacentes a través de enlaces de señalización.

Basado en el campo de dirección de los mensajes SS7, los STP enrutan los mensajes hacia el enlace de señalización de salida apropiado. Edge STP también puede enrutar los mensajes basado en el contenido del cuerpo del mensaje, para esto utiliza técnicas de inspección profunda de paquetes, adicionalmente puede realizar la traducción de la dirección y verificación del contenido con el fin de limitar la transferencia de mensajes con contenido dudoso o enviados a partir de fuentes no fiables. Para cumplir con los requisitos de fiabilidad, los STP son provisionados en pares.

Los STP se conectan únicamente con enlaces de señalización; esto quiere decir que no tienen usuarios conectados (donde un usuario podría ser una estación móvil, un usuario PSTN o un equipo terminal en el extremo de un canal ISDN B). Los nodos SEP pueden enviar mensajes de señalización a otro SEP, pero los mensajes son enrutados a través de STP adyacentes. Una de las funciones principales de los STP es identificar la mejor ruta para que dos SEP puedan comunicarse.

Normalmente los STP no son el origen o destino para los mensajes transferidos. En algunos casos, los STP pueden originar mensajes, esto con la

finalidad de conocer el estado de la red de señalización, a continuación, se describen algunos de estos casos:

- Un STP envía un mensaje para conocer la disponibilidad de una ruta establecida con anterioridad.
- Un STP puede enviar un mensaje MTP de bajo nivel, a un nodo de señalización adyacente para comprobar la tasa de error en un enlace de señalización en particular.
- Un STP puede enviar un mensaje a otros STP adyacentes para comunicarles que se encuentra fuera de servicio, en este caso los STP adyacentes evitarán usar rutas que incluyan el STP fuera de servicio.

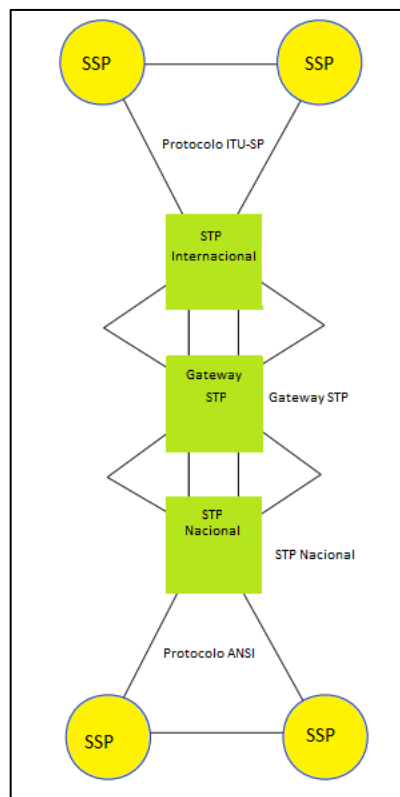
Los STP dependiendo de la configuración del administrador de la red, pueden ser integrados o independientes. Un STP integrado combina la funcionalidad de dos nodos, los cuales son los SSP y los STP. Ellos pueden ser tanto origen como destino del tráfico MTP. Adicional, un STP integrado también puede ser utilizado para transferir mensajes a otros nodos.

Los STP independientes son aquellos que se utilizan para garantizar la disponibilidad de la red, esto se realiza mediante la implementación de STP pares. Los pares STP independientes realizan un balanceo de tráfico, en caso que uno de los dos STP falle, el otro asume la totalidad del tráfico. Los STP independientes se encuentran divididos por su utilización geográfica. En el primer nivel se encuentran los STP internacionales, en el segundo nivel se encuentran los STP nacionales y en el tercer nivel se encuentran los llamados Gateway STP. En la figura 16 se observa la jerarquía de los STP.

Los STP internacionales funcionan dentro de una red internacional. Se utilizan para proporcionar una interconexión SS7 a todos los países que soporten el protocolo ITU-TS.

Los STP nacionales funcionan dentro de una red nacional. Pueden transferir mensajes que utilizan el mismo estándar nacional. Los mensajes pueden ser transferidos a un STP internacional, pero no pueden ser convertidos por el STP nacional. Los protocolos de conversión, a menudo se utilizan para interconectar STP nacionales con STP internacionales, mediante la conversión de ANSI a ITU-TS.

Figura 16. **Jerarquía STP**



Fuente: elaboración propia.

Un Gateway STP convierte los mensajes de señalización de un protocolo a otro. Este tipo de STP son utilizados, a menudo, como punto de acceso a una red internacional. Dependiendo de su ubicación los Gateway STP deben ser capaces de soportar los protocolos nacionales o internacionales. Los Gateway STP también cumplen con las funciones de ser utilizados como una interfaz dentro de bases de datos de otras redes, y proporcionar mediciones de tráfico y utilización del nodo. Adicionalmente, realizan las funciones de medir la cantidad de mensajes que entran y salen de la red, búsqueda de eventos como enlaces fuera de servicio.

2.3.3.4. Service Control Point (SCP)

Un SCP es una base de datos la cual recibe mensajes de solicitud de información de la red SS7 y devuelve la información necesaria para la realización de llamadas o ejecución de servicios. Un SCP generalmente recibe solicitudes de un SSP a través de los STP que determinan que se información adicional es necesaria para la ejecución del servicio.

Los SCP también puede comunicarse con un periférico inteligente para reproducir mensajes de voz, o solicitar información al usuario. Esto se realiza mediante la implementación de códigos de funciones. Se realiza mediante la utilización de la INAP, la cual se encuentra por encima de TCAP en la pila de protocolos SS7. Normalmente los SCP se encuentran conectados con STP, en otros casos menos frecuentes con SSP. Esto dependerá de la arquitectura de la red y las necesidades del administrador de red.

3. SERVIDORES FTP Y SSH

Una red de telecomunicaciones basa su funcionamiento en equipos y servidores, los cuales, en conjunto, hacen posible que los usuarios puedan utilizar los diversos servicios que ofrece la red de telefonía local. Los servidores realizan funciones de administración, ejecución y finalización de tareas establecidas, dichas tareas son agregadas, modificadas o removidas, mediante una serie de instrucciones introducidas mediante una terminal de ejecución. Existen diversos sistemas operativos que pueden ser instalados en los servidores, pero para el presente trabajo de graduación se hará énfasis en servidores que ejecuten el sistema operativo Linux o Unix.

3.1. Sistema operativo Linux

Linux es un sistema operativo desarrollado bajo el modelo Free and Open-Source Software. Linux fue desarrollado originalmente como un sistema operativo libre para ordenadores personales basados en la arquitectura Intel x86, pero debido a su alta eficiencia y su creciente popularidad, se ha convertido en el sistema operativo con mayor número de adaptaciones a diferentes plataformas de hardware (por ejemplo, el núcleo de Linux, es utilizado para el desarrollo del sistema operativo Android). Linux es el sistema operativo más utilizado para servidores, ordenadores centrales y prácticamente todos los superordenadores. Linux también puede ser ejecutado en sistemas integrados, que son dispositivos cuyo sistema operativo normalmente está integrado en el *firmware* y este se encuentra altamente adaptado al sistema.

El desarrollo de Linux es uno de los ejemplos más destacados de la colaboración de software libre y de código abierto. El código fuente subyacente puede ser utilizado, modificado y distribuido, para fines no comerciales y comerciales, por cualquier persona bajo los términos de sus respectivas licencias.

Linux, ha sido utilizado como sistema operativo para una gran cantidad y variedad de servidores, y cada vez cobra más popularidad en este campo. En 2006, Netcraft informó que ocho de las diez empresas de alojamiento de archivos más confiables utilizan servidores con sistemas operativos Linux.

Linux utiliza un núcleo monolítico, el núcleo de Linux, que maneja el control de procesos, la creación de redes, el acceso a los periféricos y sistemas de archivos. Los controladores de dispositivos pueden integrarse directamente con el *kernel*, o añadirse como módulos independientes, una vez el sistema operativo ya se encuentre instalado. GNU es una de las partes más importantes de la mayoría de los sistemas Linux, que proporciona la aplicación más común de la biblioteca C, la terminal Shell, la cual es una terminal para la ejecución de instrucciones.

Linux soporta docenas de lenguajes de programación. Las herramientas de desarrollo originales utilizadas para la construcción de aplicaciones Linux y los programas del sistema operativo, se encuentran dentro de la cadena de herramientas GNU, que incluye la colección de compiladores de GNU (GCC, GNU Compiler Collection) y el sistema de compilación GNU. Muchos lenguajes de programación tienen una implementación de referencia multiplataforma que soporta Linux, por ejemplo, PHP, Perl, Ruby, Python, Java, Go, Rust y Haskell.

Una característica común de todas las distribuciones Linux, es que incluyen los lenguajes tradicionales de programación de propósito específico dirigidos a secuencias de comandos, el procesamiento de textos, la configuración del sistema y la administración del sistema. El presente trabajo de graduación nos enfocaremos en los lenguajes Shell Scripting, AWK y Perl. Entre las características más importantes de los sistemas operativos basados en Linux, se encuentran:

- Varios usuarios pueden ejecutar tareas de manera simultánea en el mismo servidor.
- Ejecución simultánea de más de una tarea, proceso, rutina o instrucción del administrador.
- Capacidad para soportar CPU Intel y otro gran número de CPU distintas.
- Altamente seguro, debido a que soporta la función de modo seguro.
- Alta confiabilidad ante errores de congestión de memoria, esto se logra mediante las rutinas de protección de memoria entre ejecución de procesos, con esto se consigue que, si un proceso falla, no afectará la disponibilidad del sistema.
- Ahorro en la utilización de recursos, ya que Linux solo lee del disco las partes de un programa que se encuentre en ejecución.
- Recursos compartidos, esto significa que varios procesos pueden usar la misma zona de memoria para ejecutarse.
- Paginación de memoria virtual sin intercambio de procesos completos.
- Gestión unificada de los recursos de memoria.
- Soporte para librerías de carga dinámica y carga estática.

En cuanto a temas de seguridad, los sistemas operativos más recientes, basados en Linux soportan algoritmos de codificación más potentes como MD5 o SHA. Estos algoritmos son más robustos que sus antecesores y permiten

claves más extensas. El algoritmo MD5 utiliza claves de 128 bits, mientras que SHA512 utiliza claves de 512 bits de longitud. Debido a que Linux, es un sistema operativo multiusuario y multitarea, necesita una gran cantidad de memoria física para poder ejecutar todos los procesos configurados. Los espacios de paginación son particiones de disco que permiten ampliar virtualmente la memoria del sistema, guardando el estado de los procesos que en un determinado momento están a la espera de ser ejecutados, si la memoria física está agotada.

Para los administradores de servidores Linux es importante, a la hora de elegir el tamaño de la memoria de paginación, tomar en cuenta factores como la capacidad de memoria y de disco del sistema, la cantidad prevista de procesos, la cantidad de servicios activos en el sistema y la cantidad estimada de clientes/servidores.

3.1.1. Shell Scripting

El protocolo Shell Scripting, es utilizado para la creación de rutinas o procesos, los cuales serán ejecutados por el servidor de manera manual o automática, a estas rutinas o procesos se les conoce con el nombre de Shell Script.

Un Shell Script, es un archivo de texto ASCII almacenado con la extensión .sh; dentro de un Shell Script se describen los comandos a ser ejecutados por el servidor. Para crear un Shell Script, se debe ejecutar una terminal Shell; una terminal Shell es un intérprete de comandos, que puede ser ejecutada bajo permisos de usuario normal o de superusuario.

Dentro de las funciones más comunes de un Shell Script se encuentran la creación, modificación y administración de archivos, ejecución de programas e impresión de texto en pantalla. Adicionalmente, un Shell Script proporciona una variedad de comandos para la ejecución de funciones específicas, las cuales dependen del sistema operativo, especificaciones técnicas del servidor y configuraciones de red.

Dentro de un Shell Script, se incluyen instrucciones y variables. Las variables son herramientas del sistema que se utilizan para almacenar valores numéricos o cadenas de caracteres. Las variables pueden ser locales o globales, las locales son declaradas dentro de subrutinas, las variables globales son aquellas que se declaran en el principio del programa. Las instrucciones son comandos los cuales son utilizados para ejecutar funciones específicas. Dentro de los comandos que se utilizarán para el desarrollo del Script, que será utilizado en el presente trabajo de graduación, se encuentran sh, cat, echo, rm, grep, more, if.

El comando sh se utilizará para ejecutar archivos con extensión .sh; la sintaxis de este comando es sh <archivo.sh>.

El comando cat se utilizará para concatenar un archivo para posteriormente desplegarlo en la terminal. La instrucción cat, admite varios archivos, los cuales se desplegarán en el orden que fueron ingresados. La sintaxis de este comando es cat <archivo.txt>.

El comando echo se utilizará para desplegar un texto en pantalla, el cual luego será almacenado en un archivo de texto. El texto es ingresado por el usuario. El comando echo es capaz de interpretar varias opciones, las cuales deben ser ingresadas entre comillas dobles y deberá utilizar el indicador -e.

Entre las opciones que se utilizarán se tienen \a, \b, \c, \n, \r, \t; \a emite un sonido de alerta, \b borra un carácter, \c suprime toda la salida posterior al indicador, \n se cambia a una nueva línea, \ r retrocede el indicador; \t ingresa una tabulación. La sintaxis de este comando es echo -e "Hola mundo \n".

El comando rm se utilizará para borrar archivos, los cuales son utilizados de manera temporal, y serán borrados para ahorrar espacio de memoria. La sintaxis de este comando es rm <archivo.txt>.

El comando grep, se utilizará para realizar búsqueda en un archivo de texto, de una cadena de caracteres de texto. El comando grep imprime, por defecto, las líneas encontradas en la salida estándar. El comando grep se utiliza en conjunto con el comando cat. La sintaxis para realizar esta búsqueda es cat <archivo> | grep "Hola".

El comando more, se utiliza para visualizar archivos de texto. Para archivos de texto de gran tamaño, serán mostrados por partes parciales. La sintaxis de este comando es more <archivo>.

El comando if, es un comando condicional. Esto quiere decir que el comando if, evalúa una condición, si la condición es verdadera ejecuta una opción; si la condición es falsa, el comando if puede, o no, ejecutar una opción. La estructura de este comando es la siguiente:

```
If <condición>  
then  
<instrucción>  
else  
<instrucción>.
```

El comando `cd` se utilizará para moverse entre directorios. La sintaxis de este comando es `cd </ruta>`. El comando `pwd` se utiliza para imprimir la ruta actual. El comando `ls` se utiliza para listar los archivos que se encuentran dentro del directorio actual. El comando `chmod` se utiliza para asignar permisos especiales a un archivo determinado prevista de procesos, la cantidad de servicios activos en el sistema y la cantidad estimada de clientes/servidores.

3.1.2. Perl Scripting

Perl, es un lenguaje de programación el cual se basa en el lenguaje C. Adicionalmente, Perl también es considerado un Shell Interpreter. Perl pertenece a la familia de lenguajes alto nivel, de propósito general, interpretados y dinámicos. Perl es de naturaleza procesal, con variables, expresiones, instrucciones, bloques delimitados por llaves, estructuras de control y subrutinas. Perl también tiene características de programación de lenguaje Shell. Todas las variables están marcadas con un signo al principio. Sin embargo, a diferencia de Shell, Perl utiliza *sigils* para todos los accesos a las variables.

Perl también soporta una diversidad de funciones integradas que proporcionan herramientas de uso frecuente en la programación de Shell como la clasificación y comunicación con el Sistema Operativo. Perl toma las listas de *Lisp*, *hash* y expresiones regulares. Estos simplifican y facilitan la manipulación de texto y las tareas de gestión de datos. Esto significa que todas las declaraciones tienen un valor, y por lo tanto también son expresiones y se pueden utilizar como expresiones más grandes.

La versión 5 de Perl añade características que apoyan a las estructuras de datos, funciones de primera clase y un modelo de programación orientado a

objetos. Una característica importante, introducida en Perl 5 fue la capacidad de empaquetar el código como módulos reutilizables. Todas las versiones de Perl realizan de forma automática la función Data Typing y la gestión automática de memoria. Perl conoce el tipo y las necesidades de cada objeto de datos en el programa; reserva y libera el espacio a medida que sea necesario. En cuanto a los comandos utilizados por Perl, son los mismo que se utilizan en Shell Scripting, esto debido a sus características en común.

3.2. Protocolo FTP

El protocolo FTP (File Transfer Protocol) es un protocolo de red estándar que se utiliza para transferir archivos informáticos entre un cliente y un servidor. FTP está basado en la arquitectura cliente-servidor y utiliza conexiones de control y de datos separadas entre el cliente y el servidor. Los usuarios de FTP pueden autenticarse con un texto claro de sesión de protocolo, normalmente en forma de un nombre de usuario y contraseña, pero puede conectarse de forma anónima si el servidor está configurado para permitirlo. Para realizar una conexión segura, es decir envío de datos de usuario cifrados, normalmente FTP utiliza SSL / TLS. Las primeras aplicaciones de cliente FTP eran programas de línea de comandos desarrollados antes de los sistemas operativos gráficos. Desde entonces se han desarrollado muchos clientes FTP y utilidades de automatización para equipos, servidores, dispositivos móviles y hardware.

FTP puede ser configurado para funcionar en dos modos, el modo pasivo y el modo activo, estos modos determinan la forma en la cual será establecida la conexión para la transferencia de datos. En el modo activo y pasivo, el cliente crea, de manera aleatoria, una conexión de control TCP por medio de un usuario normal, es decir, sin privilegios de súper usuario.

En el modo activo, el cliente recibe las peticiones de conexiones de datos entrantes desde el servidor en el puerto M. Se envía el comando FTP PORT M para informar al servidor en el que el puerto está escuchando. El servidor inicia entonces un canal de datos al cliente de su puerto 20, el puerto de datos de servidor FTP.

El modo pasivo se utiliza cuando el cliente está detrás de un cortafuegos y no puede aceptar conexiones TCP entrantes. En este modo, el cliente utiliza la conexión de control para enviar un comando PASV al servidor y entonces recibe un número de la dirección IP del servidor y el puerto del servidor, entonces el cliente inicia una conexión de datos desde un puerto de cliente a la dirección IP del servidor y el puerto del servidor número recibido.

Una vez establecida la conexión, se puede iniciar con la transferencia de datos. FTP puede utilizar 4 representaciones para la transferencia de datos, las cuales son:

- Modo ASCII. Este modo es utilizado para texto.
- Modo Imagen. A este modo normalmente se le conoce como Binary Mode. En este modo el transmisor envía la información byte por byte, mientras que el receptor almacena la ráfaga de bytes y luego las reconstruye.
- Modo EBCDIC. Este modo se utiliza para la transferencia de texto plano.
- Modo Local. Este modo permite que dos equipos con configuraciones idénticas puedan enviar datos en un formato propietario y sin necesidad de convertirlo en ASCII.

3.3. Protocolo SSH

El protocolo SSH (Secure Shell) es un protocolo de red cifrada para la ejecución segura de tareas o rutinas sobre una red no segura. SSH proporciona un canal seguro a través de una red no segura, basado en una arquitectura cliente-servidor, es decir, la conexión de una aplicación cliente SSH con un servidor SSH. Las aplicaciones más comunes incluyen el acceso remoto por línea de comandos y la ejecución remota de comandos, pero cualquier servicio de red se puede asegurar con SSH. La especificación del protocolo distingue entre dos versiones principales, conocidos como SSH-1 y SSH-2. SSH fue diseñado como un reemplazo para Telnet y para los protocolos de Shell remotos no seguros, los cuales envían la información importante (como contraseñas) en texto plano, haciéndolas vulnerables a interceptación y divulgación mediante el análisis de paquetes. El cifrado utilizado por SSH está destinado a proporcionar confidencialidad e integridad a los datos a través de una red no segura, tales como internet.

SSH se utiliza normalmente para iniciar sesión en una máquina remota y ejecutar comandos, pero también es compatible con un túnel, reenvío de puertos TCP y conexiones X11; Se pueden transferir archivos mediante la transferencia asociada de archivos SSH (SFTP) o protocolos copia segura (SCP). Para realizar esto, SSH tiene determinado el puerto 22.

Un programa cliente SSH es utilizado, normalmente para el establecimiento de conexiones remotas con un servidor SSH. Este protocolo que puede utilizar para muchas aplicaciones a través de muchas plataformas, Algunas de las aplicaciones más adelante pueden requerir características que solo están disponibles o son compatibles con los clientes o servidores SSH

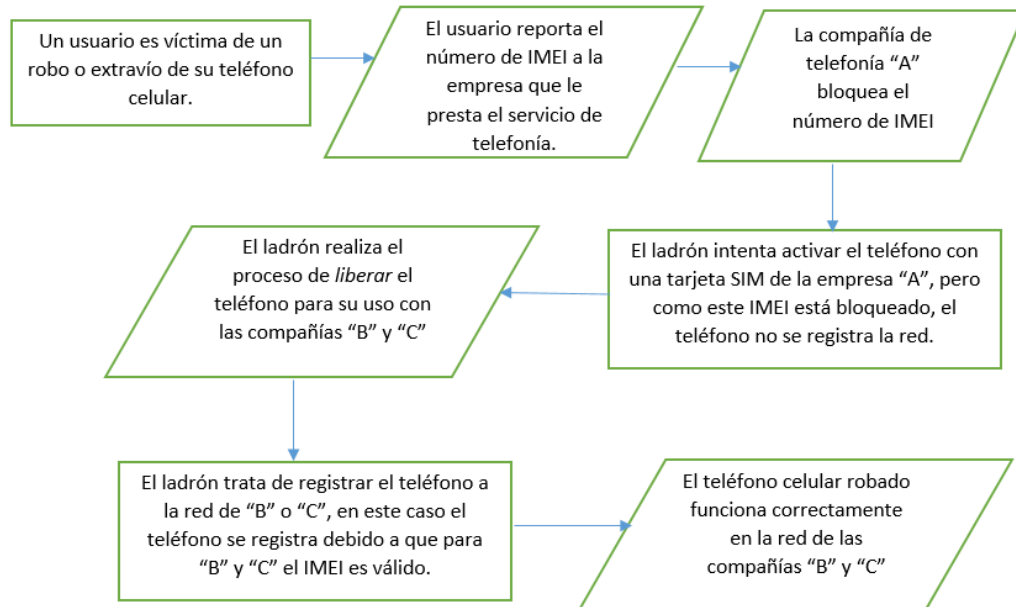
específicos. Por ejemplo, utilizando el protocolo SSH es posible implementar una VPN.

4. PROPUESTA DE UN SISTEMA SSH/FTP PARA EL REPORTE AUTOMÁTICO DE UN IMEI REPORTADO COMO ROBADO O EXTRAVIADO

Cuando un usuario de telefonía celular es víctima del robo o extravío de su teléfono móvil, tiene la posibilidad de reportar el robo o extravío a su compañía de telefonía; con el reporte de IMEI se logra bloquear el teléfono móvil con la compañía de telefonía que le presta el servicio al usuario. Pero, si el teléfono móvil es “liberado” para su uso con las otras compañías, el teléfono funcionará correctamente. Por esta razón, se debe realizar un bloqueo total del IMEI (es decir, un bloqueo de IMEI en las 3 compañías de telefonía celular: Claro, Tigo y Movistar). Para ello, se debe implementar un proceso de bloqueo con las 3 compañías de telefonía celular existentes en Guatemala. La figura 17 muestra proceso de bloqueo que se tiene actualmente en Guatemala, el cual no es un proceso de bloqueo total.

Para realizar el proceso automático de bloqueo con las tres compañías de telefonía móvil existentes en Guatemala es necesaria la utilización de Shell Script, Perl Script, Crontrab y un servidor Linux. Los Scripts y archivos necesarios para el reporte automático son los siguientes:

Figura 17. **Proceso de bloqueo por IMEI actual**



Fuente: elaboración propia.

- Shell Script principal. Este script es el encargado de ejecutar todos los demás scripts secundarios. Este script será el único que se declarará para su ejecución automática en el servidor Linux por medio de un Crontab.
- Shell Script Tigo. Este script es el encargado de verificar si al servidor principal han ingresado reportes sobre nuevos IMEI reportados como robados o extraviados, por la empresa Tigo.
- Shell Script Claro. Este script es el encargado de verificar si al servidor principal han ingresado reportes sobre nuevos IMEI reportados como robados o extraviados, por la empresa Claro.
- Shell Script Movistar. Este script es el encargado de verificar si al servidor principal han ingresado reportes sobre nuevos IMEI reportados como robados o extraviados, por la empresa Movistar.

- Shell Script de borrado. Este script es el encargado de borrar periódicamente los archivos para el reporte temporal de los IMEI.
- Perl Script Tigo. Este script es el encargado de enviar las notificaciones de los nuevos IMEI bloqueados a las Claro y Movistar.
- Perl Script Claro. Este script es el encargado de enviar las notificaciones de los nuevos IMEI bloqueados a las Tigo y Movistar.
- Perl Script Movistar. Este script es el encargado de enviar las notificaciones de los nuevos IMEI bloqueados a las Claro y Tigo.
- Tigo.txt; es el archivo donde se almacenan los IMEI reportados por Tigo.
- Claro.txt; es el archivo donde se almacenan los IMEI reportados por Claro.
- Movistar.txt; es el archivo donde se almacenan los IMEI reportados por Movistar.

4.1. Creación de Shell Scripts

Primeramente, se creará el Script principal, el cual recibirá el nombre Principal.sh; el código de programación es el siguiente:

```
#!/ bin/sh
sh Script_Tigo.sh
sh Script_Claro.sh
sh Script_Movistar.sh
sh Script_Borrado.sh
```

Seguidamente se procederá a crear los Scripts que se encargan de verificar los archivos de texto de las 3 compañías de telefónica celular. Si este Script detecta un nuevo IMEI, entonces proceder a ejecutar el Perl Script de Tigo. El código para el Script_Tigo.sh es el siguiente:


```
#!/bin/sh
$contador_Tigo == 0
cat Tigo.txt | wc -l >> $contador_Tigo
if [$contador_Tigo != 0] then
pl Perl_Tigo.pl
end if
```

El código para el archivo Script_Claro.sh es el siguiente:

```
#!/bin/sh
$contador_Claro == 0
cat Tigo.txt | wc -l >> $contador_Claro
if [$contador_Claro != 0] then
pl Perl_Claro.pl
end if
```

El código para el archivo Script_Movistar.sh es el siguiente:

```
#!/bin/sh
$contador_Movistar == 0
cat Movistar.txt | wc -l >> $contador_Movistar
if [$contador_Movistar != 0] then
pl Perl_Movistar.pl
end if
```

El código para el archivo Script_Borrado.sh es el siguiente:

```
#!/bin/sh
cat /dev/null >> Tigo.txt
```

```
cat /dev/null >> Claro.txt
cat /dev/null >> Movistar.txt
```

4.2. Creación de Perl Scripts

Los Perl Scripts son utilizados para la creación de los scripts que se encargaran de enviar las notificaciones automáticamente. Se creará un script para que una de las tres compañías de telefonía. El código para el archivo Perl_Tigo.pl es el siguiente:

```
#!/bin/sh
use lib('lib');
use MIME::Lite;
use Net::SMTP;
my $date = $ARGV[0];
my $from_address = 'IMEI_Tigo@gmail.com';
my $to_address = 'IMEI_Claro@gmail.com', 'IMEI_Movistar@gmail.com';
my $mail_host = '172.16.0.1';
my $subject = "Nuevo IMEI reportado por Tigo";
my $message_body = "La compañía telefónica Tigo, reporta nuevo(s)
numero(s) de IMEI reportado(s) como robados(s) y/o extraviado(s). Se adjunta
el archivo Tigo.txt para su pronta validacion".
my $my_file_xls = '/home/Tigo.txt ';
$msg = MIME::Lite->new (
    From => $from_address,
    To => $to_address,
    Subject => $subject,
    Type =>'multipart/mixed'
MIME::Lite->send('smtp', $mail_host, Timeout=>60);
```

```
$msg->send;
```

El código para el archivo Perl_Claro.pl es el siguiente:

```
#!/bin/sh
use lib('lib');
use MIME::Lite;
use Net::SMTP;
my $date = $ARGV[0];
my $from_address = 'IMEI_Claro@gmail.com';
my $to_address = 'IMEI_Tigo@gmail.com', 'IMEI_Movistar@gmail.com';
my $mail_host = '172.16.0.1';
my $subject = "Nuevo IMEI reportado por Claro";
my $message_body = "La compañía telefónica Claro, reporta nuevo(s)
numero(s) de IMEI reportado(s) como robados(s) y/o extraviado(s). Se adjunta
el archivo Tigo.txt para su pronta validacion".
my $my_file_xls = '/home/Claro.txt ';
$msg = MIME::Lite->new (
    From => $from_address,
    To => $to_address,
    Subject => $subject,
    Type => 'multipart/mixed'
);
MIME::Lite->send('smtp', $mail_host, Timeout=>60);
$msg->send;
```

El código para el archivo Perl_Movistar.pl es el siguiente:

```
#!/bin/sh
use lib('lib');
```

```

use MIME::Lite;
use Net::SMTP;
my $date = $ARGV[0];
my $from_address = 'IMEI_Movistar@gmail.com';
my $to_address = 'IMEI_Tigo@gmail.com', 'IMEI_Claro@gmail.com';
my $mail_host = '172.16.0.1';
my $subject = "Nuevo IMEI reportado por Movistar";
my $message_body = "La compañía telefónica Movistar, reporta nuevo(s)
numero(s) de IMEI reportado(s) como robados(s) y/o extraviado(s). Se adjunta
el archivo Tigo.txt para su pronta validacion".
my $my_file_xls = '/home/Claro.txt ';
$msg = MIME::Lite->new (
    From => $from_address,
    To => $to_address,
    Subject => $subject,
    Type =>'multipart/mixed'
MIME::Lite->send('smtp', $mail_host, Timeout=>60);
$msg->send;

```

4.3. Creación rutinas automáticas

Los sistemas operativos basados en Linux, proporcionan la funcionalidad de programar rutinas que ejecutan automáticamente una o más tareas. Esta funcionalidad recibe el nombre de Cron, la cual es básicamente un administrador de procesos que se ejecuta en segundo plano. Para especificar la hora y días para la ejecución en segundo plano de una rutina, se utiliza un archivo de texto llamado Crontab. Este archivo contiene un formato específico en el cual se ingresa el minuto, la hora, el día de la semana, el día del mes y el mes en el cual debe ser ejecutada la tarea; si se desea especificar todos los

valores posibles, se puede usar el signo *. En la figura 18 se muestra el formato del archivo Crontab.

Figura 18. **Formato Crontab**

```
.----- minuto (0-59)
| .----- hora (0-23)
| | .----- día del mes (1-31)
| | | .----- mes (1-12) o jan,feb,mar,apr,may,jun,jul... (meses en inglés)
| | | | .--- día de la semana (0-6) (domingo=0 ó 7) o sun,mon,tue,wed,thu,fri,sat (días en inglés)
| | | | |
| * * * * * comando a ejecutar
```

Fuente: *Aprendiendo Lixux*. <http://LearnLinux/rutinas/Cron%Crontab.html>.

Consulta: julio de 2016.

El código utilizado para la creación de la rutina es el siguiente:

```
00 00 * * * sh /home/Principal.sh
00 01 * * * sh /home/Principal.sh
00 02 * * * sh /home/Principal.sh
00 03 * * * sh /home/Principal.sh
00 04 * * * sh /home/Principal.sh
00 05 * * * sh /home/Principal.sh
00 06 * * * sh /home/Principal.sh
00 07 * * * sh /home/Principal.sh
00 08 * * * sh /home/Principal.sh
00 09 * * * sh /home/Principal.sh
00 10 * * * sh /home/Principal.sh
00 11 * * * sh /home/Principal.sh
00 12 * * * sh /home/Principal.sh
00 13 * * * sh /home/Principal.sh
```

```
00 14 * * * sh /home/Principal.sh
00 15 * * * sh /home/Principal.sh
00 16 * * * sh /home/Principal.sh
00 17 * * * sh /home/Principal.sh
00 18 * * * sh /home/Principal.sh
00 19 * * * sh /home/Principal.sh
00 20 * * * sh /home/Principal.sh
00 21 * * * sh /home/Principal.sh
00 22 * * * sh /home/Principal.sh
00 23 * * * sh /home/Principal.sh
```

4.4. Diagrama final del proceso

Una vez finalizada la creación de todos los scripts, ya estará lista la rutina de verificación automática de IMEI reportados como robados. El proceso para la notificación y bloqueo de un número de IMEI de la compañía Claro, es el siguiente:

- Un usuario de la compañía telefónica Claro es víctima del robo de su teléfono celular.
- El usuario reporta el número de IMEI de su teléfono celular a la compañía Claro.
- Claro, ingresa el número de IMEI a la lista negra de su EIR. Al mismo tiempo ingresa el número de IMEI a un archivo de texto llamado Claro.txt.
- A la siguiente hora en punto (por ejemplo 15:00) el servidor principal ejecutará el script Principal.sh; este script, ejecutará el Script_Claro, el cual verificará si el archivo Claro.txt está vacío o no. En el caso que este vacío no ejecutará ninguna acción. En caso que el archivo contenga un número de IMEI, procederá a ejecutar los Scripts Perl_Tigo.pl y

Perl_Movistar.pl; estos dos scripts procederán a notificar a Tigo y Movistar sobre el número IMEI que debe ser bloqueado.

El proceso para la notificación y bloqueo de un número de IMEI de la compañía Tigo, es el siguiente:

- Un usuario de la compañía telefónica Tigo es víctima del robo de su teléfono celular.
- El usuario reporta el número de IMEI de su teléfono celular a la compañía Tigo.
- Tigo, ingresa el número de IMEI a la lista negra de su EIR. Al mismo tiempo ingresa el número de IMEI a un archivo de texto llamado Tigo.txt.
- A la siguiente hora en punto (por ejemplo 16:00) el servidor principal ejecutará el script Principial.sh; este script, ejecutará el Script_Tigo, el cual verificará si el archivo Tigo.txt está vacío o no. En el caso que este vacío no ejecutará ninguna acción. En caso que el archivo contenga un número de IMEI, procederá a ejecutar los Scripts Perl_Claro.pl y Perl_Movistar.pl; estos dos *scripts* procederán a notificar a Claro y Movistar sobre el número IMEI que debe ser bloqueado.

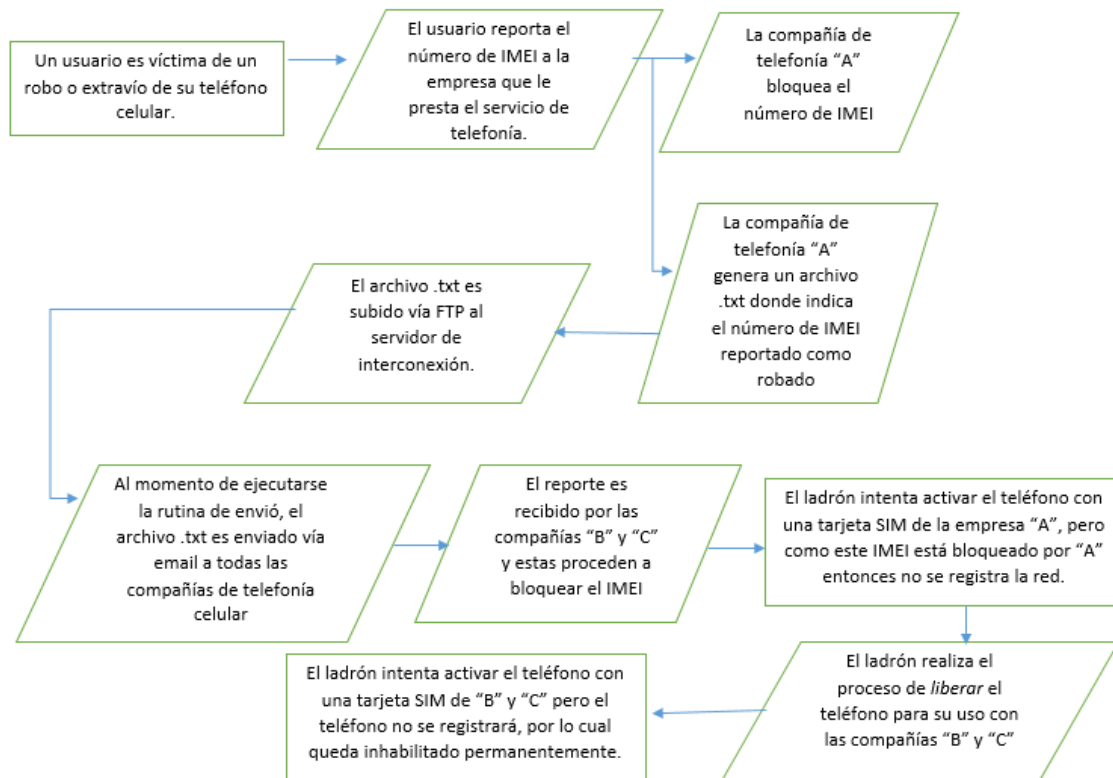
El proceso para la notificación y bloqueo de un número de IMEI de la compañía Movistar, es el siguiente:

- Un usuario de la compañía telefónica Movistar es víctima del robo de su teléfono celular.
- El usuario reporta el número de IMEI de su teléfono celular a la compañía Movistar.

- Movistar, ingresa el número de IMEI a la lista negra de su EIR. Al mismo tiempo ingresa el número de IMEI a un archivo de texto llamado Movistar.txt.
- A la siguiente hora en punto (por ejemplo 17:00) el servidor principal ejecutará el script Principal.sh; este script, ejecutará el Script_Movistar, el cual verificará si el archivo Movistar.txt está vacío o no. En el caso que esté vacío no ejecutará ninguna acción. En caso que el archivo contenga un número de IMEI, procederá a ejecutar los scripts Perl_Claro.pl y Perl_Tigo.pl; estos dos Scripts procederán a notificar a Claro y Tigo sobre el número IMEI que debe ser bloqueado.

De acuerdo con los 3 procesos anteriores, el diagrama general final para el proceso de reporte y bloqueo es el siguiente:

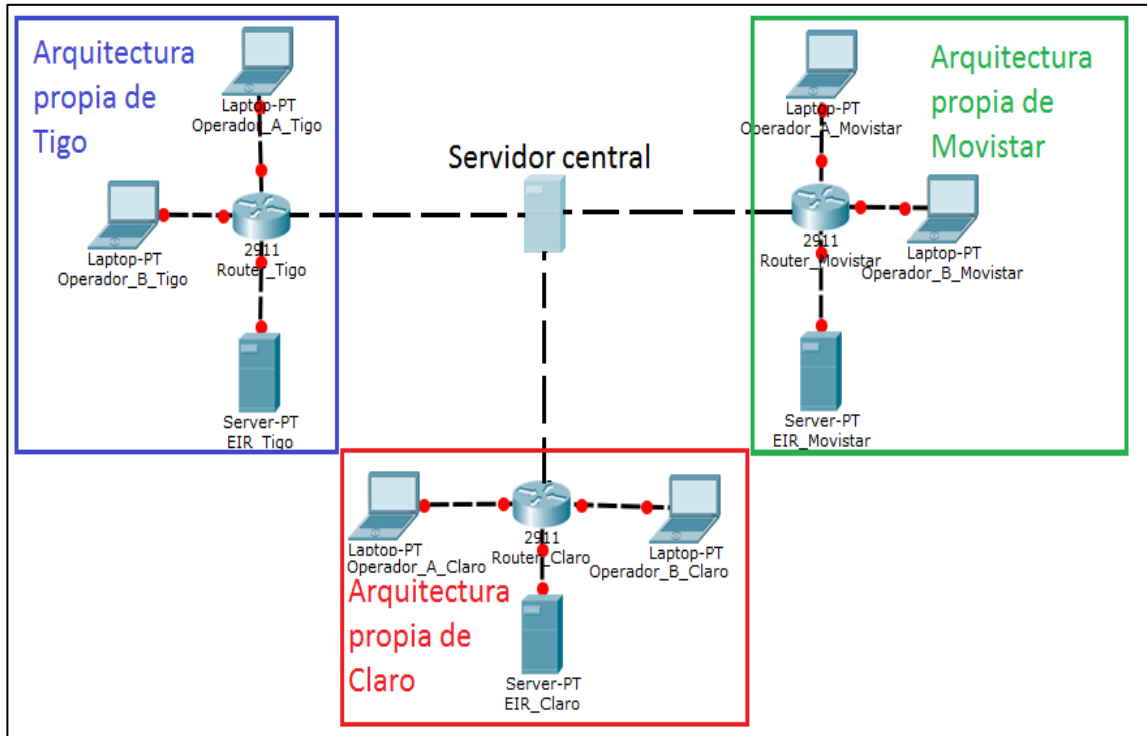
Figura 19. Proceso final del reporte y posterior bloqueo por IMEI



Fuente: elaboración propia.

La arquitectura final del sistema de reporte y posterior bloqueo por IMEI, se muestra en la figura 20. Se observa que cada compañía de telefonía cuenta con su propio EIR y una estación (o más) de computadoras las cuales pueden administrar el ingreso de los IMEI. Adicional, se observa que todo se interconecta con un servidor central, este servidor será el encargado de ejecutar todas las rutinas automáticas.

Figura 20. **Arquitectura final**



Fuente: elaboración propia.

Como se observa en la figura, se respeta la arquitectura interna propia de cada Operadora, es decir, la conectividad entre los operadores/administradores y el EIR. El servidor central se interconectará a la arquitectura propia de cada Operador, pero con la ventana que ninguna de las 3 compañías de telefonía tendrá conocimiento de la arquitectura de las otras 2, es decir, Tigo no conocerá a Claro, Claro no conocerá a Movistar y Movistar no conocerá a Tigo. Viendo la anterior arquitectura, se puede realizar un análisis de los costos de implementación necesarios. Dichos costos de implementación se detallan en la tabla VI.

Tabla VI. **Costos de implementación del sistema**

DISPOSITIVO	CANTIDAD	DESCRIPCIÓN	COSTO UNITARIO	COSTO FINAL
HP ProLiant Micro Server Gen8	1	Servidor HP el cual cumplirá con la función de servidor principal	Q5 400,00	Q5 400,00
Navepoint 9U Deluxe	1	<i>Rack</i> para el servidor HP	Q1 100,00	Q1 100,00
FSP Group 700W ATX	2	<i>Power Supply</i> . Uno activo y uno en <i>Stand-by</i>	Q1 400,00	Q2 800,00
Cableado interno		Cableado interno para conectividad		Q2 000,00
Configuración Servidor		Configuración de todos los servicios necesarios para el funcionamiento del servidor		Q8 000,00
Mano de obra		Mano de obra calificada para la instalación del servidor		Q5 000,00
TOTAL				Q24 300,00

Fuente: elaboración propia.

Como se observó en la tabla VI, el costo total para la implementación del sistema SSH/FTP de interconexión entre empresas de telefonía en Guatemala, para el reporte automático y posterior bloqueo de IMIE reportados como robados, es de Q24 300,00.

CONCLUSIONES

1. Aunque la tecnología GSM ya es la de mayor utilización, su arquitectura de una red sigue la base para el desarrollo de nuevas arquitecturas. La arquitectura UMTS es una arquitectura GSM con Packet Core.
2. El protocolo de señalización SS7, es de mayor utilización en la actualidad para la señalización de todos los protocolos de telecomunicaciones. SS7 realiza interconexión de bloques a nivel de arquitectura, lo cual se realiza mediante una serie de protocolos de comunicaciones estándares.
3. El protocolo FTP se utiliza para la transferencia segura de datos entre un servido y un cliente, un cliente y un cliente, o un cliente y un servidor. El protocolo SSH se utiliza para la administración remota de un servidor. La diferencia fundamental entre ambos protocolos es que FTP únicamente puede transferir archivos, mientras que el SSH puede trasferir archivos y administrar el servidor.
4. El sistema SSH/FTP para el reporte automático de un IMEI reportado como robado o extraviado tiene como beneficio fundamental reducir el índice de robo de teléfonos celulares, ya que los mismos no podrán ser utilizados en Guatemala nuevamente. Adicional, se conseguirá que si un número de IMEI es utilizado para acciones anormales, las 3 compañías de telefonía lo bloquearán y ya no podrá seguir operando.

RECOMENDACIONES

1. Revisar a detalle las arquitecturas de red GSM y UMTS, para entender las diferencias existentes entre ambas y entender la razón por la cual GSM es utilizada para servicios de voz y UMTS para servicios de datos.
2. Dentro de una arquitectura de red con SS7, se debe tener en cuenta los tipos de enlaces a utilizar dependiendo de los equipos o bloques que se interconectarán.
3. El servidor SSH/FTP debe ser protegido contra accesos indebidos, uno de los métodos más fáciles para realizar dicha protección es cambiando las credenciales de usuario con una periodicidad de 1 mes.
4. Para la creación de cada Shell Script se debe iniciar el archivo con la declaración de cabecera `#!/bin/sh` y posteriormente guardar el archivo con la extensión `.sh`.
5. Para la generación del archivo Perl Script se debe iniciar el archivo con la declaración de cabecera `#!/bin/sh` y dicho archivo debe ser guardado con la extensión `.pl`.
6. Tanto el servidor principal como los servidores de cada compañía de telecomunicaciones, deben tener configurada una misma fecha y hora, esto para evitar problemas horarios.

BIBLIOGRAFÍA

1. 3GPP. *GSM History*. [en línea]. < <http://www.3gpp.org/specifications/gsm-history> >. [Consulta: 25 de abril de 2016].
2. _____. *GSM specifications*. [en línea]. < <http://www.3gpp.org/specifications>>. [Consulta: 1 de mayo de 2016].
3. _____. *UMTS*. [en línea]. <<http://www.3gpp.org/technologies/keywords-acronyms/103-umts>>. [Consulta: 20 de abril de 2016].
4. _____. *OPEN SS7. Mobile Application Part Interface Specification* [en línea]. <<http://www.openss7.org/specs/mapi.pdf>>. [Consulta: 15 de mayo de 2016].
5. HARTMANN, Christian. *GSM Architecture, Protocols and Services*. Inglaterra: Wiley, 2009. 325 p. ISBN: 978-0470030707.
6. HOLMA, Harri. *HSDPA / HSUPA For UMTS*. Inglaterra: Wiley, 2006. 245 p. ISBN: 978-0470018842.
7. JOHNSON, Chris. *Pro Bash Programming: Scripting the GNU/Linux Shell*. United State of America: APRESS, 2009. 230 p. ISBN: 978-1430219972.

8. LAITINEN, Lauri. *Redes UMTS. Arquitectura, movilidad y servicios*. España: Ra-ma, 2006. 584 p. ISBN: 978-84-7897-709-3.
9. MOULY, Michel. *The GSM System for Mobile Communications*. Inglaterra: &Sys, 2008. 280 p. ISBN: 978-1114561548.
10. OPEN SS7. *Map Desing*. [en línea]. <http://www.openss7.org/map_design.html>. [Consulta: 17 de mayo de 2016].
11. SAUTER, Martin. *From GSM to LTE-Advanced*. Inglaterra: Wiley, 2015. 441 p. ISBN: 978-1118861950.
12. SCHWARTZ, Randal. *Learning Perl*. United State of America: O'Reilly Media, 2011. 360 p. ISBN: 978-1449303587.
13. SILVERMAN, Richard. *SSH The Secure Shell*. United State of America: O'Reilly, 2005. 645 p. ISBN: 978-0596008956.