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

DESARROLLO DE UN DICCIONARIO DE LA LENGUA ESPAÑOLA EN LÍNEA ACCESADO VÍA MENSAJES CORTOS (SMS) EN LA RED CELULAR GSM DE COMCEL (TIGO)

Juan Eduardo Solares Villalobos

Asesorado por el Ing. Marlon Giovanni Rojas Cancinos

Guatemala, julio de 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DESARROLLO DE UN DICCIONARIO DE LA LENGUA ESPAÑOLA EN LÍNEA ACCESADO VÍA MENSAJES CORTOS (SMS) EN LA RED CELULAR GSM DE COMCEL (TIGO)

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

JUAN EDUARDO SOLARES VILLALOBOS
ASESORADO POR EL ING. MARLON GIOVANNI ROJAS CANCINOS

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, JULIO DE 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Ing. Alfredo Enrique Beber Aceituno
VOCAL II	Ing. Pedro Antonio Aguilar Polanco
VOCAL III	Inga. Elvira Miriam Ruballos Samayoa
VOCAL IV	Br. Walter Rafael Véliz Muñoz
VOCAL V	Br. Sergio Alejandro Donis Soto
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. Guillermo Antonio Puente Romero
EXAMINADOR	Ing. Kenneth Issur Estrada Ruíz
EXAMINADOR	Ing. Marlon Giovanni Rojas Cancinos
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:

DESARROLLO DE UN DICCIONARIO DE LA LENGUA ESPAÑOLA EN LÍNEA ACCESADO VÍA MENSAJES CORTOS (SMS) EN LA RED CELULAR GSM DE COMCEL (TIGO)

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 11 de octubre de 2006.

Juan Eduardo Solares Villalobos

Guatemala, 13 de Agosto del 2010

Ing. Julio César Solares Peñate
Coordinador de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Ingeniero Solares:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **"DESARROLLO DE UN DICCIONARIO DE LA LENGUA ESPAÑOLA EN LINEA ACCESADO VIA MENSAJES CORTOS (SMS) EN LA RED CELULAR GSM DE COMCEL (TIGO)"**, desarrollado por el estudiante **Juan Eduardo Solares Villalobos**, ya que considero que cumple con los requisitos establecidos, por lo que el autor y mi persona somos responsables del contenido y conclusiones del mismo.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

Ing. Marlon Giovanni Rojas Cancinos.
ASESOR
Marlon Giovanni Rojas Cancinos
INGENIERO ELECTRONICO
COLEGIADO No. 6589

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

Ref. EIME 30. 2011
Guatemala, 18 de MAYO 2011.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingeniería Mecànica Elèctrica
Facultad de Ingeniería, USAC.

Señor Director:

Me **permito dar aprobación al trabajo de Graduación titulado: "DESARROLLO DE UN DICCIONARIO DE LA LENGUA ESPAÑOLA EN LÍNEA ACCESADO VÍA MENSAJES CORTOS (SMS) EN LA RED CELULAR GSM DE COMCEL (TIGO)", del estudiante JUAN EDUARDO SOLARES VILLALOBOS, 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 de Electrónica

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

CEGS/sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

REF. EIME 37. 2011.

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; JUAN EDUARDO SOLARES VILLALOBOS titulado: "DESARROLLO DE UN DICCIONARIO DE LA LENGUA ESPAÑOLA EN LÍNEA ACCESADO VÍA MENSAJES CORTOS (SMS) EN LA RED CELULAR GSM DE COMCEL (TIGO), procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 19 DE MAYO 2,011.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

DTG. 511 .2013

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: **DESARROLLO DE UN DICCIONARIO DE LA LENGUA ESPAÑOLA EN LÍNEA ACCESADO VÍA MENSAJES CORTOS (SMS) EN LA RED CELULAR GSM DE COMCEL (TIGO),** presentado por el estudiante universitario **Juan Eduardo Solares Villalobos,** autoriza la impresión del mismo.

IMPRÍMASE:

Ing. Murphy Olympo Paiz Recinos
Decano

Guatemala, 19 de julio de 2013

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

/gdech

ACTO QUE DEDICO A:

Mis padres

Madre, padre he aquí al ingeniero que forjaron y alentaron, desde tu vientre madre, desde tu sueños padre.

AGRADECIMIENTOS A:

Dios	Fuerza que todo lo une.
La Virgen María	Que ha guiado mi vida llenándola de fe.
Mis padres	Sr. Juan Solares Navarro y Sra. Francisca Villalobos Romero, porque predicaron en mí con el ejemplo de esfuerzo, dedicación, amor y sencillez.
Mis hermanos	Gilda, Jorge, Sandra, Lucrecia, María, Marcos (q.e.p.d.), Lissette y Lesbia Solares Villalobos**,** porque me han dado día con día un significado de unión y cariño.
Mi esposa	Brenda Jo, por su amor en cada momento.
Mis hijos	Guillermo, Irene y Juan Fernando por ser la manifestación máxima de mi felicidad.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

ACK Acuse de recibo o *ACK* (*ACKnowledgement*), en comunicaciones entre computadores, es un mensaje que se envía para confirmar que un mensaje o un conjunto de mensajes han llegado.

AOC *(Advice of charge).* Notificación del importe, en transmisión de datos.

APDU *(Application Protocol Data Unit.)* Unidad de comunicación entre un lector de tarjetas inteligentes y una tarjeta inteligente.

ARPU *(Average Revenue Per User).* Crecimiento de subscriptores sin mermar el ingreso promedio por usuario.

AT *(Attention.)* Comandos *AT* de instrucciones codificadas que conforman un lenguaje de comunicación entre el hombre y una terminal *MODEM*.

ATM *(Automatic Teller Machine).* Una tecnología de conmutación y multiplexación denominada modo de transferencia asíncrona, con características de alta velocidad para transmisión de información a través de área local.

AUC *(Authentication Centre).* Centro de autentificación verifica la identidad de cada tarjeta *SIM* que intenta conectarse a la red GSM.

BACKoff Retroceso incremental, es un algoritmo que utiliza retroalimentación para disminuir la tasa multiplicativamente de algún proceso, a fin de encontrar poco a poco una tasa aceptable.

Bluetooth Es una especificación industrial para redes inalámbricas de área personal que posibilita la transmisión de voz y datos entre diferentes dispositivos mediante un enlace por radiofrecuencia en la banda ISM de los 2,4 GHz.

BSC *(Base Station Controler).* Controlador de estación base, en redes celulares.

BTS (*Base Transceiver Station).* Estación transceptor base, en redes celulares.

BW *(Band Width).* Ancho de banda, transmisión de datos.

CFNRc Desvío de llamadas no alcanzables.

CFU Desvío de llamada incondicional.

Checksum Una suma de verificación es una forma de control de redundancia, una medida muy simple para proteger la integridad de datos, verificando que no hayan sido corruptos.

CPDU *(Cotrol Protocol Data Unit).* PDU de control que sirve para gobernar el comportamiento completo del protocolo en sus funciones de establecimiento y ruptura de la conexión, control de flujo, control de errores, etc. No contienen información alguna proveniente del nivel N+1.

CSMA/CD Acceso múltiple por detección de portadora con detección de colisiones (*Carrier Sense Multiple Access with Collision Detection*), es una técnica usada en redes *Ethernet* para mejorar sus prestaciones.

CUGs *(Closed User Groups).* Grupos de usuarios cerrados, aplicación de red inteligente.

CWND *(Congestion Window).* Ventana de congestión. Espacio de tiempo utilizado en envío de segmentos de una transmisión de datos.

DPDU *(Data Protocol Data Unit).* Contiene los datos del usuario final (en el caso de la capa de aplicación) o la PDU del nivel inmediatamente superior**.**

DSAP *(Destination Service Access Point).* El estándar del instituto de ingenieros eléctricos y electrónicos, incluye esta subcapa que añade las etiquetas estándar de 8-bit o el punto de acceso del servicio de destino (*Destination Service Access Point*).

EIR *(EquipmentIidentity Register).* Registro de identidad del equipo guarda la lista de las estaciones móviles que están prohibidas para operar en la red GSM.

ESME *(External Short Message Entity).* Entidades externas de mensajes cortos usualmente designado así a la parte cliente en el protocolo de envío, punto a punto de mensajes cortos.

ETC *(Explicit Transfer call).* Transferencia de llamadas explícitas.

Ethernet El protocolo de capa dos de mayor uso en las redes *LAN*.

FIN Indicador de terminación de trasmisión en estados TCP, puede ser terminada por la aplicación o por la parte remota de la conexión.

Firewalls	Corta fuego es una parte de un sistema o una red que está diseñado para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.
FTP	*(File tranfer protocol).* Servidor de ficheros que se refiere al protocolo de transferencia de archivos.
Gateway	Una combinación de hardware y software que interconecta redes o dispositivos de red que son incompatibles.
GCP	*(Gateway Control Protocol).* Protocolo de control de entrada usado en comunicación de voz sobre *IP*.
GPRS	*(General Packet radio Service).* Protocolo de servicio general de paquetes de radio**,** usado en trasmisión de datos en GSM.
GSM	*(Groupe Special Mobile).* Sistema global para comunicación móvil.
HLR	*(Home Location Register).* Registro de localización base. Base de datos de abonados en sistemas de conmutación.
HSCSD	*(High Speed Circuit Switched Data).* Alta velocidad de conmutación de circuitos de datos.

Host	Huésped o terminal, referente a una red.
Hub	Elemento central de una red, típicamente usado en las primeras redes *Ethernet*.
IN	*(Intelligent Network).* Red inteligente, integraciones de servicios en redes de conmutación.
IP	*(Internet Protocol).* Protocolo de Internet, opera en la capa tres del modelo OSI, es usado en el conjunto de protocolos TCP*/IP* que operan en Internet y la mayoría de redes privadas.
ISDN	*(Integrated Services Digital Network).* Red digital de servicios integrados**;** set de estándares de comunicación para trasmisión digital.
ISO	*(International Organization for Standardization).* Organización Internacional de Normas.
IT	*(Information Technology).* Tecnología de la información.
LAN	Red que interconecta todos los dispositivos que están en una localidad.

MAN Una red de área metropolitana (*Metropolitan Area Network*) es una red de alta velocidad (banda ancha) que da cobertura en un área geográfica extensa.

MP3 **(***MPEG*-1 *Audio Layer* 3). Formato de audio digital comprimido con pérdida desarrollado por *Moving Picture Experts Group* (MPEGH) para formar parte de la versión 1 (y posteriormente ampliado en la versión 2) del formato de vídeo MPEG.

MS *(Movil station).* Estación móvil que se refiere al aparato telefónico.

MSC *(Movil Switch Centre).* Centro de conmutación móvil, distribuidor de llamadas en redes telefónicas.

MSRN *(Mobile Station Roaming Number).* Número de estación móvil temporal, usado para identificación en centrales telefónicas de estaciones móviles combinadas con localidad y origen.

MSS *(Mobile Station Roaming Number).* Máximo tamaño de segmento en una trasmisión de datos.

NPDU *(Network Protocol Data Unit).* Unidad de datos de protocolo que es la información intercambiada entre entidades pares.

NSAP	*(Network Service Access Point).* El servicio de red punto de acceso (NSAP) es uno de los dos tipos de direcciones jerárquicas (el otro tipo es el título entidad de red) para implementar interconexión de sistemas abiertos.
OSI	*(Open Systems Interconnection).* Interconexión de sistemas abiertos.
PERL	*(Practical Extraction and Report Language).* Lenguaje práctico para la extracción e informe.
PCI	*(Protocol Control Information).* Protocolo de control.
PDU	*(Protocol Data Unit).* Unidad de control de datos.
PDUs	Unidades de datos de protocolo que se utilizan para el intercambio entre unidades parejas, dentro de una capa del modelo OSI.
PhPDU	(*Physical Layer Protocol Data Unit).* Utilizado para trasmitir mensajes en segmento del protocolo de datos.
PhSAP	(*Physical Services Access Point).* Punto de acceso de servicio físico.

PLMN *(Public Land Mobile Network).* Red móvil pública terrestre.

POP *(Post Office Protocol).* En informática se utiliza el protocolo de la oficina de correo (*POP3*) en clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. Es un protocolo de nivel de aplicación en el modelo OSI.

PPDU (*Presentation Layer Protocol Data Unit).* Unidad de datos en la capa de presentación en el modelo OSI.

PSTN *(Public Switched Telephone Network).* Red pública de telefonía conmutada.

RFC Petición de comentarios o RFC (*Request for Comments*) son una serie de notas sobre Internet que comenzaron a publicarse en 1969. Se abrevian como RFC.

Roaming Recepción de llamada en otro país o red vecina, en referencia a una unidad móvil.

Router Ruteador, asociado a equipos de telecomunicaciones que hacen la función de enlace entre varios dispositivos en un área TCP-*IP*, a diferencia del *switch* un ruteador tiene capacidad de decidir rutas.

RTO *(Recovery time objective).* Tiempo objetivo de recuperación, parte de la ventana TCP.

RTT *(Round-Trip Time).* Tiempo medio de viaje, parte de TCP.

SAP *(Service Access Point).* Punto de acceso de servicio, parte de TCP.

SDL *(Specification and Design Language).* Enlace de señalización de datos, parte de TCP.

SDU *(Service Data Unit).* Unidad de Servicio, parte de TCP.

SIM *(Subscriber Identity Module).* Módulo de identificación del abonado, es una tarjeta inteligente desmontable usada en teléfonos móviles y módems

SMPP *(Short Message Peer-to-Peer).* Mensajes cortos punto a punto desarrollado con la intención de proveer la flexibilidad de una interfase en la comunicación de datos para transferir mensajes cortos.

SMS *(Short Message Service).* Mensaje corto de texto.

SMSC *(Short Message Service Centre).* Centro de mensaje.

SMTP	*(Simple Mail Transfer Protocol).* Protocolo de trasporte de mensaje.
SNA	*(Systems Network Architecture).* Sistema de arquitectura de red.
Switch	Conmutador asociado a equipos de telecomunicaciones que hacen la función de enlace entre varios dispositivos en un área TCP-IP.
SYN	Sincronismo, parte del estado TCP.
TCP	*(Transmission Control Protocol).* Protocolo de transporte.
TDMA	*(Time Division Multiple Access).* La multiplexación por división de tiempo (TDM).
TPDU	*(Transport Protocol Data Unit).* Unidad de datos en la capa de transporte.
Transceiver	En redes de computadoras y telecomunicación este término se aplica a un dispositivo que realiza dentro de una misma caja o chasis, funciones tanto de trasmisión como de recepción.
TS	*(Time Slot).* Ranuras de tiempo.

UDP *(User Datagram Protocol).* Protocolo datagrama de usuario, es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión.

UMTS *(Universal Mobile Telecommunications System).* Sistema universal de telecomunicaciones móviles, es una de las tecnologías usadas por los móviles de tercera generación (3G, también llamado W-CDMA), sucesora de GSM.

USSD *(UnStructured Supplementary Services).* Servicio complementario de servicio de datos, estándar**.**

VLR *(Visitor Location Register).* Registro de localización del visitante.

VPN *(Virtual Private Network).* Red privada virtual.

WAN *(Wide Area Network).* Un área amplia se extiende sobre un área geográfica extensa, a veces a un país o un continente y su función fundamental está orientada a la interconexión de redes o equipos terminales que se encuentran ubicados a grandes distancias entre sí.

WAP *(Wireless Application Protocol).* Protocolo de aplicaciones inalámbricas, utilizado en el despliegue de datos a unidades móviles.

W-CDMA *(Wideband Code Division Multiple Access).* Acceso múltiple por división de código de banda ancha es una tecnología móvil inalámbrica de tercera generación que aumenta las tasas de transmisión de datos de los sistemas GSM utilizando la interfaz aérea CDMA en lugar de TDMA (Acceso Múltiple por División de Tiempo).

RESUMEN

El objetivo de este trabajo de graduación que se ejecuta por medio del Ejercicio Profesional Supervisado (EPS), es unir el conocimiento adquirido de Ingeniería Electrónica, con la tecnología utilizada actualmente en redes de telefonía celular.

Presenta un marco teórico general, que empieza con la descripción del modelo de interconexión de sistemas abiertos que llegan a un ámbito de redes ethernet, en donde se toman conceptos de redes celulares GSM, para luego unirlas en una aplicación de mensajes cortos que presenta un modelo cliente-servidor, entre dos entidades. Estas son tecnológicas públicas como CONCYT y otra privada como TIGO que, haciendo uso de una aplicación como soporte del servicio, interactúan con usuarios de teléfonos celulares devolviéndoles significados y contenido a consultas de palabras en diccionario en línea.

OBJETIVOS

General

Aplicar tecnología para promoción y educación, así como dar una herramienta de fácil uso para consulta y aprendizaje.

Específicos

1. Describir las aplicaciones, medios de transmisión y uso de la mensajería corta.

2. Aplicar conocimientos de telecomunicaciones en usos prácticos.

3. Utilizar un medio conocido y de fácil uso para consultas a un diccionario.

4. Aplicar conocimientos administrativos y comerciales en proyectos tecnológicos.

5. Proyectar socialmente servicios tecnológicos.

6. Incluir aplicaciones educacionales en los modelos de negocio de telecomunicaciones.

INTRODUCCIÓN

Una aplicación móvil de amplio uso en la red tanto en Latinoamérica como en el mundo, es aquella que recibe y trasmite mensajes de texto vía red celular, desde una terminal hasta el repositorio de contenido en un proveedor.

Tomando la importancia y el potencial de llegar a usuarios que requieran información y tengan facilidad de uso y acceso, nació el proyecto de realizar una aplicación de mensajes cortos cuyo contenido esté en los servidores del Consejo Nacional de Ciencia y Tecnología (CONCYT) y que la red celular de TIGO pueda proporcionar acceso directo, con tan solo enviar la palabra a un número corto determinado, que aplique los conocimientos adquiridos durante la carrera de Ingeniería Electrónica de la Universidad de San Carlos de Guatemala.

El capítulo uno expone temas que engloban los fundamentos base en el desarrollo posterior, pasando por las capas físicas de red, abordando el funcionamiento de protocolos, de tecnología de acceso celular como GSM, y finalizando en cómo se pueden trasmitir datos por la red haciendo entrega de mensajes cortos con el protocolo SMPP.

En el capítulo dos describe paso a paso las partes en el protocolo y la interacción entre estas que hacen referencia a componentes de red SS7 y sus respectivas capas, como la capa de aplicación y presentación que se unen para dar significado al envío de datos y caracteres que componen un mensaje corto.

En el capítulo 3 detalla el flujo para la entrega de un mensaje, las posibles interacciones y mensajes de error o éxito en ese flujo.

En el capítulo 4 expone información general de la empresa y cómo funciona TIGO y SENACYT en el tema de tecnología y envío de mensajes cortos, dando ejemplos que ayudarán a entender la unión de un proveedor de servicios con un operador de telefonía celular.

En el capítulo 5 describe cómo se desarrolla una aplicación de envío y recepción de mensajes cortos por medio de Perl, cómo se almacena la información y se maneja la respuesta a quien origina el mensaje.

En el capítulo 6 expone la realización de análisis económico y aplicativo en forma funcional de mensajes cortos vía celular, cómo se analiza el precio o acuerdo entre operador y quien presta el servicio.

En el capítulo 7 concluye con una presentación de documentación de funcionalidad de la aplicación en servidores y los pasos para conexión y operación-mantenimiento de la aplicación

1. CONCEPTOS Y DEFINICIONES ELEMENTALES DE COMUNICACIONES

1.1. Protocolo de comunicación de datos

El protocolo de comunicación de datos se refiere al conjunto de reglas y acuerdos por medio de los cuales se trasfiere información entre dos partes en una red.

1.1.1. Modelo de interconexión de sistemas abiertos u OSI

La Unión Internacional de Telecomunicaciones (UIT), es el organismo especializado de las Naciones Unidas encargado de regular las telecomunicaciones, a nivel internacional, entre las distintas administraciones y empresas operadoras.

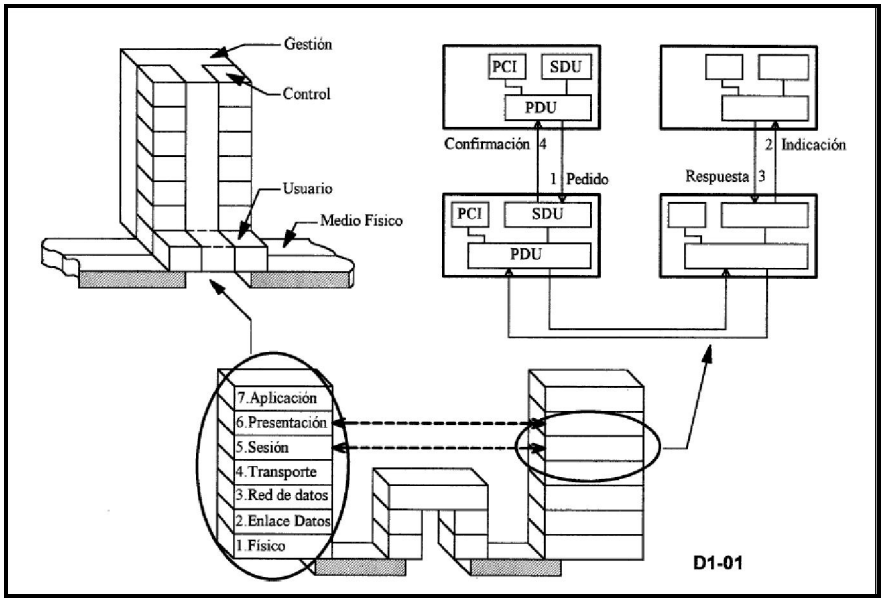
El 3 de septiembre de 1932, se inició en Madrid (España), la reunión conjunta de la XIII Conferencia de la Unión Telegráfica Internacional (UTI), creada en París el 17 de mayo de 1865, y la III de la Unión Radiotelegráfica Internacional (URI) para el 9 de diciembre del mismo año en virtud de los acuerdos alcanzados en dicha reunión, se firmó el convenio por el que se creaba la Unión Internacional de Telecomunicaciones, que en el futuro sustituiría a los dos organismos anteriores (UTI y URI). El nuevo nombre comenzó a utilizarse a partir de enero de 1934. ITU-T X.200, específicamente describe el modelo OSI como sector de Normalización de las Comunicaciones.

El modelo es iniciado por la IBM para redes de computadoras. En IBM se denomina SNA (*Systems Network Arquitectura*) y es original de 1974, con versión definitiva en 1985. Este modelo es perfeccionado por la Organización Internacional de Normalización, ISO en el estándar ISO 3309. El modelo ISO se inicia en 1977 y se adopta en 1984. Se denomina Modelo de Interconexión de Sistemas Abiertos OSI con 7 capas. En ITU-T X.200 se adopta el modelo ISO/*IEC* 7498-1 para sistemas de comunicaciones.

La finalidad del modelo OSI es permitir la cooperación entre sistemas abiertos. Un sistema real abierto es aquel conjunto de ordenadores, material lógico, periféricos, terminales, operadores humanos, etc., que forma un todo autónomo capaz de procesar y/o transferir información. Cada sistema abierto se considera constituido por un conjunto de 7 capas o estratos representados en forma vertical.

El modelo prevee una comunicación vertical entre capas (capa N+1 con N y N con N-1) (ver figura 1) denominado servicio y una comunicación horizontal (capa N con N) entre distintos sistemas abiertos denominado protocolo (protocolo entre entidades pares o iguales *peer-to-peer*). Cada capa N ofrece un servicio a la capa inmediatamente superior N+1 y requiere los servicios de la inferior N-1. Para la comunicación se definen los puntos de conexión SAP (*Service Access Point*) que funcionan como direcciones de la capa superior. Una entidad puede tener activas varias direcciones SAP simultáneamente.

Figura 1. **Modelo de siete capas OSI**



Fuente: PEDRA, Marcelo. Domótica, modelo OSI. p. 34.

Las distintas capas verticales requieren y ofrecen un servicio, en la figura 1 se puede concluir que:

- Cada capa genérica N recibe una unidad de servicio o SDU desde la capa N+1.

- Agrega una información adicional denominado protocolo de control o PCI.

- Forma la unidad de datos PDU que corresponde al PCI de la capa N-1. El término PDU (*Protocol Data Unit*) es usado por ISO para todas las capas e incluye a PCI y el encabezado PCI. Para cada capa se antepone la inicial a la sigla que la identifica y el nombre más usual:

- APDU, PPDU, SPDU: para las capas 7, 6 y 5 respectivamente.
- TPDU (capa 4: segmento en TCP y mensaje en SMTP y SS7).
- NPDU (capa 3: paquete en X.25 y datagrama en IP).
- DPDU (capa 2: tramas en LAN y FR, celda en ATM y MAN y paquete en X.25).
- *Ph*PDU (capa 1: trama y envoltura): la dirección que identifica la capa se indica como SAP; de esta forma da lugar a las direcciones NSAP, DSAP y PhSAP. La comunicación entre capas determina 4 servicios primitivos:
    - Pedido desde N a N-1 (requerimiento de servicio)
    - Indicación desde N-1 a N (notificación de requerimiento)
    - Respuesta desde N a N-1 (reconocimiento de indicación)
    - Confirmación desde N-1 a N (pedido completado)

1.1.1.1. Descripción de las capas del modelo OSI

De acuerdo con la figura 2 se dispone de un modelo de 7 capas en general. Las capas superiores (5-6-7) corresponden a funciones de elaboración de la información; las intermedias (3-4) corresponden a funciones de comunicación y las inferiores (1-2) a control de la conexión.

En la figura 2 se tiene la definición y funciones que cumple cada capa del modelo de interconexión de sistemas abiertos u OSI (*Open System Interconnection*) de ISO.

Los elementos que determina el protocolo de capa 5-6-7 son:

- Sintaxis: formato de datos (relación entre campos de datos)
- Semántica: control de información (significado de los datos)
- Temporización: adaptación de velocidad y secuencia

Al conjunto de capas superiores pertenecen el sistema de operación del host (MS-DOS, UNIX, Windows NT), el sistema de operación de red LAN (NetWare, IBM OS/2 LAN Server), los programas de aplicación de usuario (Lotus Notes, cc: Mail, MS Mail, Schedule, etc.) y los programas utilitarios de LAN (Transferencia de file, emulación de terminal, etc.). Los programas involucrados en las capas 3 y 4 se basan en alguna de las estructuras de facto (Microsoft/IBM Net, Novell SPX/IPX) o de jure (TCP/IP e ISO). En las capas 2 y 1 se identifica la conexión al medio físico. Pueden ser provistas mediante conexiones punto a punto o redes de datos (LAN, MAN y WAN). De esta forma se tiene en cuenta el acceso a la red LAN o MAN. También, se involucra la operación de internetwork consistente en Switch-Router que permiten la interconexión de redes iguales o distintas.

El modelo especifica el protocolo que debe ser usado en cada capa (ver figura 2), y suele hablarse de modelo de referencia, ya que es usado como una gran herramienta para la enseñanza de comunicación de redes. Este modelo está dividido en siete capas: nivel de aplicación, nivel de presentación, nivel de sesión, nivel de trasporte, nivel de red, nivel de datos y nivel físico.

Figura 2. **Niveles del modelo de siete capas**

Fuente: PANTOJA, Pablo. La pila OSI. Scribd documento 24338955 p. 4.

1.1.1.2. Capa física

Se encarga de las conexiones físicas de la computadora hacia la red, tanto en lo que se refiere al medio físico como a la forma en la que se transmite la información.

Sus principales funciones se pueden resumir como:

- Definir el medio o medios físicos por los que va a viajar la comunicación: cable de pares trenzados o no como en RS232/EIA232, coaxial, guías de ondas, aire y fibra óptica.

- Definir las características materiales (componentes y conectores mecánicos) y eléctricas (niveles de tensión), que se van a usar en la transmisión de los datos por los medios físicos.

- Definir las características funcionales de la interfaz (establecimiento, mantenimiento y liberación del enlace físico).

- Transmitir el flujo de datos a través del medio.

- Manejar las señales eléctricas y electromagnéticas.

- Especificar cables, conectores y componentes de interfaz con el medio de transmisión, polos en un enchufe, etc.

- Garantizar la conexión aunque no la fiabilidad de esta.

1.1.1.3. Capa de enlace de datos

Se ocupa del direccionamiento físico, de la topología y acceso a la red; de la notificación de errores, distribución ordenada de tramas y del control del flujo. Se hace un direccionamiento de los datos en la red, ya sea en la distribución adecuada desde un emisor a un receptor, la notificación de errores y de la topología de la red de cualquier tipo.

1.1.1.4. Capa de red

El objetivo de la capa de red es hacer que los datos lleguen desde el origen al destino aun cuando ambos no estén conectados directamente. Los

dispositivos que facilitan tal tarea se denominan enrutadores o *routers* (mayormente conocidos).

Los *routers* trabajan en esta capa, aunque pueden actuar como *switch* de nivel 2 en determinados casos, dependiendo de la función que se le asigne. Los bloqueadores de accesos no autorizados o *firewalls* actúan sobre esta capa, principalmente, para descartar direcciones de máquinas. En este nivel se realiza el direccionamiento lógico y la determinación de la ruta de los datos hasta su receptor final.

1.1.1.5. Capa de transporte

Encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete), de la máquina de origen a la de destino, independizándolo del tipo de red física que se esté utilizando. La PDU de la capa 4 se llama Segmento. Sus protocolos son TCP y UDP el primero orientado a conexión y el otro sin conexión.

1.1.1.6. Capa de sesión

Encargada de mantener y controlar el enlace establecido entre las dos computadoras que están transmitiendo datos de cualquier índole.

Por lo tanto, el servicio provisto por esta capa tiene la capacidad de asegurar de que dada una sesión establecida entre dos máquinas, la misma se pueda efectuar para las operaciones definidas de principio a fin, reanudándolas en caso de interrupción. En muchos casos, los servicios de la capa de sesión son parcial o totalmente prescindibles.

1.1.1.7. Capa de presentación

El objetivo es encargarse de la representación de la información, de manera que aunque distintos equipos puedan tener diferentes representaciones internas de caracteres los datos lleguen de manera reconocible. Esta capa es la primera en trabajar, el contenido de la comunicación y cómo se establece la misma. En ella se tratan aspectos tales como: la semántica y la sintaxis de los datos transmitidos, ya que distintas computadoras pueden tener diferentes formas de manejarlas. Esta capa, también, permite cifrar los datos y comprimirlos.

1.1.1.8. Capa de aplicación

Ofrece a las aplicaciones la posibilidad de acceder a los servicios de las demás capas y define los protocolos que utilizan las aplicaciones para intercambiar datos, como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros o FTP. Hay tantos protocolos como aplicaciones y puesto que continuamente se desarrollan nuevas aplicaciones, el número de protocolos crece sin parar.

Cabe aclarar que el usuario normalmente no interactúa directamente con el nivel de aplicación. Suele interactuar con programas que a su vez interactúan con el nivel de aplicación pero ocultando la complejidad subyacente.

1.1.2. Protocolo de transporte o TCP orientado a protocolo de internet o IP

El protocolo de transporte TCP/IP orientado a una conexión extendida en Internet. Las aplicaciones de red más populares (ftp, telnet, acceso Web…) lo utilizan en sus comunicaciones. La función principal del nivel de transporte dentro de la arquitectura de protocolos TCP/IP es la de permitir la comunicación extremo a extremo entre dos aplicaciones de forma económica y fiable.

La unidad básica de transferencia se denomina segmento de tamaño máximo o MSS (*Maximum Segment Size*) expresado en octetos, que se observará más adelante negociará los extremos de la comunicación en el establecimiento de la misma.

Existe otro protocolo de transporte en la arquitectura TCP/IP muy diferente, en el protocolo datagrama de usuario o UDP (*User Datagram Protocol*).

Este es mucho más sencillo que TCP se limita a enviar paquetes de datos denominados datagramas, de una terminal a otra sin garantizar que éstos sean recibidos correctamente. Si la aplicación requiere confiabilidad en la comunicación, deberá ser ella misma la que se la proporcione o bien se tendrá que recurrir al TCP.

1.1.2.1. Características generales del protocolo de transporte o TCP

El protocolo de transporte o TCP proporciona un servicio de transporte de datos que ofrece a nivel superior:

- Fiabilidad
- Control de flujo
- Orientación a conexión
- Multiplexación
- Orientación a flujo de octetos
- Transferencia con almacenamiento

Aunque en la definición de TCP no aparece ningún mecanismo específico para el control de la congestión, son varios los algoritmos desarrollados posteriormente con este objetivo. A continuación se analizarán cada una de estas características.

- Transmisión fiable: TCP está diseñado para recuperarse ante situaciones de corrupción, pérdida, duplicación o desorden de datos que puedan generarse durante el proceso de comunicación. Para conseguirlo, utiliza reconocimientos positivos y retransmisiones. Cada octeto de datos transmitido tiene asignado un número de secuencia. El número de secuencia del primer octeto de datos en un segmento que se almacena en la cabecera del mismo y recibe el nombre de número de secuencia del segmento. Los segmentos, también, contienen un número de reconocimiento que identifica la secuencia del siguiente octeto que se espera recibir.

Cuando TCP transmite un segmento con datos, coloca una copia en la cola de retransmisión e inicia un temporizador. Al recibir el reconocimiento o ACK (*knowledge*) para él, TCP lo borra de la cola. Si no se llega a recibir el ACK antes de que el temporizador expire, el segmento es retransmitido.

En recepción, los números de secuencia son utilizados para ordenar correctamente los segmentos (en caso de que alguno llegue fuera de orden) y para eliminar los duplicados. La corrupción de segmentos a nivel de transporte se detecta a través del *Checksum* incluido en cada uno de ellos y el cual es verificado en recepción. Todo segmento erróneo es descartado inmediatamente y no da lugar a reconocimiento alguno.

TCP utiliza un esquema de reconocimientos acumulativos, es decir, el receptor informa con el número de reconocimiento hasta qué el octeto del flujo de datos enviados reciba correctamente. Este sistema presenta varias ventajas:

- Por un lado los reconocimientos son fáciles de generar y no resultan ambiguos.

- Por otro, la pérdida de reconocimientos no fuerza, necesariamente, la retransmisión de segmentos.

Esta característica de TCP permitirá mejorar su comportamiento en enlaces asimétricos, tal y como se verá en el capítulo correspondiente. Sin embargo, el carácter acumulativo de los reconocimientos hace que el emisor no reciba información de todas las transmisiones correctas, sino únicamente del último octeto de flujo continuo recibido sin errores.

El tratamiento de la temporización y la retransmisión es fundamental en TCP, tanto en entornos como el móvil en los que las pérdidas son frecuentes, tambien en redes fijas en las cuales la congestión puede dar lugar a pérdidas de paquetes o retardos importantes. Para llevar a cabo este tratamiento se han establecido las siguientes estrategias:

- Algoritmo de retransmisión adaptativo [Ste94, Jac88]

  - El ajuste del temporizador de retransmisión o RTO (*Retransmission Time Out*), es especialmente crítico en TCP, al actuar tanto en redes locales, en enlaces punto a punto o en una red tan cambiante como Internet. Debe asegurarse un mecanismo que funcione correctamente en entornos tan diferentes como en los que opera TCP. RTO debe ser suficientemente pequeño para responder rápidamente a las pérdidas, pero no tanto para forzar la retransmisión de datos que han sufrido un pico de retardo en la red sin haber llegado a perderse, como sería el caso de congestión.

  - Para adaptarse a los retardos variables característicos de un entorno como Internet, TCP usa un algoritmo de retransmisión adaptativo que monitoriza el retardo en cada conexión y ajusta el valor de RTO de acuerdo con ese valor. La especificación del protocolo sugiere tomar muestras del tiempo de ida y vuelta o RTT (*Round Trip Time*), calculado como la diferencia de tiempo entre la emisión de un segmento y la recepción de su reconocimiento. Con esta información, TCP puede ajustar dinámicamente una variable que identifique el tiempo medio de ida y vuelta.

- Algoritmo de Karn [KaP87]

    - Cuando se recibe un reconocimiento de un segmento que ha sido objeto de retransmisión, es imposible determinar si éste corresponde al primer segmento transmitido o a su posterior retransmisión. El algoritmo de Karn evita esta ambigüedad.

    - Este algoritmo establece el cálculo del RTT estimado para determinar RTO, debe hacerse ignorando las muestras correspondientes a segmentos retransmitidos.

- Marca temporal o *Timestamp*

    - Existe una solución alternativa para la medida exacta de RTT que hace desaparecer la ambigüedad, de una forma que hace innecesaria la aplicación del algoritmo de Karn. Esta solución se basa en aprovechar el ancho de banda para mandar la información de tiempo en cada segmento. De esta forma puede realizarse una medida por cada segmento de 2-5 enviado independientemente, de si se trata de un segmento retransmitido o no, obteniendo así más medidas. Esta solución, si bien es adecuada para redes de alta velocidad en las que el ancho de banda no es un recurso escaso, no lo es para transmisiones sobre el canal móvil en las que el ancho de banda es un recurso que debe gestionarse y utilizarse de forma eficiente.

- *B*ACK*off* exponencial

  - Cuando se producen retransmisiones, según el RFC 793, debe aplicarse el RTO que exista en ese momento. No obstante, en caso de congestión esta política es contraproducente, ya que la propia congestión produce incrementos en el RTT. Consecuentemente se producirán retransmisiones innecesarias, ya que debido a la ambigüedad en la medida de RTT, las medidas de paquetes retransmitidos no se tienen en cuenta, y por lo tanto, el valor de RTO no se actualizará. Para evitar esta situación, la mayoría incorporan el algoritmo de *b*ack*off* exponencial.

  - Se establece un mecanismo de *b*ack*off* exponencial para espaciar las retransmisiones consecutivas de un mismo paquete, dando así tiempo a la red para que resuelva la congestión. La estrategia de *b*ack*off* exponencial utiliza, inicialmente, el tiempo de retransmisión calculado a partir de las fórmulas de RTT, sin embargo, si el temporizador expira y se produce una retransmisión, TCP incrementa el tiempo de retransmisión, si las retransmisiones persisten, TCP incrementa sucesivamente el RTO (para evitar un aumento excesivo de este parámetro, la mayoría de implementaciones de TCP limitan su valor a un máximo que supera el mayor retardo posible en Internet). Se utiliza el *b*ack*off* hasta que llega confirmación de un paquete que no ha sido retransmitido.

Aunque existen implementaciones que utilizan técnicas diferentes para establecer el *BACKoff*, la mayoría utilizan un factor multiplicativo:

$$RTO_{nuevo} = (beta)\ RTO_{anterior}$$
$$\text{con (beta)} = 2 \text{ (Normalmente)}$$

- Puesto que las pérdidas de paquetes son interpretadas por TCP como síntoma claro de congestión en la red, esta estrategia ayuda a frenar la inyección de datos, en estos casos, mejorando así la situación en la red. Ahora bien, en entornos móviles en el que los errores no tienen su origen en la congestión del enlace sino, fundamentalmente, en el propio carácter errático del canal de comunicación, tanto este como el resto de mecanismos de control de la congestión que incorpora TCP resultan muy poco idóneos, ya que contribuyen a retrasar la detección y recuperación del protocolo ante los errores.

- En particular, este algoritmo puede provocar una pérdida considerable de eficiencia del protocolo en casos de ráfagas de errores o de desconexiones temporales. En estos casos, es muy probable que tras repetidas retransmisiones el valor de RTO llegue a su valor máximo (RTOmáx), de forma que una vez se restablezca la comunicación, no sea tras RTOmáx que se retransmita el primer segmento afectado por la desconexión. Esto produce retardos muy elevados, ya que este valor máximo está adecuado a los casos de congestión.

- Existen también implementaciones de TCP en las que la retransmisión se realiza de forma selectiva [RFC2018]. De esta forma se solucionan los problemas que portan la confirmación positiva, evitando retransmisiones innecesarias, en este caso el emisor conoce con exactitud los segmentos recibidos en el extremo receptor.

- La retransmisión selectiva implica complejidad en el protocolo y solamente será justificable en aquellos casos en los que haya múltiples pérdidas por ventana de transmisión y las ganancias de un método respecto al otro sean considerables.

- Control de flujo

  TCP es un protocolo de ventana deslizante. Este mecanismo surge como una mejora de los protocolos con reconocimientos positivos de tipo *Stop&Wait*. Estos protocolos obligan al emisor a retrasar la emisión de cada nuevo paquete hasta que se recibe el ACK del anterior, desaprovechando así, la posible capacidad de comunicación bidireccional de la red. Los protocolos de ventana deslizante aprovechan mejor el ancho de banda al permitir transmitir un número determinado de paquetes antes de que llegue el ACK correspondiente. La ventana se coloca sobre la secuencia de octetos que configuran el flujo de datos proveniente de la aplicación e indica qué paquetes pueden ser transmitidos.

  Secuencia de segmentos ventana SEG N-3 SEG N-2 SEG N-1 SEG N SEG N+1 SEG N+2 SEG N+3 SEG N+4. El número de paquetes no reconocidos es como máximo, en cada momento, igual al tamaño de la ventana. Si el protocolo está bien sintonizado, mantendrá el enlace

completamente saturado. El valor óptimo para optimizar el ancho de banda disponible o BW es: ventana igual a RTT por BW

TCP utiliza un mecanismo de ventana deslizante especial que le sirve tanto para conseguir una transmisión eficiente (el emisor puede enviar múltiples segmentos sin esperar su reconocimiento), como para proporcionar control de flujo permitiendo al receptor restringir el número de octetos que puede recibir en cada momento. El receptor envía, junto con cada reconocimiento, el tamaño de ventana que puede aceptar en ese momento, es decir, el rango de números de secuencia aceptables a partir del último segmento recibido correctamente. Este tamaño puede variar. El emisor aplica continuamente la ventana recibida para determinar qué paquetes puede enviar.

- Multiplexación

Permite que varios procesos de una misma máquina utilicen simultáneamente el servicio que ofrece TCP. Éstos se diferencian dentro de la misma máquina por el valor del puerto asignado.

Tabla I. **Números de puerto universalmente conocidos**

Puerto	Nombre	Descripción
11	*systat active users*	Protocolo
20	ftp-data datos de *file transfer*	Protocolo
23	Telnet	Protocolo
22	SSH	Protocolo

Fuente: PEDRA, Marcelo**,** El protocolo TCP.

El protocolo proporciona una dirección o puerto a cada aplicación que lo usa. El conjunto formado por un número de puerto (que identifica una aplicación en una máquina) y una dirección IP (que identifica una máquina) recibe el nombre de *socket*. La asignación de puertos a procesos es manejada de forma independiente por cada máquina. No obstante, es común asignar números de puerto universalmente conocidos (ver tabla I) a algunos servidores de aplicaciones estándar sobre TCP. Algunos de ellos son [RFC1700]:

- Comunicación orientada a conexión

Los mecanismos que utiliza TCP para proporcionar fiabilidad, control de flujo y control de congestión, requieren que el protocolo inicialice y mantenga cierta información sobre el estado del flujo de datos. La combinación de toda esta información recibe el nombre de conexión. Cada conexión está unívocamente identificada por un par de *sockets* que identifica a los dos extremos de la comunicación.

Cuando dos procesos quieren comunicarse, sus TCP deben establecer primero, una conexión (es decir, inicializar la información de estado en cada extremo). Cuando la comunicación se ha completado, la conexión se cierra liberando los recursos para otros usos posteriores.

TCP inicia la conexión mediante un intercambio de mensajes de sincronismo o SYN a tres bandas (*Three Way Handshake*). Primero el extremo que quiere iniciar la conexión envía un mensaje SYN. En caso de que el extremo remoto acepte la conexión, manda a su vez un mensaje SYN, que además, confirma al mensaje anterior. Finalmente, el que ha iniciado la conexión manda a su vez un mensaje de confirmación o ACK.

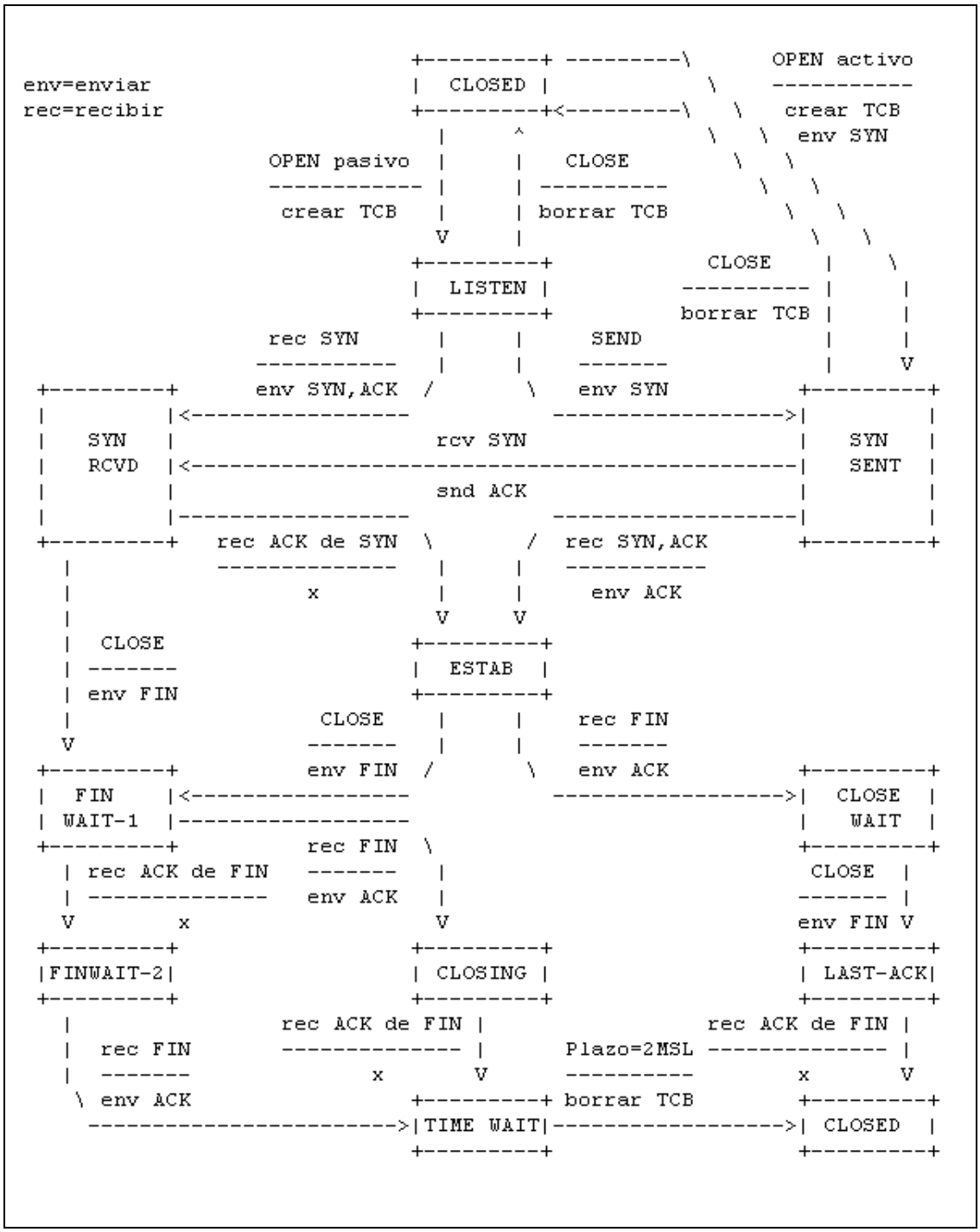
De esta forma los dos extremos 2-8 de la conexión se aseguran que ésta puede establecerse, es decir, que ambos extremos están de acuerdo.

Además, este intercambio de mensajes a tres bandas permite a ambos extremos acordar un número de secuencia inicial. Éstos se seleccionan de forma aleatoria y se usarán para identificar los octetos en el flujo de datos que se envía. Se trata del sincronismo de la conexión.

Una vez iniciada la conexión, empieza el período de intercambio de datos hasta que el programa de aplicación informa a TCP ya no tiene más datos para enviar. Para cerrar la conexión en cada uno de los sentidos se termina de transmitir los datos restantes y se envía un segmento de finalización o FIN. El otro extremo reconoce el segmento FIN y notifica a la aplicación que ya no existen más datos disponibles. Aunque se haya cerrado la conexión en uno de los sentidos, ésta todavía puede permanecer activa en el otro.

En la figura 3 se muestran estos intercambios de mensajes. En ella, además, se identifican los diferentes estados en los que se encuentra el TCP.

Figura 3. **Estados del protocolo de transporte o TCP**



Fuente: RFC 793. Protocolo de control de transmisión: especificación funcional. p. 10.

- Orientación a flujo de octetos

  El volumen de información transferido entre dos aplicaciones que utiliza TCP como protocolo de transporte, consiste en un flujo de octetos sin ningún tipo de marcas insertadas por TCP, para indicar formato o estructura alguna.

  - Si en un extremo de la conexión, la aplicación lleva a cabo una escritura de 10 octetos seguida de otra de 20 octetos y otra de 30 octetos, la aplicación del otro extremo no tiene forma alguna de determinar el tamaño concreto de cada una de ellas ya que se limita a recibir un flujo de 60 octetos sin marca o indicación alguna (es decir, quizá lo reciba a través de 3 lecturas de 20 octetos o 6 2-9 lecturas de 10 octetos, etc.). Un extremo inyecta un flujo de octetos en el nivel de transporte y el otro recibe exactamente la misma secuencia de octetos.

- Transferencia con almacenamiento

  Los programas del nivel de aplicación envían un flujo de datos a través del circuito virtual establecido entre los dos extremos, entregando continuamente octetos de información al software del protocolo. Al transferir los datos, cada aplicación utiliza fragmentos del tamaño que considera adecuado. TCP puede almacenar el número apropiado de octetos que permita, posteriormente, generar el datagrama de tamaño adecuado para ser transmitido por la red. Esto significa que, aunque la aplicación genere bloques de datos de tamaño muy reducido, TCP puede unirlos y permitir una transmisión más eficiente.

1.1.2.2. Control de la congestión

Cuando se definió e implementó TCP, las redes existentes presentaban como problema principal una baja fiabilidad, es decir, la presencia de errores era la característica limitante del comportamiento eficiente de la red. Las situaciones de congestión, causa principal del deterioro del comportamiento de las redes actuales, no fueron tenidas en cuenta y por ello, no se especificó mecanismo alguno para su control. Con el tiempo; sin embargo, se han ido desarrollando una serie de algoritmos con ese propósito [Jac88, RFC2581]:

1.1.2.3. Inicio lento o *slow start*

Esta estrategia se basa en el siguiente principio de equilibrio en la conexión: la tasa a la cual deberían inyectarse nuevos paquetes en la red es la tasa a la que llegan nuevos reconocimientos.

Esta afirmación indica que TCP es un protocolo auto sincronizado, ya que utiliza los reconocimientos como marcas para inyectar nuevos paquetes en la red. Cuando no hay segmentos en tránsito, como en el inicio de una conexión o en una expiración del temporizador de retransmisión, no existen ACK que permitan activar tal comportamiento; para conseguir que los paquetes fluyan, son necesarios ACK que lo permitan y para tener ACK es necesario un flujo de paquetes.

El mecanismo de inicio lento permite incrementar, gradualmente, la cantidad de datos en tránsito. Es el impulso inicial necesario para conseguir llevar la conexión al estado de equilibrio.

Este mecanismo utiliza una nueva ventana llamada de congestión o CWND, de manera que en cada momento, el emisor puede enviar el mínimo número de segmentos entre la cantidad permitida por la ventana de control de flujo y la permitida por la ventana de congestión. Esto significa que el algoritmo de inicio lento dejará de tener efecto una vez que CWND alcance el 2-10 tamaño de la ventana del receptor (siempre y cuando no se haya producido antes una pérdida de paquetes que inicie de nuevo el algoritmo).

El algoritmo opera de la siguiente forma:

- Al iniciarse una nueva conexión o al reiniciarse debido a una pérdida, inicializa CWND a un segmento: CWND igual a 1.

- Cada vez que se recibe un ACK incrementa en una unidad CWND: CWND++

Si, por ejemplo, el receptor envía un reconocimiento por cada segmento recibido, el emisor enviará 1 segmento durante el primer *RTT*, 2 segmentos durante el segundo, 4 durante el tercero y así sucesivamente. Esto provoca un incremento exponencial de la ventana, ya que con cada reconocimiento recibido el emisor puede enviar dos paquetes: uno debido al propio ACK (la ventana se desliza un segmento hacia la derecha) y otro por la apertura de la ventana exigida por el mecanismo de Inicio Lento.

1.2. Introducción al sistema global para las comunicaciones globales o GSM

A continuacion se detallan las tecnologias que soportan a al sistema global para comunicaciones.

1.2.1. Concepto

Los primeros trabajos con GSM los inició en 1982 un grupo dentro del Instituto Europeo de Normas de Comunicaciones o ETSI (*European Telecommunications Standards Institute*).

Originalmente, este organismo se llamaba *Groupe Sociale Mobile*, lo que dio pie al acrónimo GSM.

El objetivo de este proyecto era poner fin a la incompatibilidad de sistemas en el área de las comunicaciones móviles y crear una estructura de sistemas de comunicaciones a nivel europeo.

GSM se diseñó para incluir una amplia variedad de servicios que incluyen transmisiones de voz y servicios de manejo de mensajes entre unidades móviles o cualquier otra unidad portátil.

1.2.2. Componentes de GSM

El Centro de Conmutación Móvil o MSC (*Mobile Switching Center*), es el corazón de todo sistema GSM y se encarga de establecer, gestionar y despejar conexiones, así como de enrutar las llamadas a la célula correcta. El MSC proporciona la interfaz con el sistema telefónico, se describen los componentes acontinuacion:

- El tamaño de la célula es de aproximadamente 35 km.

- La unidad móvil o MS (*Mobile Station*).

- El controlador de estaciones base o BSC (*Base Station Controller*), es un elemento nuevo introducido por GSM. Se encarga de las operaciones de transferencia de control de las llamadas y también de controlar las señales de potencia entre las BTS y las MS, con lo cual releva al centro de conmutación de varias tareas.

- La estación de transmisión, recepción base o BTS (*Base Transceiver Station*), establece la interfaz a la unidad móvil. Está bajo el control del BSC.

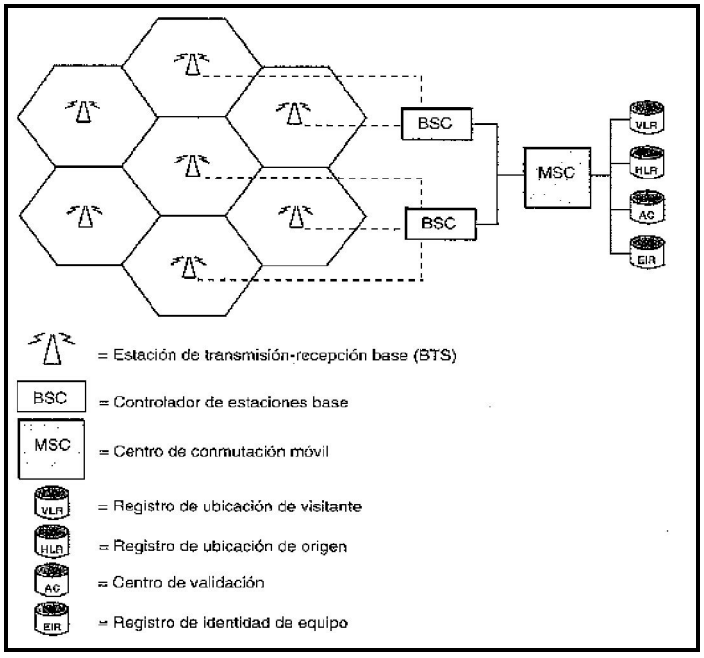
- El registro de localización base o HLR (*Home Location Register*), es una base de datos que proporciona información sobre el usuario, su base de suscripción de origen y los servicios suplementarios que se le proveen.

- El registro de localización del visitante o VLR (*Visitor Location Register*), es también una base de datos que contiene información sobre la situación de encendido y apagado de las estaciones móviles y si se han activado o desactivado de los servicios suplementarios.
- El centro de validación o AC – AUC (*Authentication Center*) sirve para proteger a cada suscriptor contra un acceso no autorizado o contra el uso de un número de suscripción por personas no autorizadas; opera en relación estrecha con el HLR.

1.2.3. Tecnología GSM

El registro de identidad del equipo o EIR (*Equipment Identity Register*), (ver figura 4) sirve para registrar el tipo de equipo que existe en la estación móvil y también puede desempeñar funciones de seguridad como bloqueo de llamadas que se ha determinado que emanan de estaciones móviles robadas, así como evitar que ciertas estaciones que no han sido aprobadas por el proveedor de la red usen ésta.

Figura 4. **Configuración estándar de la tecnología GSM**



Fuente: FORMER CLAVIJO Enric; et al. *Tecnología* GSM. p. 10.

1.2.3.1. Bandas

El interfaz de radio de GSM se ha implementado sobre diferentes bandas de frecuencia, por asuntos legales de disponibilidad de frecuencias no asignadas. En Guatemala las bandas son controladas y administradas por la Superintendencia de Telecomunicaciones, SIT.

Las redes GSM operan en varios rangos de frecuencia de transmisión diferentes (separados en rangos de frecuencia GSM de 2G y bandas de frecuencias del sistema universal de telecomunicaciones móviles o UMTS de 3G), la mayoría de 2G redes GSM operan en la banda de 900 MHz o 1800 MHz. Cuando estas bandas fueron asignados, la de 850 MHz y 1900 se

utilizaron en su lugar (por ejemplo, en Canadá y los Estados Unidos). En algunos casos el 400 y 450 MHz son las bandas de frecuencias asignadas en algunos países, ya que se utilizaron anteriormente para los sistemas de primera generación.

Tabla II. **Descripción de bandas GSM**

Banda	**Nombre**	**Canales**	***Uplink* (MHz)**	***Downlink* (MHz)**	**Notas**
GSM 850	GSM 850	128 – 251	824,0 - 849,0	869,0 - 894,0	Usada en los EE.UU., Sudamérica y Asia
GSM 900	P-GSM 900	1-124	890,0 - 915,0	935,0 - 960,0	La banda con que nació GSM en Europa y la más extendida
	E-GSM 900	975 – 1023	880,0 - 890,0	925,0 - 935,0	E-GSM, extensión de GSM 900
	R-GSM 900	n/a	876,0 - 880,0	921,0 - 925,0	GSM ferroviario (GSM-R)
GSM1900	GSM 1900	512 – 810	1850,0 - 1910,0	1930,0 - 1990,0	Usada en Norteamérica

Fuente: Wikipedia Bandas_de_frecuencia_GSM. Consulta: 1 de agosto de 2008.

Independientemente de la frecuencia seleccionada por un operador (ver tabla II), que divide en ranuras de tiempo o TS para teléfonos individuales de uso. Esto permite ocho canales *full-rate* o dieciséis canales de expresión de la velocidad media por frecuencia de radio. Estas ocho ranuras de tiempo de radio (u ocho períodos de bloques) se agrupan en una trama de acceso múltiple por división de tiempo o TDMA. Los canales Half-rate usan tramas alternas en las mismas ranuras de tiempo. El tipo de canal de datos para los 8 canales es 270 833 kbit/s y la duración de las tramas es 4 615 ms. La potencia de transmisión en los receptores está limitada a 2 vatios en GSM 850/900 y 1 vatio en GSM 1800/1900.

1.2.3.2. Aplicaciones

Las aplicaciones que pueden obtenerse o soportarse en una red GSM son muy variadas, se pueden ver algunos ejemplos a continuacion.

1.2.3.2.1. Acceso a una red GSM

Para poder tener acceso a los servicios GSM, un usuario necesita tres cosas:

- Una relación de facturación con un operador de telefonía móvil: esto es generalmente, que los servicios se pagan por adelantado de los cuales son consumidos (prepago), o una donde las facturas que se emiten y se establecieron después de que el servicio ha sido consumido (postpago).

- Un teléfono móvil: que es GSM compatible y que funcione a la misma frecuencia que el operador. La mayoría de las compañías telefónicas venden los teléfonos de otros fabricantes.

- Una tarjeta SIM (Subscriber Identity Module): la cual es activada por el operador una vez que la relación de facturación se establece. Después de la activación de la tarjeta se programa con el abonado MSISDN (Mobil Subscriber Integrated Services Digital Network Number) (el número de teléfono). La información personal, como números de contacto de los amigos y la familia, también, se pueden almacenar en la tarjeta SIM del abonado.

Después de que el abonado se suscribe, la información acerca de su identidad y los servicios que se le permite con su respectivo acceso, se almacenan en una tarjeta SIM en el registro de localidad o HLR. Una vez que la tarjeta SIM se carga en el teléfono y el teléfono está encendido, el móvil busca la cobertura de señal más cercana en la Base Transceiver Station o BTS.

La característica clave de un teléfono móvil es la capacidad de recibir y realizar llamadas en cualquier área donde la cobertura está disponible. Esto generalmente, se denomina roaming desde la perspectiva del cliente. Cada área geográfica tiene una base de datos llamada Visitor Location Register o VLR, que contiene detalles de todos los teléfonos móviles actualmente en esa zona. Cada vez que un teléfono se conecta, o visita una nueva área, el VLR debe comunicarse con el Home Location Register para obtener los datos para ese teléfono. La cobertura del teléfono se introduce en el registro del VLR y se utilizará durante un proceso llamado paging o de localización, cuando la red GSM desea localizar el teléfono móvil.

Cada tarjeta SIM contiene una clave secreta llamada Ki, que se utiliza para proporcionar servicios de autenticación y cifrado. Esto es útil para prevenir el robo de servicio y también, para evitar que se capte o interfiera por el aire la actividad de un usuario. La red hace esto, utilizando el centro de autenticación y se lleva a cabo sin transmitir directamente la llave. Cada teléfono GSM contiene un identificador único (distinto del número de teléfono), llamado el International Mobile Equipment Identity o IMEI.

1.2.3.2.2. Las llamadas de voz salientes

Una vez que un teléfono móvil se ha unido con éxito a una red GSM, como se describio anteriormente, se pueden realizar llamadas desde el teléfono a cualquier otro dentro de red telefónica pública conmutada o PSTN. El usuario marca el número de teléfono, presiona la tecla de enviar o hablar y el teléfono móvil envía un mensaje de solicitud de establecimiento de llamada a la red de telefonía móvil a través de la radio base o cobertura más cercana (BTS). El establecimiento de llamada hace una petición al centro de conmutación móvil o MSC más cercano, que comprueba el registro del abonado en el registro de localidad de visitante o VLR, para ver si la llamada saliente está permitida. Si es así, entonces el MSC direcciona la llamada de la misma manera que una central telefónica hace en una red fija.

Si el abonado se encuentra plan prepago, se realiza una comprobación adicional para ver si el abonado tiene suficiente crédito para continuar. Si no, la llamada se rechaza. Si la llamada se permite, entonces se hace un seguimiento constante y la cantidad apropiada se disminuye de la cuenta del abonado. Cuando el crédito llegue a cero, la llamada es cortada por la red. Los sistemas que supervisan y proporcionan los servicios de prepago no forman parte de los servicios estándar GSM, sino son un ejemplo de la red inteligente o IN que los operadores de telefonía móvil deciden agregar, además de los que la Norma GSM señala.

1.2.3.2.3. Llamadas de voz entrantes o puerta de enlace de contacto del MSC

Cuando alguien realiza una llamada a un teléfono móvil, marca el número de teléfono o MSISDN asociado con el usuario del teléfono y la llamada se direcciona al operador de telefonía móvil vía la puerta de enlace de conmutación. En la puerta de enlace de conmutación o *Gateway* MSC, como su nombre indica, actúa como la entrada desde las partes exteriores de la red telefónica pública conmutada o PSTN hacia el proveedor de la red.

Como se señaló anteriormente, el teléfono es libre de hacer itinerancia en cualquier lugar de la red del operador o en las redes de socios de *roaming*, incluso en otros países. Así, que el primer trabajo del MSC *Gateway* es determinar la ubicación actual del teléfono móvil con el fin de conectar la llamada. Para ello, consulta al registro de localidad principal o HLR, como ya se describe y sabe a qué registro de localidad de visitante o VLR el teléfono está asociado, si es el caso.

1.2.3.2.4. Enrutamiento de la llamada

Cuando el HLR recibe este mensaje de consulta, determina si la llamada se direcciona a otro número (desvío de llamada), o si es para ser enviado directamente al móvil.

- Si el propietario del teléfono ya ha solicitado que todas las llamadas entrantes se desvíen a otro número, conocido como el desvío de llamada incondicional o CFU (Call Forward Unconditional), este número se almacena en el registro principal de localidad o HLR. Si ese es el caso,

entonces el número de CFU se devuelve a la puerta de enlace MSC inmediata para su desvío respectivo.

- Si el teléfono móvil no está asociado con un registro de localización visitante (ya que el teléfono está apagado), el HLR devuelve un número conocido como el desvío de llamadas no alcanzable o CFNRc a la MSC Gateway y la llamada es enviada allí. Muchos operadores pueden establecer este valor automáticamente al número de teléfono de correo de voz, de modo que los que llaman pueden dejar un mensaje. El teléfono móvil a veces puede anular la configuración predeterminada.

- Por último, si el HLR sabe que el teléfono está en roaming en una determinada área de VLR, entonces va a pedir un número temporal o MSRN al mismo. Este número se retransmite de nuevo a la puerta de enlace de MSC y luego es utilizado para enviar la llamada a la MSC donde el teléfono destino está en roaming.

1.2.3.2.5. Timbre del teléfono

Cuando la llamada llega a la MSC de visita, el MSRN se utiliza para determinara qué teléfono se está llamando. El MSC entonces, hace un anuncio a todas las antenas de telefonía móvil en la zona con el fin de informar al teléfono que hay una llamada entrante para él. Si el abonado responde, un circuito de llamada se cierra a través de la MSC de visita y la puerta de enlace MSC de la red de la persona que efectúa la llamada.

También, es posible que la llamada no se conteste. Si el abonado está ocupado en otra llamada (y llamada en espera no se utiliza) la MSC de visita direcciona la llamada a un pre-determinado número de desvío en ocupado o

CFB. Del mismo modo, si el abonado no contesta la llamada después de un período de tiempo (Normalmente 30 segundos), la MSC de visita desvía la llamada a un pre-determinado número de desvío de llamadas en no respuesta o CFNR. Una vez más, el operador podrá decidir la sustitución de este valor por defecto a los de correo de voz del móvil, para que las personas que llamen puedan dejar un mensaje.

Si el abonado no responde a la solicitud de búsqueda, ya sea por estar fuera de cobertura, o su batería se ha descargado o removido, a continuación la MSC de visita desvía la llamada a un pre-determinado número de desvío de llamadas no es alcanzable o CFNR. Una vez más, el operador podrá decidir la sustitución de este valor por defecto a los de correo de voz del móvil, para las personas que llamen pueden dejar un mensaje.

1.2.3.2.6. La transmisión de datos

El estándar GSM, también, ofrece instalaciones separadas para la transmisión de datos digitales. Esto permite que un teléfono móvil actúe como cualquier otro ordenador de la Internet, enviar y recibir datos a través del protocolo de internet .

El móvil, también, puede ser conectado a un computador portátil o PDA, para su uso como una interfaz de red (como un módem o tarjeta Ethernet, pero usando uno de los protocolos de datos GSM). Algunos teléfonos GSM también pueden ser controlados por un sistema estandarizado de comando AT de Hayes a través de un cable serial o un enlace inalámbrico (con IrDA o Bluetooth). Los comandos AT pueden controlar cualquier cosa desde tonos de llamada a los algoritmos de compresión de datos.

1.2.3.2.7. Circuito de conmutación de protocolos de datos

En una conexión de datos de conmutación de circuitos se reserva una cierta cantidad de ancho de banda entre dos puntos para la conexión, al igual que una llamada telefónica tradicional asigna un canal de audio de una cierta calidad entre dos teléfonos para la duración de la llamada.

Dos protocolos de conmutación de circuitos de datos se definen en la norma GSM: datos por conmutación de circuitos o CSD y alta velocidad de conmutación de circuitos de datos o HSCSD. Estos tipos de conexiones son normalmente cobrados por segundo, independientemente de la cantidad de datos enviados por el enlace. Esto se debe a que una cierta cantidad de ancho de banda se dedica a la conexión, independientemente de si es o no necesario.

Las conexiones por conmutación de circuitos tienen la ventaja de proporcionar un servicio constante, garantizado y con calidad, útil para aplicaciones en tiempo real, como videoconferencia.

1.2.3.2.8. Servicio General de Paquetes de Radio, GPRS

El servicio general de paquetes de radio o GPRS (General Packet Radio Service), es un servicio de conmutación de paquetes de protocolo de transmisión de datos que se incorporó en la Norma GSM en 1997. GPRS hace esto mediante el envío de paquetes al teléfono móvil vía la BTS en los canales no utilizados por las conexiones de conmutación de circuitos o llamadas de voz. Múltiples usuarios pueden compartir un canal de GPRS sin usar porque cada uno de ellos lo utiliza solo por ocasionales en ráfagas cortas.

La ventaja de las conexiones por conmutación de paquetes es que el ancho de banda se utiliza cuando en realidad hay datos a transmitir. Este tipo de conexión es, pues, en general facturado por el lugar de kilobytes por segundo y suele ser una alternativa más barata para las aplicaciones que sólo necesitan enviar y recibir datos de forma esporádica, como la mensajería instantánea.

A continuación se listan algunos servicios de común uso en la tecnología GSM.

- Servicio de mensajes cortos o SMS : mensajes de texto *SMS* pueden ser enviados por usuarios de teléfonos móviles a otros usuarios de móvil o los servicios externos que aceptan SMS. Los mensajes se envían, generalmente, desde dispositivos móviles a través del centro de servicio de mensajes cortos con el protocolo MAP.

- Servicios suplementarios: GSM soporta un amplio conjunto de servicios suplementarios que complementan y apoyan la telefonía y servicios de los datos descritos anteriormente. Todos ellos están definidos en las Normas GSM. Una lista parcial de los servicios complementarios se detalla a continuación.

    - Desvío de llamadas: este servicio le permite al suscriptor la posibilidad de desviar las llamadas entrantes a otro número si la unidad móvil llamada no es alcanzable, si está ocupado, si no recibe una respuesta, o si el desvío de llamadas se concedería de forma incondicional.

- Bloqueo de llamadas salientes: este servicio permite que un abonado móvil deshabilite el servicio para evitar que todas las llamadas salientes sean generadas.

- Restricción de llamadas entrantes: esta función permite al abonado evitar las llamadas entrantes. Las siguientes dos condiciones permiten excluir las llamadas: restringir todas las llamadas entrantes y restricción de llamadas entrantes en *roaming* fuera de la red móvil pública terrestre o PLMN del suscriptor.

- Notificación del importe o AOC: el servicio de AOC proporciona información al abonado móvil con estimación de los gastos de teléfono. Hay dos tipos de información AC: uno que proporciona al abonado con una estimación de la factura y que puede ser usado para los propósitos inmediatos de carga y AC para llamadas de datos, proporciona la base de mediciones de tiempo.

- Llamada en espera: este servicio permite que el abonado pueda interrumpir una llamada en curso y posteriormente, restablecer la llamada. El servicio de llamada en espera sólo es aplicable a la telefonía normal.

- Servicio de conferencia: este permite a un abonado móvil establecer una conversación múltiple, es decir, una conversación simultánea en conferencia entre tres y seis abonados. Este servicio sólo es aplicable a la telefonía normal.

- Identificación, restricción de identificación de llamada: estos servicios proporcionan en una llamada con la red digital de servicios integrados o ISDN, el número de la persona que llama. El servicio de restricción permite a la persona que llama restringir la presentación. La restricción prevalece sobre la presentación.

- Grupos de usuarios cerrados o CUGs: son un grupo de abonados que son capaces de llamarse a sí mismos y sólo determinados números como destino.

- Transferencia de llamadas explícitas o ETC*:* este servicio permite a un usuario que tiene dos llamadas, conectar estas dos llamadas entre sí y liberar sus conexiones con las otras partes.

1.3. Red pública de datos

La información viaja en una red GSM a través de una red pública de datos, que envía y recibe la información desde y para la unidad móvil.

1.3.1. Red de valor agregado

El crecimiento de la telefonía móvil de América Latina y el Caribe, basado primordialmente en servicios prepagos, conlleva una evolución en la maduración de los servicios de voz. Este proceso fuerza a los operadores móviles de América Latina y el Caribe a considerar el lanzamiento de otros servicios, datos especialmente, que viabilicen el crecimiento orgánico de sus ingresos.

El interés en servicios de datos que vive la región está enmarcado en una tendencia global enfocada en fomentar el crecimiento de subscriptores, sin mermar el ingreso promedio por usuario o ARPU. Estudios han identificado los siguientes desarrollos que podrían contribuir a acelerar la adopción de servicios de datos:

- Introducción del servicio en capas sociales desfavorecidas con terminales de baja gama, lo cual impactaría primordialmente en mercados emergentes que están en proceso o han alcanzado el punto de saturación para adopción de servicios básicos de telefonía móvil.

- Incrementar la cobertura del servicio en aquellas áreas con alto número de usuarios en tránsito y con tiempo ocioso, por ejemplo; carreteras; esto debe ser acompañado con una campaña de educación que incite a los consumidores a utilizar servicios de datos.

- Aumentar la cobertura internacional por medio de acuerdos de *roaming* que contemplen los servicios de datos.

- Promover la oferta de servicios de datos a usuarios existentes, para incrementar ingresos y mejorar los niveles de retención de clientes.

Los datos móviles son los servicios que presentan el mayor potencial de crecimiento en el mediano y largo plazo. Además de permitirles a los operadores un aumento del ingreso promedio por usuario o ARPU (*Average Revenue Per User*), los servicios de datos contribuirán a una recuperación más veloz de la inversión para las empresas de telefonía móvil que han desplegado redes de siguiente generación.

Para catalogar la oferta actual de servicios de datos móviles pueden dividirse en tres categorías, basada en la segmentación inicial realizada por la gran mayoría de los operadores a escala mundial y, más cercanamente, en América Latina y el Caribe:

- Conectividad: lanzamiento de redes 2G+ 3G
- Productividad: lanzamiento de aplicaciones para el sector corporativo
- Entretenimiento: lanzamiento de aplicaciones y contenido para las masas

1.3.2. Red *Ethernet*

Ethernet es un estándar de redes de computadoras de área local con acceso al medio por contienda de acceso múltiple, detección de portadora con detección de colisiones o CSMA (Carrier Sense Multiple Access with Collision Detection) esto con dispositivos de red o CD. El nombre viene del concepto físico de ether. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo ISO.

La Ethernet se tomó como base para la redacción del estándar internacional del Instituto de Ingenieros Eléctricos y Electrónicos IEEE 802.3. Usualmente se toman Ethernet e IEEE 802.3 como sinónimos. Ambas se diferencian en uno de los campos de la trama de datos. Las tramas Ethernet e IEEE 802.3 pueden coexistir en la misma red.

1.3.3. Redes de área local o LAN

Los componentes de una red de área local o LAN (Local Area Network) son:

- Sistema operativo u OS (Operation Systems) de la red LAN: por ejemplo: Novell NetWare, UNIX, Appleshare, DECnet, IBM LAN Server, Microsoft Windows NT. El Novell NetWare poseía el 60 por ciento del mercado en USA (en 1993). MS-DOS (Disk Operating System de Microsoft) se ha diseñado con una memoria limitada a 640 kBytes, lo que constituye una seria limitación para la interconexión de PC (networking).

- Servidor: el concepto cliente servidor o client/server se ha introducido en 1987 para ambientes de operación LAN. Este modelo contrasta con el modelo de anfitrión Host (por ejemplo, IBM-3090, 4381 y 9370). El Host es un computador que procesa los datos de varios terminales informáticos en tiempo compartido. El modelo cliente y servidor reparte las funciones centrales en el server y las distribuidas en los clientes. Puede ser un software que trabaja en una PC (servidor no-dedicado) o una PC dedicada a tal efecto. Un server de interés es el de la impresora, trabaja mediante un Spool (SIMultaneous Peripherical Operation On-Line). El Spool es un hardware o software que controla el buffer de memoria para acceso a la impresora. Hay que tener presente que los requerimientos de velocidad se incrementan permanentemente, debido a los servicios multimediales y la industria basada en computadoras. Por ejemplo: el avión Boeing 777 fue el primero diseñado completamente mediante computadoras CAD-CAM.

- Mainframe: en una red se puede conectar una Mainframe, se trata de computadores con más de un procesador central. El Mainframe comparte la carga de trabajo y fueron las primeras computadoras desde 1960. Las funciones del servidor son: administrar la memoria de archivos y el *BACKup* de ellos (file); permite el servicio de comunicación con otros servidores de red y permite el servicio de Email y facsímil electrónico. Por otro lado, administra la presencia de base de datos, de directorios y el uso compartido de la impresora.

- Cliente (Nodos y estaciones de trabajo): se trata de las PC que se conectan a la red y completa el concepto cliente/servidor. Se utiliza como procesador de palabras, para diseño gráfico, base de datos, gestión de proyectos, etc. Muchas veces se utiliza la palabra *Host* para denominar una simple estación de trabajo. En la red Internet cada computadora se denomina Host o Nodo. En otras oportunidades Host se reserva para computadoras que tienen varios usuarios.

- NIC (Network Interface Cards o Network Board): conecta una PC a la red. Cumple funciones de capa 1 para conexión al medio físico de enlace. En una PC convencional se trata de una tarjeta interna al bastidor. Puede usar un conector modular telefónico de 4 pin RJ-11 o de 8 pin RJ-45. En el caso de disponer de una Notebook o Laptop la puerta denominada PCMCIA permite la conexión. PCMCIA (Personal Computer Memory Card International Association) es una interfaz al exterior. Existen 3 tipos:

    - Tipo I (expansión de memoria)
    - Tipo II (adaptador a modem y LAN)
    - Tipo III (conexión a disco duro)

- Hub: permite reunir en un punto los elementos de la red LAN. Se trata de componentes, generalmente, activos (regeneran las señales y tienen funciones de supervisión).

- Bridge: permiten la interconexión de redes LAN o la subdivisión de redes muy grandes. Su función es filtrar los paquetes de datos de acuerdo con la dirección de destino.

- Switch: reealiza funciones de conmutación en una estructura en estrella. Simula un Hub desde el punto de vista topológico, pero conmuta paquetes en lugar de regenerarlos. Hub, Bridge y Switch son elementos internos a una LAN. Router permite la conexión al exterior.

- Router: permite la conexión de una red LAN hacia una red amplia o WAN. Desde el punto de vista del hardware es siempre el mismo, modificándose el software incorporado. Las interfaces de salida dependen de la velocidad a ser utilizada:

    - RS-232 o V24/V.28 para interfaz de 9,6 o 19,2 KB/s hacia redes X.25.
    - V.35 para interfaz de Nx64 KB/s hacia redes Frame Relay.
    - G.703 hacia redes de 2 Mb/s del tipo Frame Relay o ATM.
    - Interfaz óptica para alta velocidad; por ejemplo, STM-1 en ATM o 100/1000 Mb/s en Ethernet.

1.3.4. Red privada virtual o VPN

Una red privada virtual o VPN (Virtual Private Network), es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Ejemplos comunes son, la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo doméstico desde un sitio remoto, como por ejemplo un hotel. Todo ello utilizando la infraestructura de Internet.

1.3.4.1. Medios

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación, integridad y confidencialidad de toda la comunicación:

- Autentificación y autorización: ¿Quién está del otro lado? Usuario, equipo y qué nivel de acceso debe tener.

- Integridad: de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

- Confidencialidad: dado que solo puede ser interpretada por nadie más que los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

- No repudio: es decir, un mensaje tiene que ir firmado, y el que lo firma no puede negar que el mensaje lo envío él.

1.3.4.2. Requerimientos básicos

Identificación de usuario: las VPN deben verificar la identidad de los usuarios y restringir su acceso a aquellos que no se encuentren autorizados.

Codificación de datos: los datos que se van a transmitir a través de la red pública (Internet), antes deben ser cifrados, para que no puedan ser leídos, esta tarea se realiza con algoritmos de cifrado como DES o 3DES que sólo pueden ser leídos por el emisor y receptor. Administración de claves: las VPN deben actualizar las claves de cifrado para los usuarios.

1.3.4.3. Tipos de VPN

Básicamente existen tres arquitecturas de conexión VPN.

- VPN de acceso remoto: es el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autentificados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

- VPN punto a punto: este esquema se utiliza para conectar oficinas remotas con la sede central de la organización. El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía

Internet provenientes de los sitios y establece el túnel VPN. Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicional, sobre todo en las comunicaciones internacionales. Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

- Tunneling (túnel): la técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras. El establecimiento de dicho túnel se implementa incluyendo una PDU determinada dentro de otra PDU con el objetivo de transmitirla desde un extremo al otro del túnel sin que sea necesaria una interpretación intermedia de la PDU encapsulada. De esta manera se encaminan los paquetes de datos sobre nodos intermedios que son incapaces de ver en claro el contenido de dichos paquetes. El túnel queda definido por los puntos extremos y el protocolo de comunicación empleado, que entre otros, podría ser SSH.

  El uso de esta técnica persigue diferentes objetivos, dependiendo del problema que se esté tratando, como por ejemplo la comunicación de islas en escenarios multicast, la redirección de tráfico, etc.

  Uno de los ejemplos más claros de utilización de esta técnica consiste en la redirección de tráfico en escenarios IP móvil. En escenarios de IP móvil, cuando un nodo-móvil no se encuentra en su red base, necesita que su home-agent realice ciertas funciones en su puesto, entre las que se encuentra la de capturar el tráfico dirigido al nodo-móvil y redirigirlo hacia él. Esa redirección del tráfico de paquetes se realiza usando un mecanismo de tunneling, ya que es necesario que los paquetes conserven

su estructura y contenido originales (dirección IP de origen y destino, puertos, etc.) cuando sean recibidos por el nodo-móvil.

- VPN over LAN (red virtual sobre redes locales): este esquema es el menos difundido pero uno de los más poderosos para utilizar dentro de la empresa. Es una variante del tipo acceso remoto pero, en vez de utilizar Internet como medio de conexión, emplea la misma red de área local (LAN) de la empresa. Sirve para aislar zonas y servicios de la red interna. Esta capacidad lo hace muy conveniente para mejorar las prestaciones de seguridad de las redes inalámbricas (WiFi).

  Un ejemplo clásico es un servidor con información sensible, como las nóminas de sueldos, ubicado detrás de un equipo VPN, el cual provee autenticación adicional más el agregado del cifrado, haciendo posible que sólo el personal de recursos humanos habilitado pueda acceder a la información.

  Otro ejemplo, es la conexión a redes WIFI haciendo uso de túneles cifrados IPSEC o SSL, que además de pasar por los métodos de autenticación tradicionales (WAP, WEP, MAC address, etc.) agregan las credenciales de seguridad del túnel VPN creado en la LAN interna.

1.3.4.4. Implementaciones

El protocolo estándar de hecho es el IPSEC, pero también, se tiene el PPTP, L2F, L2TP, SSL/TLS, SSH, etc. Cada uno con sus ventajas y desventajas en cuanto a seguridad, facilidad, mantenimiento y tipos de clientes soportados.

Actualmente, hay una línea de productos en crecimiento relacionada con el protocolo SSL/TLS, que intenta hacer más amigable la configuración y operación de estas soluciones.

- Las soluciones de hardware casi siempre ofrecen mayor rendimiento y facilidad de configuración, aunque no tienen la flexibilidad de las versiones por software. Dentro de esta familia se tiene a los productos de Fortinet, SonicWALL, WatchGuard, Nortel, Cisco, Linksys, Netscreen (Juniper Networks), Symantec, Nokia, U.S. Robotics, D-link, etc.

- Las aplicaciones VPN por software son las más configurables y son ideales cuando surgen problemas de interoperabilidad en los modelos anteriores. Obviamente el rendimiento es menor y la configuración más delicada, porque se suma el sistema operativo y la seguridad del equipo en general. Aquí se tiene por ejemplo a las soluciones nativas de Windows, GNU/Linux y los Unix en general. Por ejemplo: productos de código abierto como OpenSSH, OpenVPN y FreeS/Wan.

  En ambos casos se pueden utilizar soluciones de firewall (barrera de fuego o cortafuego), obteniendo un nivel de seguridad alto por la protección que brinda, en detrimento del rendimiento.

1.3.4.5. Ventajas

- Integridad, confidencialidad y seguridad de datos
- Las VPN reducen los costos y son sencillas de usar
- Facilita la comunicación entre dos usuarios en lugares distantes
- Se utiliza más en campus de universidades

1.3.4.6. Tipos de conexión

- Conexión de acceso remoto: una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

- Conexión VPN router a router (conexión virtual de ruteador a ruteador): una conexión VPN router a router es realizada por un router y éste a su vez se conecta a una red privada. En éste tipo de conexión, los paquetes enviados desde cualquiera de éstos no se originan en los routers. El que realiza la llamada se autentifica ante el que responde y éste a su vez se autentica ante el que realiza la llamada y también sirve para la intranet.

- Conexión VPN firewall a firewall (conexión virtual de cortafuego a cortafuego) una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada. En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet. El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante.

1.3.5. Protocolos de servicio de mensajes cortos sobre GSM

El servicio de mensajes cortos o SMS, es un sistema para enviar y recibir mensajes de texto para y desde teléfonos móviles. El texto puede estar compuesto de palabras o números o una combinación alfanumérica. SMS fue creado como una parte del estándar GSM fase 1. El primer mensaje corto se cree que fue enviado en diciembre de 1992 desde un ordenador personal o PC

a un teléfono móvil a través de la red GSM Vodafone del Reino Unido. Cada mensaje puede tener hasta 160 caracteres cuando se usa el alfabeto latino y 70 caracteres si se usa otro alfabeto como el árabe o el chino.

1.3.5.1. Características

Hay varias características únicas del servicio de mensajes cortos o SMS , según lo definido dentro del estándar digital de telefonía móvil GSM, un mensaje corto puede tener una longitud de hasta 160 caracteres. Esos 160 caracteres pueden ser palabras, números o una combinación alfanumérica.

Los mensajes cortos basados en no texto (por ejemplo, en formato binario), también, se utilizan los mensajes cortos no se envían directamente del remitente al receptor, sino que se envían a través de un centro de SMS. Cada red de telefonía móvil que utiliza SMS tiene uno o más centros de mensajería para manejar los mensajes cortos.

El servicio de mensajes cortos se caracteriza por la confirmación de mensaje de salida. Esto significa que el usuario que envía el mensaje recibe posteriormente otro mensaje notificándole si su mensaje ha sido enviado o no. Los mensajes cortos se pueden enviar y recibir simultáneamente a la voz, datos y llamadas del fax. Esto es posible porque mientras que la voz, los datos y las llamadas del fax asumen el control de un canal de radio dedicado durante la llamada, los mensajes cortos viajan sobre un canal dedicado a señalización independiente de los de tráfico. Hay formas de enviar múltiples mensajes cortos como: la concatenación SMS (que encadena varios mensajes cortos juntos) y la compresión de SMS (que consigue más de 160 caracteres de información dentro de un solo mensaje corto).

1.3.5.2. Tecnología del sistema global de comunicaciones móviles o GSM

Para utilizar el servicio de mensajes cortos los usuarios necesitan la suscripción y el hardware específico:

- Una suscripción a una red de telefonía móvil que soporte SMS.
- Un teléfono móvil que soporte SMS.
- Un destino para enviar o recibir el mensaje, ya sea una máquina de fax, un PC, un terminal móvil o un buzón de e-mail.

1.3.6. Mensajes cortos o SMS como parte de los servicios de valor agregado

Mensajes cortos: (más comúnmente conocido como mensajes de texto) se ha convertido en la aplicación más utilizada de datos en móviles, con un 74 por ciento de todos los usuarios de teléfonos móviles a nivel mundial, ya que la actividad de usuarios de SMS registro 2,4 millones de personas a finales de 2007. En muchos países avanzados, los usuarios han pasado de considerar la llamada de voz siendo la característica más deseada de un teléfono móvil, a considerar los mensajes de texto SMS, como la característica más deseada. Este servicio llega a ser uno del los pioneros en servicios de valor agregado, abriendo posibilidades de aplicaciones, descargas, distintos esquemas de cobro y aplicaciones costo efectivas.

El SMS C es una central de enrutamiento de mensajes cortos. Muchos operadores de servicios móviles utilizan su SMSCs como vías de acceso a sistemas externos, incluida la Internet, SMS entrantes de alimentación de noticias y otros operadores de telefonía móvil (a menudo con el estándar SMPP para el intercambio de SMS).

1.3.7. Descripción del mensaje de texto

Un mensaje de texto se refiere a caracteres trasmitidos en una red, que codifican el mensaje desde el origen hasta el destino.

1.3.7.1. Data grama de SMS como comunicación de datos

Hay 2 formas de tratar los mensajes SMS que son:

- Modo texto
- Modo PDU (Protocol Description Unit)

El modo PDU trata el SMS como una cadena de caracteres en octetos hexadecimales u semioctetos decimales, de cuya codificación resulta el SMS en modo texto. La ventaja de modo PDU respecto al modo texto es que en modo texto la aplicación queda limitada a la opción de codificación que se haya preestablecido, en modo PDU se puede implementar cualquier codificación. La cadena PDU no sólo contiene el mensaje, sino que lleva información del centro de servicio SMS (AT+CSCA), hora de llegada, tipo de mensaje, información sobre el que envía el SMS, vigencia del SMS, número de caracteres del SMS, tipo de llamada (nacional o internacional), tipo de alfabeto usado.

1.3.7.2. Estructura de los SMS en formato PDU

A continuación en las tablas III y IV se describen los SMS de acuerdo a su estructura.

Tabla III. **Estructura de encabezado SMS**

DCS	TIPO PDU	DD	PID	NR	COD	PV	LD	DATOS

Fuente: ETSI GSM 03.40 y GSM 03.38. p. 8.

Tabla IV. **DCS dirección centro de servicio**

LNº	TLL	Nº C S

LNº: longitud número centro servicio. Nº de octetos (pares de caracteres hexadecimales o decimales) que forman el nº del centro de servicio más 1 octeto que indica tipo de llamada nacional o internacional. Si en este campo se pone 00 se toma automáticamente el valor del nº del centro de servicio (dado por at+csca)

TLL: tipo de llamada:
-nacional: 81
-internacional: 91

Nº C S: nº centro de servicio. (Se pondrá el número del centro de servicio que se utiliza, invirtiendo el orden por pares, por ejemplo: 674562345 se pondría 7654325F4, la F se pone cuando la longitud del número es impar).Ejemplo:0791437654325F4 (llamada con prefijo internacional al nº +34674562345)

Fuente: ETSI GSM 03.40 y GSM 03.38. p. 8.

Tabla V. **Tipo PDU tipo protocolo de la unidad de datos**

PC	CD	PRE	PV	RD	TIPO
PC: Path contestación (0 No, 1 Sí)					
CD: Cabecera datos (0 Sin, 1 Con)					
PRE: Petición reporte de estado (0 No, 1 Sí)					
PV: campo período vigencia presente (0 0 No, 01 Reservado, Sí como entero, Sí como semiocteto)					
RD: permite que el centro de SMS acepte un SMS -SUBMIT para un mensaje que todavía está en el centro. (0 Sí, 1 No)					
TIPO: 0 1 Mensaje de envío					

Fuente: ETSI GSM 03.40 y GSM 03.38. p. 9.

DD o Dirección destino. Se rellenará igual que el campo Dirección centro de servicio, poniendo el nº de teléfono del destinatario del SMS . En el campo longitud nº se contarán por semioctetos sin contar la F en caso de que haya habido que ponerla. (ver Tablas III, IV y V)

Ejemplo: nº 34676543524(11=0B semioctetos) en el campo DD será 0B914376563425F4).

PID: identificación de Protocolo usualmente puesto a “00”
NR: número de referencia
COD: codificación trama de datos

Tabla VI. **Codificación trama de datos**

Indica el alfabeto con el que se codifica la trama (alfabeto por defecto= codificación a 7 bits o codificación a 8 bits) e indica tipo de SMS .

0000	**0**	**0**	**00**	Alfabeto a 7 bits
1111	**0**			
		0		7 bits
		1		8 bits
			00	Mensaje clase 0 (se muestra en la pantalla inmediatamente)
			01	Mensaje clase 1 ME
			10	Mensaje clase 2 SIM
			11	Mensaje clase 3 TE

Fuente: ETSI GSM 03.40 y GSM 03.38. p. 9.

Tabla VII. **PV: período de vigencia del SMS**

Valor de PV:

0 a 143	(PV+1)*5 minutos
144 a 167	12horas+(PV-143)*30 minutos
168 a 196	(PV-1) *1 día
197 a 255	(PV-192)*1 semana
Ejemplo_AA:	(AA=170-> 170-166=4 * 1 día=4 días)

Fuente: ETSI GSM 03.40 y GSM 03.38. p. 10.

Tabla VIII. **LD: longitud de la cadena de datos**

	Ejemplo: si el mensaje está formado por la siguiente cadena **C8 27 33 08** El campo **LD** se rellenará con 04 (ya que hay 4 octetos= 2 caracteres hexadecimal)

Fuente: ETSI GSM 03.40 y GSM 03.38. p. 10.

Datos: para explicar la codificación a 7 BITS (ver tablas VI, VII, y VIII) se usará un ejemplo. Codificación de la palabra hola (ver tabla IX):

Tabla IX. **Codificación de trama de datos ejemplo 1**

	H	**O**	**L**	**A**
Hex	48	4F	4C	41
Bin	1001000	1001111	1001100	1000001

Para transformarlo a octetos, se toma el número de caracteres de la siguiente letra que falten para llegar a 8, cuando se hayan tomado caracteres de una letra para la anterior, ésta se queda sin esos caracteres y los debe tomar de la siguiente letra

1 1001000	00 100111 1	001 10011 00	1000 001
C8	27	33	08

Fuente: ETSI GSM 03.40 y GSM 03.38 p. 11.

Ejemplo: envío SMS en formato PDU. Envío de un SMS con la palabra alarma (ver tabla X).

Tabla X. **Codificación de trama de datos ejemplo 2**

	A	**L**	**A**	**R**	**M**	**A**
Hex	41	4C	41	52	4D	41
Bin	1000001	1001100	1000001	1010010	1001101	1000001
	01000001	01100110	01010000 01	11011010 010	00001100 1101	1000001
	41	66	50	DA	0C	02

Fuente: ETSI GSM 03.40 y GSM 03.38. p. 11.

1.3.8. Mensajes cortos punto a punto o SMPP

SMPP es un protocolo open source, lo que podría llamarse una especie de estándar en la industria, desarrollado con la intención de proveer la flexibilidad de una interface en la comunicación de datos para transferir mensajes cortos entre ESME (entidades externas de mensajes cortos), RE (entidades de ruteo) y MC (centros de mensajes).

Centro de mensajes (MC o SMSC): término genéricamente usado para la descripción de sistemas como un SMSC (centro de servicio de mensajes cortos), GSM Unstructured Supplementary Services Data o USSD, Server, o Cell Broadcast Centre (CBC).

Entidades de ruteo (RE): término general para cualquier elemento de red que es utilizado por un MC para más MC, y para encaminar ESMEs hacia MC. Un RE tiene la capacidad de emular funcionalidad asociada con un MC y un ESME. Para un ESME, una RE aparecerá como un MC y para un MC, un RE aparentará ser un ESME. Un proveedor de telefonía móvil puede utilizar REs para ocultar un MC en la red, presentando solo las REs como interfaces de punto externas para ESMEs.

1.3.8.1. Definición de una entidad externa de mensaje corto o ESME

Las entidades externas de mensajes cortos o ESME (External Short Message Entities) representan típicamente a un cliente de sistema de mensajes cortos o SMS configurado en la red, tal como lo sería un WAP Proxy Server, un puerta de enlace para el correo, o bien un servidor de voice mail. Un ESME, también puede representar una entidad célula del broadcast (CBE -- Cell Broadcast Entity).

1.3.8.1.1. Aplicación

Dentro de lo que es el orden de uso de SMPP, una sesión SMPP deberá de ser establecida entre el ESME y el MC o la RE SMPP donde ésta sea apropiada. La sesión establecida será basada sobre una capa de aplicación TCP/IP o una conexión X.25 entre el ESME y el MC/RE, inicialmente convocada por el ESME.

Se presentan las 3 formas de inicializar una sesión con un ESME:

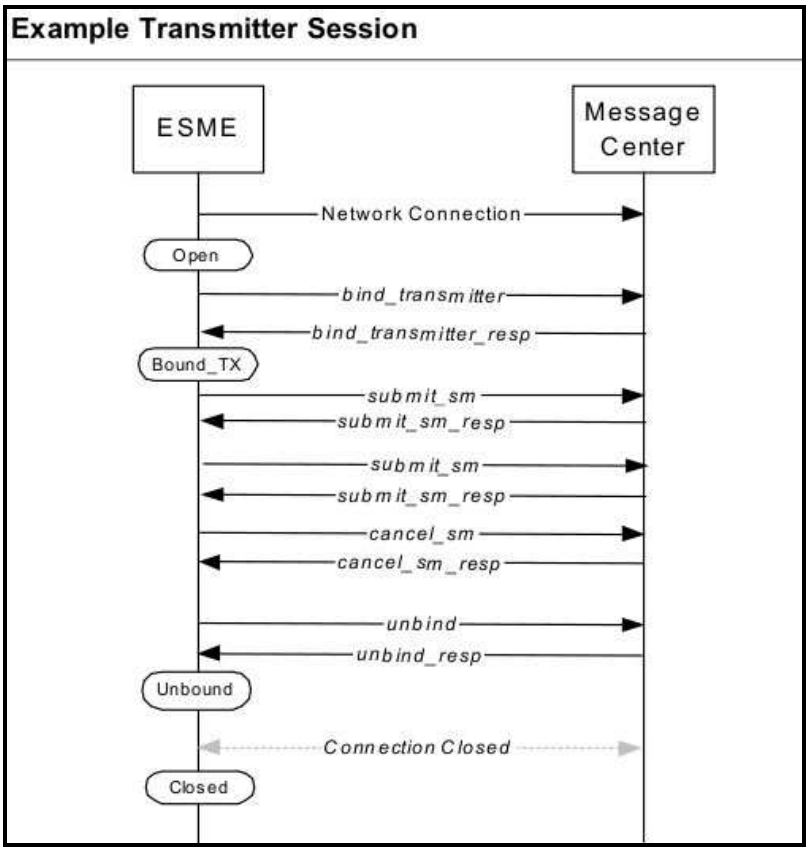
- Trasmisor (TX): cuando se está autentificado como un TX, un ESME puede disparar mensajes cortos hacia el MC para que éste haga entrega a las estaciones móviles (MS - Mobil Stations). Una sesión TX, también permitirá a un ESME. cancelar, consultar o remplazar previamente los mensajes mandados. Los mensajes mandados en TX a menudo son llamados mensajes de terminación en móviles.

- Receptor (RX): una sesión de RX permite a un ESME recibir mensajes que vienen de una MC. Estos mensajes son típicamente originados de estaciones móviles y son conocidos como mensajes que originan los móviles.

- Transceiver (TRX): una sesión TRX es la combinación de TX y RX, esto permite que una sesión sencilla de SMPP sea usada para disparar mensajes hacia un móvil y recibir los mensajes originados por el móvil. Adicionalmente, El MC puede establecer una sesión SMPP para conectar al ESME. A esto se le conoce como una Sesión de Enlace hacia el exterior.

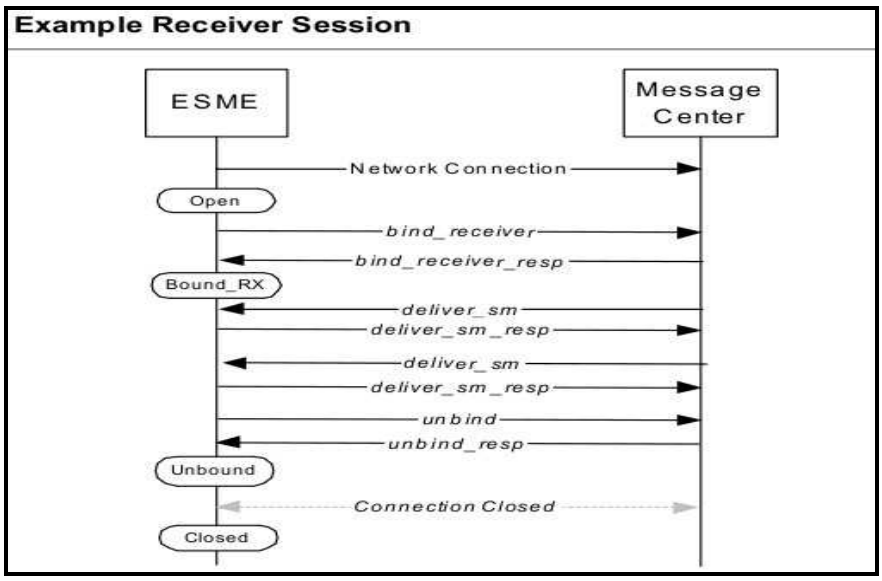
Con fines explicativos, se ilustran las operaciones SMPP y sus estados relativos. A continuación se ilustran casos típicos para 3 tipos de ESME (ver figuras 5, 6 y 7).

Figura 5. **Ejemplo de sesión de transmisión**



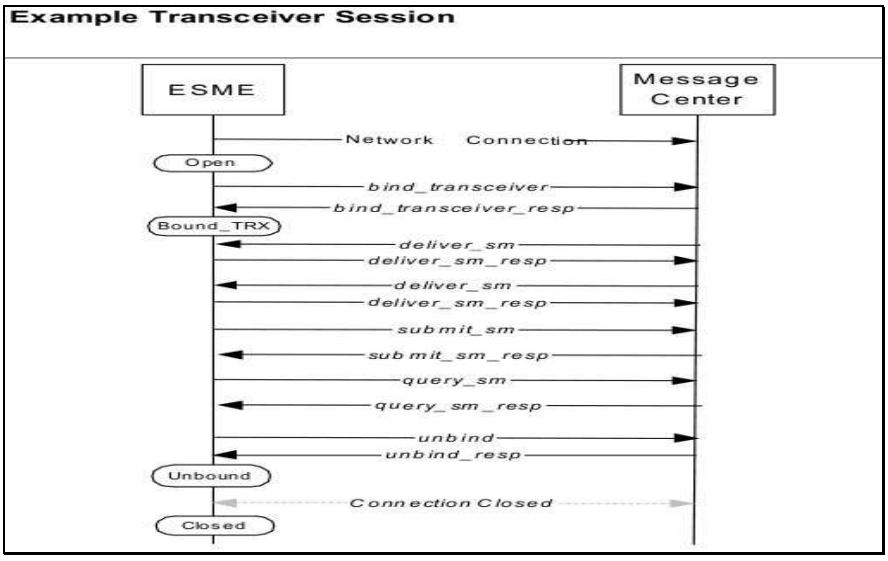
Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4 . p. 6.

Figura 6. **Ejemplo de sesión de recepción**



Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 7.

Figura 7. **Ejemplo de sesión de transcepción**



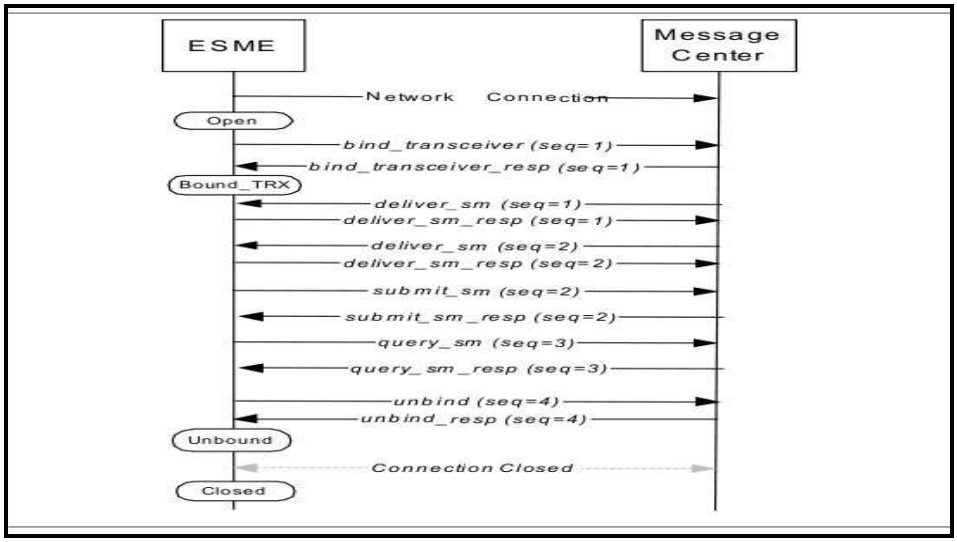
Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 7.

1.3.8.1.2. Detalle de protocolo SMPP

- Secuencia PDU: hasta este momento, se ha hecho referencia a los PDUs por nombre, indicando los pares solicitud/respuesta en forma de datagramas de sesión. La impresión que se podría estar formando es, que SMPP es una especie de protocolo de intercambio (handshake) donde cada solicitud es primero reconocida antes de la siguiente solicitud, este no es el caso, en un protocolo orientado a sesión.

- Número de secuencia PDU: cada PDU de solicitud SMPP posee un identificador llamado número de secuencia (ver figura 8) que será usado, únicamente para la identificación de el PDU dentro del contexto, este número de secuencia lo estará generando la entidad y la actual sesión SMPP. La respuesta PDU resultante (la cual debe de regresar sobre la misma sesión SMPP) es esperada para reflejar el número de secuencia de la solicitud original. El siguiente diagrama ilustra el uso de los números de secuencia.

Figura 8. **Uso de números de secuencia**



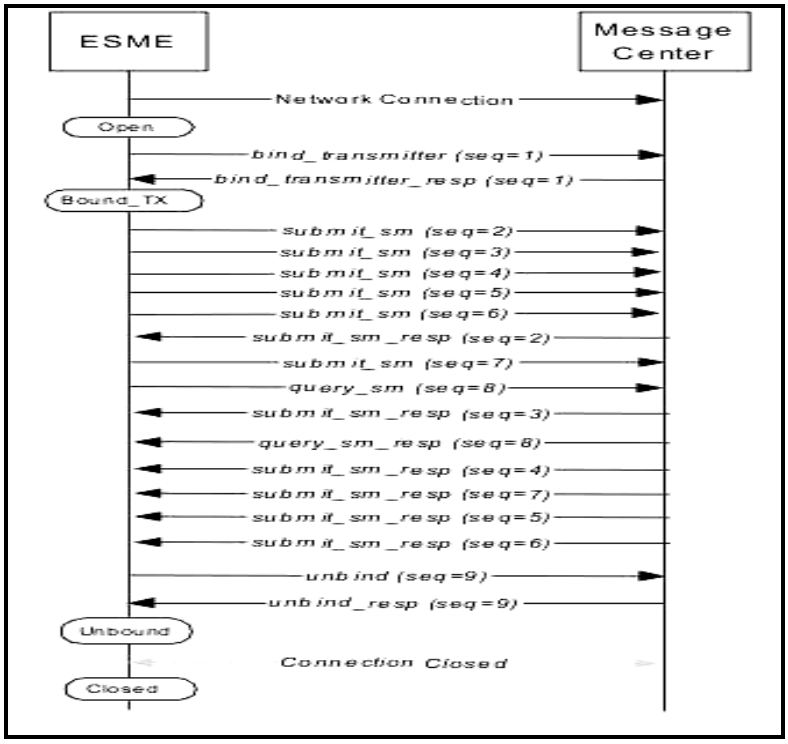
Fuente:Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 8.

En el ejemplo mostrado en la figura 8, los números de secuencia son únicamente publicados por la solicitud PDU. Cada solicitud PDU (PDU request) deberá usar un número de secuencia diferente. Lo recomendado es usar el incremento monótono, iniciando de 1 luego usar 2 y así sucesivamente. Cada respuesta PDU deberá traer consigo el número de secuencia usado durante la solicitud.

1.3.8.1.3. Síncrono vs asíncrono

SMPP es un protocolo asíncrono, esto permite que un ESME o un MC puedan mandar solicitudes a la vez que la otra parte lo hace (ver figura 9). Aquí es cuando el número de secuencia PDU juega un papel crítico, en el rol de soportar la naturaleza asíncrona de SMPP. Todos los ejemplos anteriores que se mostraron han sido síncronos. A continuación se muestra un ejemplo de sesión asíncrona.

Figura 9. **Conexión asíncrona de SMPP**



Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 9.

SMPP tiene una naturaleza asíncrona, este puede mandar varios PDU, sin tener que esperar una respuesta del primero que mandó.

Para asegurar el intercambio eficiente de transacciones SMPP, se recomienda que cada sesión SMPP esté administrada usando relojes configurables en ambos actores que interviene en la comunicación ESME y SMSC.

Los relojes relacionados, pueden incluir:

- Reloj de iniciación para una SMPP: asegura que cuando un ESME inicializa una sesión SMPP, que ésta ocurra dentro de un período específico después de abrir una conexión de red hacia el SMSC.

- Reloj de sesión SMPP: habilita cualquier solicitud ESME o SMSC, el estatus de la sesión SMPP de la otra entidad SMPP se está comunicando vía el comando enquire link.

- Reloj de inactividad SMPP: especifica el máximo período de tiempo para reaccionar. Si los mensajes SMPP no son intercambiados, la sesión SMPP podría ser terminada.

- Reloj de transacción SMPP: especifica el lapso de tiempo permitido entre una solicitud SMPP y la correspondiente respuesta SMPP.

SMPP ofrece la opción de modos de mensaje, la cual si es soportada sobre el SMSC, permite al ESME seleccionar el mecanismo de envío. Típicamente los mecanismos de envío ofrecidos por un SMSC son:

- Modo almacenamiento y reenvío (utilizado por el SME)
- Modo datagrama
- Modo de transacción

Convencionalmente los mensajes cortos son almacenados sobre un SMSC antes de pasar a ser enviados a un recipiente SME. Con este modelo, el mensaje faltante, seguramente almacenado, en caso de que esto significara

que todas las entregas fueron hechas por el SMSC. A esta forma de manejar los mensajes se le conoce comúnmente como almacenaje y reenvío.

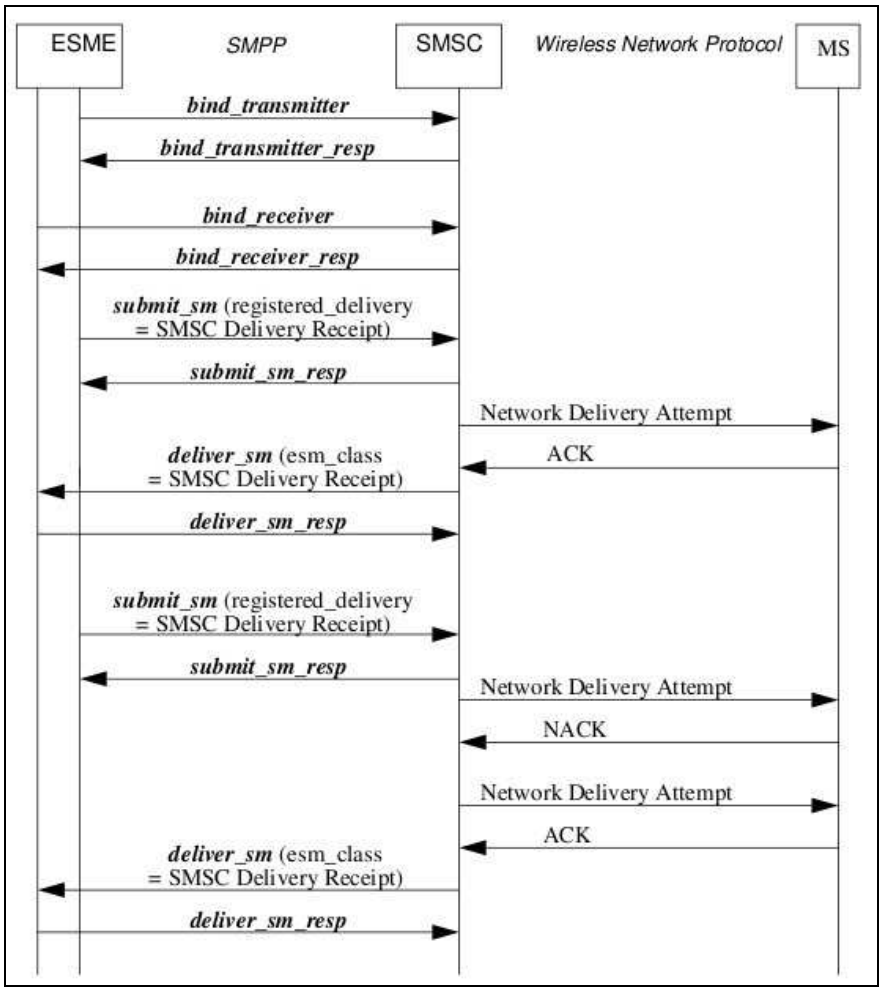
SMPP soporta el mecanismo de envío almacenaje y reenvío vía la operación submit_sm, la cual permite al ESME mandar un mensaje hacia el SMSC donde éste es almacenado, si no es así la razón será que fue exitosamente enviado o significa que el período de validación del mensaje ha expirado. El modo almacenaje y reenvío también está soportado vía la operación data_sm.

El modo de mensaje almacenaje y reenvío, también, facilita operaciones SMPP subsecuentes sobre el mensaje corto almacenado, tal como query_sm, replace_sm y cancel_sm. El PDU submit_sm también facilita funcionalmente el remplazo-si-esta-presente, lo cual requiere que el mensaje original se encuentre almacenado sobre el SMSC.

Eventualmente, para determinar la salida de un mensaje corto enviado, el ESME deberá solicitar dentro de la operación submit_sm o data_sm un recipiente de envío SMSC.

La figura 10 ilustra el flujo para almacenar y reenviar mensaje donde el ESME está funcionando como un transmisor y como un receptor. El ESME solicitó un recipiente de envío SMSC.

Figura 10. **Flujo de almacenar y reenviar mensajes**



Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 10.

Tabla XI. **Tipos de PDU SMPP y definiciones de formato**

Nombre del PDU SMPP	Descripción
Integer	Un valor sin signo con el número de octetos (bytes) definidos. Los octetos siempre habrán transmitido primero MSB (Big Endian).
C-Octet String	Definido como una serie de caracteres ASCII que finalizan con el carácter NULO.
C-Octet String(Decimal)	Definido como una serie de caracteres ASCII, cada carácter representando un digito decimal (0 - 9) y finalizados con el carácter NULO.
C-Octet String(Hex)	Definido como una serie de caracteres ASCII, cada carácter representando un digito hexadecimal (0 - F) y finalizados con el carácter NULO.
Octet String	Definido como una serie de octetos (bytes), y que no necesariamente finalizan con carácter NULO.

Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 10.

De la tabla XI se puede resaltar:

- Referencia realizada a parámetros nulo de campos *Octet-String*, implica que esos campos consisten de un carácter nulo, por ejemplo, un octeto codificado con valor 0x00 (cero) (ver tabla XI).

- Donde la referencia hecha a parámetros NULO de campos Integer, eso implicará que el campo sea llenado a cero.

- En el caso de todos los formatos de C-Octet String, el tamaño máximo de campo es mostrado con una combinación de la longitud del String y el carácter de terminación nulo (ver tabla XII), por ejemplo, un C-Octet String de 8 caracteres, será codificado en 9 octetos cuando el carácter nulo está incluido.

Tabla XII. **Medida del campo de parámetro SMPP**

Medida en octetos	Tipo	Descripción del tipo de cadena especificada
4	Integer	Medida del campo integer ajustada. Sobre este ejemplo el integer es del tamaño de bits (4 octetos)
Var 0 - 254	Octet String	Campo octeto string de medida variable. En este ejemplo el tamaño del campo oct string variara de 0 a 254 octetos.
Var Max 16	C-Octet String	Este string es de longitud variable, de 1 a 15 caracteres ASCII, seguidos de un octe que contendrá el carácter de terminación NULO. Un string vacio es codificado con un simple octeto que contiene el carácter de terminación NULO (0x00).
Ajustado 1 o 17	▪ ▪ C-Octet String	Este string tiene 2 posibles longitudes: Un octeto albergando el carácter NULO O un número ajustado de caracteres terminado con el carácter NULO (en este Ejemplo vea 16 caracteres más el carácter NULO).

Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 10.

El formato general de un PDU SMPP consiste de un encabezado (PDU header), seguido de un cuerpo (PDU body) (ver tabla XIII). El encabezado es una parte obligatoria de cada PDU SMPP y deberá estar siempre presente. El cuerpo es una parte opcional y puede no ser incluida con cada PDU SMPP.

Tabla XIII. **Formato PDU SMPP**

SMPP PDU				
PDU Header (mandatory)				**PDU Body (Optional)**
command length	*command id*	*command status*	*sequence number*	*PDU Body*
4 octets	Length = (Command Length value - 4) octets			

Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 11.

Tabla XIV. **PDU SMPP por partes**

Campo PDU SMPP	Medida en Octetos	Tipo	Descripción
ENCABEZADO			
command_length	4	Integer	El campo command_length define la longitud en octetos de un paquete PDU SMPP incluyendo la longitud del campo.
command_id	4	Integer	El campo command_id identifica el PDU SMPP del que se trata en particular, por ejemplo., submit_sm, query_sm, etc. Solo un identificador de comando es almacenado para cada solicitud SMPP. Este identificador se encuentran en el rango de: 0x00000000 a 0x000001FF. Solo un identificador de comando es también almacenado para cada respuesta SMPP.SMPP. Este identificador se encuentran en el rango de: 0x80000000 to 0x800001FF. (Nota una respuesta SMPP command_id es
command_status	4	Integer	El campo command_status indica el éxito o falla de una solicitud SMPP. Eso será solo relevante dentro del PDU SMPP de respuesta y deberá contener un valor NULO
sequence_number	4	Integer	Este campo contiene un número de secuencia que permitirá a las solicitudes y respuestas, ser asociadas en correlación a sus propósitos. El uso de números de secuencia para correlación de mensaje, permite a los SMPP PDUs el ser intercambiado asíncronamente. La asignación del sequence_number es responsabilidad de la parte que origina el PDU SMPP. El sequence_number deberá ser incrementado monótonamente para cada solicitud PDU SMPP introducida, debe ser
CUERPO			
Parámetros Obligatorios	var	mezclados	Una lista de parámetros de carácter obligatorio correspondientes al PDU SMPP definido en el campo command_id.
Parámetros Opcionales	var	mezclados	Una lista opcional de parámetros al PDU SMPP definido en el campo command_id field como sea requerido.

Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 13.

Nota: Algunos PDU SMPP pueden tener sólo una parte, por ejemplo, el enquire_link PDU.

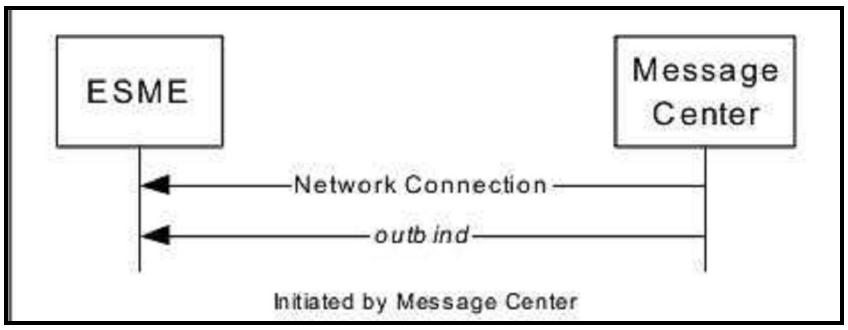
El campo command_length que inicia el encabezado PDU SMPP, indica el número total de octetos contenidos en ese PDU SMPP. El campo command_length contiene un integer de 4 octetos transmitido en formato Big Endian. Para decodificar un PDU SMPP, el ESME o SMSC deberán leer primero el campo command_length (de 4 octetos) para determinar la longitud del PDU (ver tabla XIV).

1.3.8.1.4. Descripción de la sesión SMPP

Una sesión SMPP entre un SMSC y un ESME es iniciada por el ESME, estableciendo una conexión de red con el SMSC que le mandará al ESME una respuesta a su solicitud de enlace (bind request), para que la sesión SMPP sea abierta. Un ESME que desee mandar y recibir mensajes requiere estables dos conexiones de red (TCP/IP o X.25) y dos sesiones SMPP (transmisión y recepción). Alternativamente, sobre esta versión del protocolo un ESME tiene la posibilidad de establecer una sesión SMPP Transceiver sobre una única conexión de red. Durante una sesión SMPP, un ESME posiblemente realice una serie de solicitudes hacia el SMSC, mismas que éste responderá. La sesión SMPP puede ser definida en términos de los siguientes posibles estados:

- Closed (fuera de límite y desconectado): estado proveniente del SMSC que indica una conexión de red cerrada. El SMSC puede, también terminar la conexión que viene del ESME. Un ejemplo claro de ello se puede ver en la figura 11.

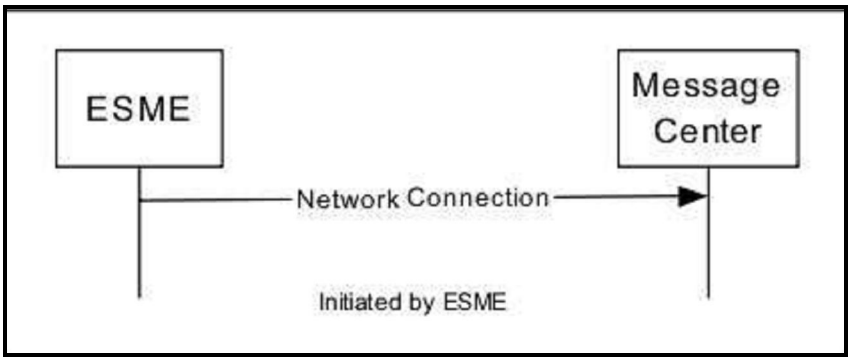
Figura 11. **Conexión de red cerrada**



Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 3.

- Open (conectado y enlace pendiente): un ESME tiene establecido una conexión de red hacia el SMSC pero éste aún no responde. (ver figura 11 y 12)

Figura 12. **Conexión abierta**

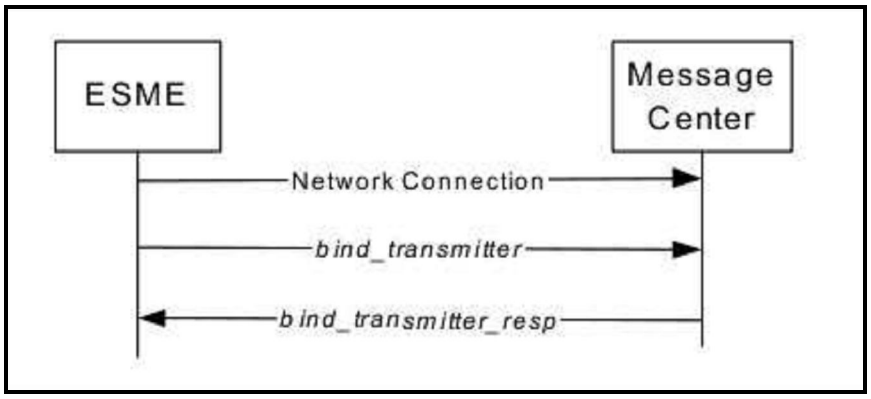


Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 3.

- BOUND_TX: un ESME conectado tiene que solicitar al enlace como un ESME transmisor (a razón de usar un PDU bind_transmitter) y tendrá que haber recibido una respuesta del SMSC autorizando la solicitud de enlace.

Un ESME limitado como un transmisor podrá mandar mensajes cortos hacia un SMSC, para que éste los envíe a una estación móvil o a otro ESME. El ESME puede también remplazar, consultar o cancelar previo mensaje corto introducido. (Ver figura 13)

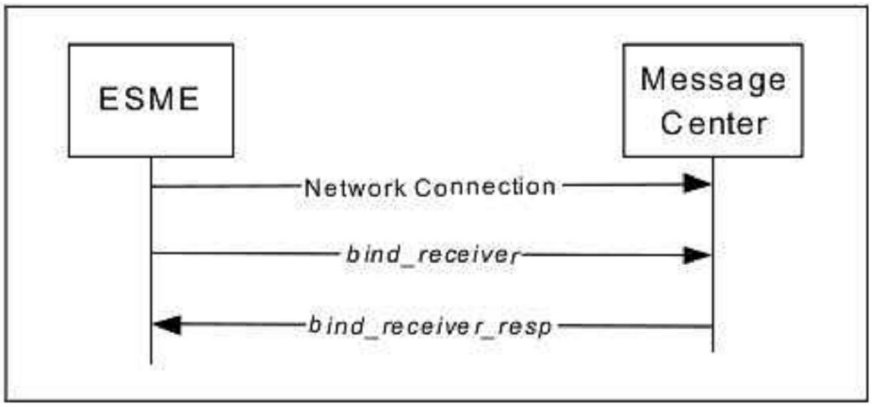
Figura 13. **Inicio de sesión Tx**



Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 3.

- BOUND_RX: un ESME conectado tuvo que haber solicitado conexión como un ESME Receiver (por usar un PDU bind_receiver) y habrá tenido que haber recibido una respuesta proveniente de el SMSC autorizando esta solicitud de enlace (Bind request). Un ESME limitado como receptor podrá recibir mensajes cortos provenientes de un SMSC los cuales pueden ser originados por una estación móvil, por otro ESME o por el centro de mensajes mismo. (Ver figura 14)

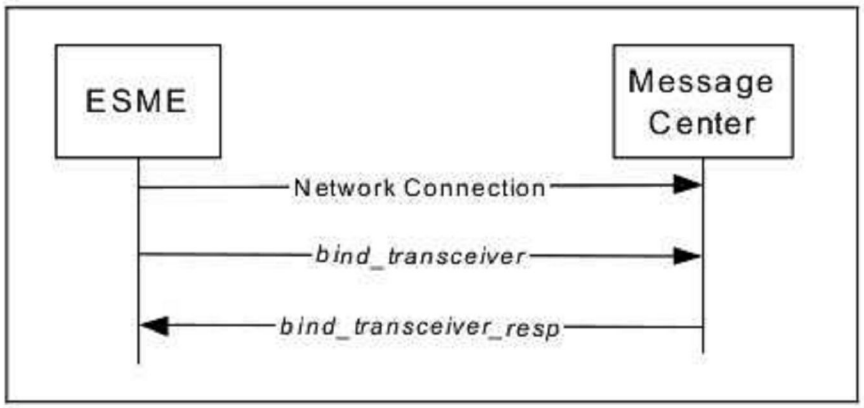
Figura 14. **Inicio de sesión RX**



Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 3.

- BOUND_TRX: un ESME conectado tuvo que haber solicitado conexión como un ESME Transceiver (por usar un PDU bind_transceiver) y tendrá que haber recibido una respuesta proveniente del SMSC autorizando esta solicitud de enlace (Bind request). Un ESME limitado como Transceiver soporta el completo conjunto de operaciones soportadas por Transmitter ESME y un receptor ESME. Un ESME limitado como transceiver podrá mandar mensajes cortos a un SMSC para que éste los envíe a una estación móvil o a otro ESME. El ESME podrá también recibir mensajes cortos que provengan de un SMSC los cuales pudieron ser originados por una estación móvil, por otro ESME o por el SMSC mismo. Como se muestra en la figura 15.

Figura 15. **Inicio de sesión TRX**



Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 4.

- Operación de protocolo y las PDUs: el protocolo SMPP es básicamente un conglomerado de operaciones, cada una tomando la forma de una solicitud y una respuesta PDU.

  Por ejemplo, si un ESME desea disparar un mensaje corto, el ESME puede mandar un submit_sm PDU hacia el MC. El MC responderá con un submit_sm_resp PDU, indicando el éxito o la falla de la solicitud. De cierta manera, si un MC desea enviar un mensaje hacia un ESME, el MC puede mandar un deliver_sm PDU hacia un ESME, el ESME al recibirlo responderá un deliver_sm_resp PDU como una forma de reconocer el envío. Ciertas operaciones son específicas para un ESME con otros específicos para el MC. Otras pueden ser específicas para lograr un tipo de sesión en particular. Un ESME puede mandar un submit_sm hacia un MC, sólo si este tiene establecido una sesión TX o TRX con su MC. Obedeciendo a lo anterior, un MC puede mandar deliver_sm PDUs sólo a ESMEs que tengan establecidas sus sesiones a RX o TRX.

Las operaciones son comúnmente categorizadas dentro de los siguientes grupos:

- Administradoras de sesiones: operaciones asignadas para permitir establecer sesiones SMPP entre un ESME y MC y proporcionar lo necesario para el manejo de errores inesperados. (Ver tabla XV).

- De mensajes introducidos: operaciones asignadas específicamente para el envío de mensajes provenientes de los ESME(s) hacia el MC. (Ver tabla XVI).

- De mensajes enviados: operaciones que permiten al MC enviar mensajes al ESME (ver tabla XVII).

- Mensajes de Broadcast: operaciones que proveen servicio de célula de Broadcast dentro de un MC.

- Operaciones varias: operaciones que proveen características reforzadas tales como la cancelación, consulta o reemplazo de mensajes.

Tabla XV. **Operación administradora de sesiones**

Nombre PDU SMPP	Descripción	Estado de sesión	Ofrecido por	Ofrecido por SMSC
bind_transmitter	PDU de autentificación usado por un TX ESME para enlazar al MC. El PDU contiene información de identificación y un password de acceso para el ESME	OPEN	Si	No
bind_transmitter_resp	MC responde al PDU bind_transmitter. Este PDU indica el éxito o falla de el ESMEs tentativo a enlazar como un transmisor	OPEN	No	Si
bind_receiver	PDU de autentificación usado por un RX para enlazar al MC. El PDU contiene información de identificación, un password de acceso para el ESME y puede también contener información de enrutador, especificando el rango de direcciones a las cuales se brinda el servicio por el ESME	OPEN	Si	No
bind_receiver_resp	MC responde al PDU bind_receiver. Este PDU indica el éxito o falla de el ESMEs tentativo a enlazar como un receptor	OPEN	No	Si
bind_transceiver	PDU de autentificación usado por un RTX ESME para enlazar al MC. El PDU contiene información de identificación, un password de acceso para el ESME y puede también contener información de enrutador, especificando el rango de direcciones a las cuales se brinda el servicio por el ESME.	OPEN	Si	No
bind_transceiver_resp	MC responde a un PDU bind_transceiver. Este PDU indica el éxito o fracaso del enlace del ESME tentativo como un transceiver.	OPEN	No	Si
outbind	PDU de Autentificación usado por un MC para enlazar desde fuera a un ESME que informará a éste qué mensajes están presentes en el MC. El PDU contiene identificación, un password de acceso para el ESME Si el ESME autentifica la solicitud, este responderá con un bind_receiver o bind_transceiver para iniciar el proceso de enlazamiento dentro del MC.	OPEN	No	Si
unbind	Este PDU puede ser mandado por el ESME o MC como un mecanismo de terminación de la sesión SMPP.	BOUND_TX BOUND_RX BOUND_TRX	Si	Si
unbind_resp	Este PDU puede ser mandado por el ESME o el MC como un mecanismo de reconocimiento a la recepción de una solicitud unbind. A posteriori De mandar este PDU el MC por lo general cerrara la conexion de red.	BOUND_TX BOUND_TRX	Si	Si
enquire_link	Este PDU puede ser mandado por el ESME o el MC, solo para probar la conexion de red.	BOUND_TX BOUND_RX BOUND_TRX	Si	Si
enquire_link_resp	Este PDU se uso para el reconocimiento de una solicitud enquire_link que fue enviada por un ESME o MC.	BOUND_TX BOUND_RX BOUND_TRX	Si	Si
alert_notification	Un MC manda alert_notification a un ESME como un mecanismo de alertamiento para verificar la disponibilidad de un SME.	BOUND_RX	No	Yes
generic_nack	Este PDU puede ser mandado por un ESME o un MC como una manera de indicar la recepción de un PDU invalido. Con base e un criterio de su medida o contenido.	BOUND_TX BOUND_RX BOUND_TRX	Si	Si

Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 14.

Tabla XVI. **Operaciones de mensajes introducidos (*submit*)**

Nombre PDU SMPP	Descripción	Estado de sesión requerid	Ofrecido por ESME	Ofrecido por SMSC
submit_sm	Un ESMEtransmisor o transceiver, que desea ingresar un mensaje corto, puede usar este PDU para Especificar el remitente, destinatario y texto del mensaje corto. Otros atributos incluirían la prioridad del mensaje, esquema de codificación, período de validez, etc.	BOUND_TX BOUND_TRX	Si	No
submit_sm_resp	El MC responderá al PDU submit_sm, indicando éxito o falla de La solicitud. También incluye una MC message_id que puede ser usada en operaciones subsecuentes a consultas, cancelaciones o remplazo de contenidos de un mensaje no enviado.	BOUND_TX BOUND_TRX	No	Si
submit_sm_multi	Una variacion del PDU submit_sm que soporta arriba de 255 recipientes para la entrega de mensaje.	BOUND_TX	Si	No
submit_sm_multi_resp	El MC responde al PDU submit_multi. Esto es algo simil del PDU submit_sm_resp. La principal diferencia estas en donde algunos de los recipientes especificados fueron por cualquier cosa invalidos o rechazados por el MC, el PDU podrá especificar la lista de recipientes fallidos, agregando el código de error especificocode para cada uno, indicando la razón de porque el recipiente fue invalido. También es incluido un MC message_id, el cual será usado en operaciones subsecuentes de consulta, cancelación o remplazar el contenido de un mensaje no enviado.	BOUND_TX BOUND_TRX	No	Si
data_sm	data_sm es una versión flujo(stream) de la operación submit_sm, designada para basarse en empaquetamiento de aplicaciones que no demanden funcionalidad extendida Normalmente disponible, en la operación submit_sm. ESMEs implementando WAP en un SMS bearer generalmente utilizará esta operación.	BOUND_TX BOUND_TRX	Si	Si
data_sm_resp	El MC responde al PDU data_sm, indicando el éxito o fallo de la solicitud. También es incluido un MC message_id, el cual será usado en operaciones subsecuentes de consulta, cancelación o remplazar el contenido de un mensaje no enviado.	BOUND_TX BOUND_RX BOUND_TRX	Si	Si

Fuente:Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 5.

Tabla XVII. **Operaciones de mensajes enviados (*delivery*)**

Nombre PDU SMPP	Descripción	Estado de sesión requerido	Ofrecido por ESME	Ofrecido por SMSC
deliver_sm	Deliver_sm es el opuesto simétrico a submit_sm y es usado por un MC para enviar y recibir o ejecutar el rol de transceiver ESME.	BOUND_RX	No	Si
deliver_sm_resp	Este PDU indica aceptación o rechazo de un mensaje enviado. El error regresado por el ESME puede causar que el mensaje sea revisado en algún momento posterior o rechazar ahí mismo éste.	BOUND_RX	Si	Si
data_sm	Data_sm también puede ser usado para enviar un mensaje desde el MC hacia el ESME. ESMEs implementando WAP en SMS por lo general usa esta operación.	BOUND_TX BOUND_RX BOUND_TRX	Si	Si
data_sm_resp	El ESME responde a un PDU data_sm, indicando el éxito o fracaso de el envío MC inicializado.	BOUND_TX BOUND_RX BOUND_TRX	Si	Si

Fuente: Short Message Peer-to-Peer. Especificación del protocolo 3.4. p. 6.

1.3.8.1.5. Interacción ESME y SMSC

Como conclusión a lo anterior, el protocolo SMPP es estandar y el más usado con el cual se comunican dos entes en función de envío y recepción de mensajes cortos en redes telefónicas, este protocolo está basado en un grupo de operaciones de unidades de datos PDU, además de información sobre ese PDU en formatos de datos o texto.

Cada operación entonces consiste en un requerimiento y una respuesta asociada a este requerimiento, esto a través de una sesión de tiempo transmisión recepción o trasmisión-recepción. Esta misma sesión es

usualmente iniciada por el ESME asociando a este un identificador de sistema (System ID) y una contraseña (password).

Más adelante en el proyecto se mostrará cómo esta asociación puede ser establecida individualmente en recepción (desde el SMSC) y en transmisión (hacia el SMSC) haciendo un flujo constante de mensajes con secuencia y estatus de comando que identifican el resultado de requerimiento o primitiva de cada acción. Para referencia de errores ver la tabla XVIII.

Tabla XVIII. **Descripción de un ejemplo de valores de estado de comando o *command status***

SMPP ERROR CODE	VALUE (HEX)	DESCRIPTION	POSSIBLE SOLUTION
ESME_ROK	0x00000000	No Error	
ESME_RINVMSGLEN	0x00000001	Message Length is invalid	Max 140 octets (160 chars in uncompressed default character encoding).
ESME_RINVCMDLEN	0x00000002	Command Length is invalid	
ESME_RINVCMDID	0x00000003	Invalid Command ID	
ESME_RINVBNDSTS	0x00000004	Incorrect BIND Status for given command	Must bind first before any other request is handled.
ESME_RALYBND	0x00000005	ESME Already in Bound State	Do not send bind requests when already bound.
ESME_RINVPRTFLG	0x00000006	Invalid Priority Flag	
ESME_RINVREGDLVFLG	0x00000007	Invalid Registered Delivery Flag	
ESME_RSYSERR	0x00000008	System Error	
Reserved	0x00000009	Reserved	
ESME_RINVSRCADR	0x0000000A	Invalid Source Address	Set to null or 0 to accept the default source address for your account.
ESME_RINVDSTADR	0x0000000B	Invalid Dest Addr	Invalid length (>3 && < 17), invalid international format
ESME_RINVMSGID	0x0000000C	Message ID is invalid	
ESME_RBINDFAIL	0x0000000D	Bind Failed	
ESME_RINVPASWD	0x0000000E	Invalid Password	Set your correct password to gain access.
ESME_RINVSYSID	0x0000000F	Invalid System ID	You are setting an invalid system id (subscriber id)
Reserved	0x00000010	Reserved	
ESME_RCANCELFAIL	0x00000011	Cancel SM Failed	
Reserved	0x00000012	Reserved	
ESME_RREPLACEFAIL	0x00000013	Replace SM Failed	
ESME_RMSGQFUL	0x00000014	Message Queue Full	
ESME_RINVSERTYP	0x00000015	Invalid Service Type	Set to NULL or defined service types for statistics logging in Call Detail Records.
Reserved	0x00000016	Reserved thru -0x00000032	
ESME_RINVNUMDESTS	0x00000033	Invalid number of destinations	

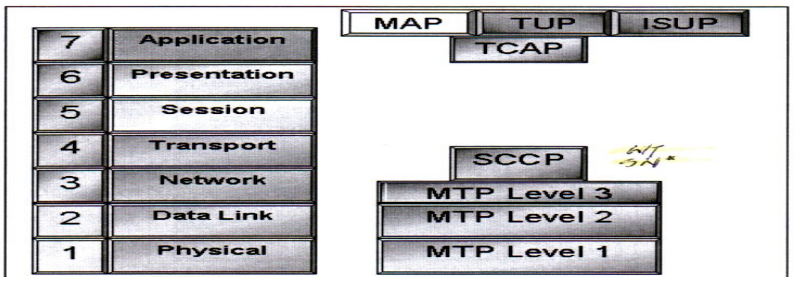
Fuente: SIMplewire Inc. Short message peer to peer error codes. Versiones 3.3 y 3.4. p.1.

2. DESCRIPCIÓN DE FLUJO DE MESAJERÍA CORTA EN REDES CELULARES

2.1. Partes del usuario o User Part

El protocolo de circuitos conmutados o ISUP, usado para configurar, manejar y gestionar llamadas de voz y datos sobre la red pública de telefonía conmutada o PSTN. Es usado para llamadas en la red digital de servicios integrados o ISDN y no ISDN es parte de la señalización de la Norma ANSI SS7 para remplazar TUP, el cual no soporta la transmisión de datos o circuitos digitales. De todas formas ISUP no soporta las tecnologías de banda ancha o broadband. Estas nuevas tecnologías utilizarán la nueva versión de ISUP llamada BISUP, la cual está todavía en desarrollo por la organización de estandarización de telecomunicaciones de la unión internacional de telecomunicaciones o ITU-T. El servicio básico que proporciona ISUP es en el establecimiento y liberación de llamadas. En la figura 16 se muestra el modelo de capas SS7.

Figura 16. **Modelo de capas SS7**



Fuente: Comverse iSMSC training manual. p. 8.

2.1.1. Partes del usuario ISDN

Las partes del usuario ISDN (ISUP) definen el protocolo y los procedimientos a seguir para instalar, manejar y liberar los conductos de los circuitos que transporten voz (release trunk circuits) y datos dentro de la central o Switch de la red de telefonía pública (PSTN). ISUP es utilizado para llamadas ISDN y No-ISDN. Es mejor recordar que las llamadas que se originen y finalicen en la central no utilizan la señal ISUP.

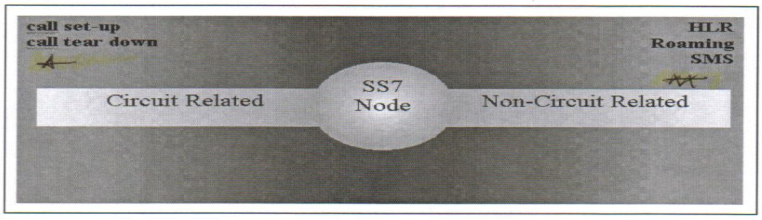
2.1.2. Partes del usuario de teléfono o Telephone User Part

En algunos lugares del mundo (ejemplo, China), las partes del usuario de teléfono o TUP, soporta procesamientos de llamadas básicas. El TUP solamente maneja circuitos análogos; las partes del usuario de datos proveen circuitos digitales y tienen la capacidad de transmitir datos.

2.1.3. El nudo o nodo SS7

En la figura 17 se puede ver un esquema genérico de nodo con relación a circuito y sin relación a circuito (esta división podría ejemplificarse como aplicaciones con voz y aplicaciones con solo señalización).

Figura 17. **Relación de nodo SS7**



Fuente: Comverse iSMSC training manual. p. 13.

2.1.3.1. Descripción de la red SS7

La red SS7 divide claramente los planos de señalización y circuitos de voz. Una red SS7 tiene que estar hecha de equipos capaces de soportar SS7 de terminal a terminal para proveer su funcionalidad completa. La red está hecha de muchos tipos de enlace (A, B, C, E, y F) y tres nodos de señalización: punto de conmutación de servicios o SSP, punto de transferencia de Señal o STP y punto de control de servicio o SCP. Cada nodo es identificado en la red por un número, un código punto. Los servicios extendidos son entregados por una interfaz de base de datos a nivel SCP usando X.25.

2.1.3.2. Relación a circuito

La dirección inicial del mensaje o IAM del ISUP usualmente separa los conductos de los circuitos que no están en uso, del switch de origen con switch de destino. El IAM incluye el código del punto de origen, el código del punto de destino, el código de la identificación del circuito, dígitos marcados y opcionalmente el grupo de números y nombres que llaman. A toda esta información se le llama circuitos relacionados.

2.1.3.3. No relación a circuito o datos de circuitos no relacionados

La capacidad de las transacciones en la parte de aplicaciones está definida por las recomendaciones de la Norma ITU del Q.771 al Q.775. La capacidad de las transacciones proporciona los medios para establecer comunicación de circuitos no relacionados entre nudos en una red con señal. Por ejemplo, cuando un usuario de telefonía móvil entra a un área nueva MSC (Mobile Switching Centre), el VLR integrado solicita al suscriptor información de

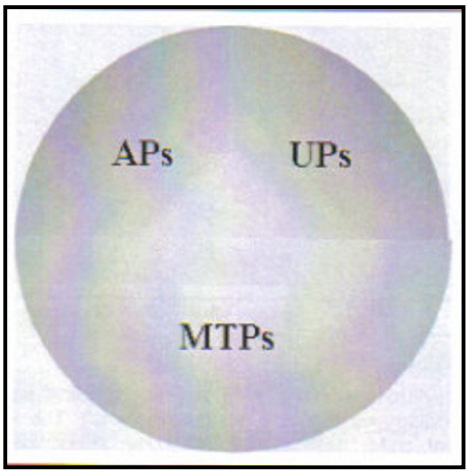
la localización del centro de servicios utilizando información del MAP (Mobile Aplication Part) transportado dentro del los mensajes TCAP. Los mensajes TCAP están dentro de una porción del SCCP en un MSU, abarcando una porción de la transacción y del componente.

2.1.3.4. Partes de un nodo

En la figura 18 se pueden apreciar las partes de un nodo o nudo SS7. Cada nudo se divide en diferentes partes según su funcionamiento:

- Partes del usuario (UP´s)
- Partes de aplicaciones (AP´s)
- Partes de transferencias de mensajes (MTP´s)

Figura 18. **Partes de un nodo SS7**



Fuente: Comverse iSMSC training manual. p. 14.

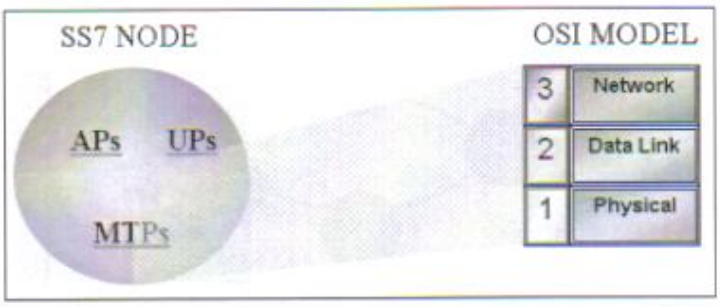
2.1.3.4.1. Partes del usuario o TUP

La parte de usuario de telefonía o TUP (Telephone User Part) es una versión internacional de ISUP, pero menos robusta. Protocolo SS7 utilizado por muchas administraciones europeas para el control básico de conexión. No está soportado en las redes norteamericanas que utilizan el más recientemente definido ISUP. Fue diseñado principalmente para controlar el establecimiento y liberación de llamadas. Además, define los procedimientos y formatos para características extras (servicios suplementarios), como: desviación de llamadas, identificación de llamadas, grupo cerrado de usuarios y conectividad digital.

2.1.3.4.2. Parte de aplicación

En la figura 19 se puede ver la parte de transferencia de mensajes comparado con las tres primeras partes del modelo ISO.

Figura 19. **MTP con referencia a capas ISO**



Fuente: Comverse iSMSC training manual. p. 14.

2.1.3.5. Parte de transferencia de mensajes o MTP

Es el responsable de entregar los mensajes entre los switches. MTP abarca los primeros tres niveles del protocolo SS7. El MTP utiliza las opciones 1 al 3 del OSI y las opciones del 4 al 7 son utilizadas por las partes del usuario y de aplicaciones. El MTP es responsable de la transferencia exitosa de los mensajes entre nudos. Los mensajes son transferidos como unidades de señalización o SU´s (Signalling Units).

El MTP se divide en tres niveles:

- Nivel 1: provee funciones para el enlace de señalización de datos o SDL (Signalling Data Link), tales como los interruptores, conexiones y las funciones de transmisión.

- Nivel 2: provee funciones básicas para el SL (Signalling Link), tales como detecciones de error y sus correcciones.

- Nivel 3: provee funciones de manejo de red y funciones de manejo de Mensaje (Message Handling Funtions).

Las funciones del MTP son las siguientes: delimita el SU, por lo tanto diferencia entre el principio y el fin de un SU, detecta y enumera las fallas, recupera el sistema (link recovery), detecta errores, corrección y retransmisión de errores. El MTP se encarga ademas de que: el SU´s sean enviados al destino correcto.

2.1.3.6. Componentes de una red SS7

El punto de control de servicio o SCP, actúa como un nudo de servicio dentro de la red SS7 y permite el despliegue de servicios en un lugar donde puedan ser accesibles por medio de señales de mensajes dentro de todos los switches en una red. Este concepto es conocido por redes inteligentes o IN. Los mensajes SS7 se intercambian con los SP (Network Signalling Points) dentro de uno o más signalling links. Información señalizada viaja fuera de banda, en canales especiales reuniéndose luego en canales de voz. Esto permite tener una mayor:

- Velocidad
- Eficiencia
- Flexibilidad
- Manejo
- Control

Normalmente, los sistemas están organizados en grupos conocidos como set de enlaces o link sets. Un link set es una colección de links que comparten un mismo destino y que usualmente están conectados entre SPs. La carga total de mensajes es compartida con diferentes links activos. Esto significa que el SS7 es muy seguro en este aspecto, si alguno llegara a fallar otro link dentro del set pasaría a estar activo y tomaría la carga. Puede haber hasta 16 links en un set, con más de un link set del SP. Cuando existe una comunicación directa entre dos SPs se le llama ruta (route). Las rutas pueden incluir más de un link set. Cuando existe más de un camino de comunicación hacia y desde el SPs o cuando existe otra alternativa, se tiene una colección de rutas a las que se les llama route set (sistema de ruta).

Dentro de la red, algunos SPs no procesan mensajes, los trasladan a otro SP's. A éstos se les llama puntos de transferencia de señalización o STP (Signalling Transfer Point). En la figura 20 se puede apreciar los componentes de la red SS7.

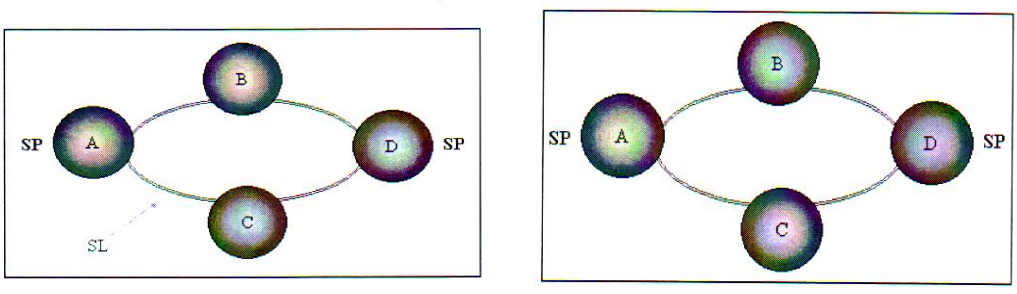
Figura 20. **Componentes de la red SS7**

Fuente: Comverse iSMSC training manual. p. 15.

2.1.3.6.1. Enlace de señalización o SL

Dentro de la red a los nudos se les llama puntos de señalización o SP (Signalling Points). La figura 21 muestra los puntos de señal o SP (Signalling Points) y su identificación según relación entre partes.

Figura 21. **Clases o tipos de conexión o links.**



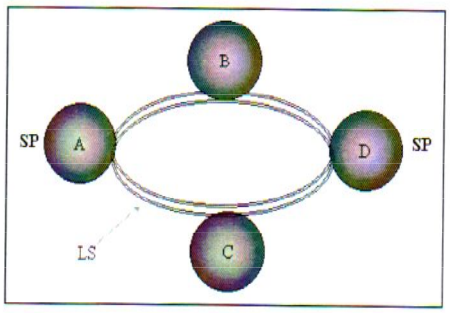
Fuente: Comverse iSMSC training manual. p. 16.

Dentro de la red, los nudos están conectados entre sí por uno o varios enlaces (links) llamados enlaces de señalización (Signalling Links).

2.1.3.6.2. Grupo de enlaces

Cuando se encuentran varios enlaces (links) juntos se le llama grupo de enlace (Link Set). En la figura 22 se puede apreciar un grupo de enlace de señalización o SL (Signalling Link Sets).

Figura 22. **Relación de SL**



Fuente: Comverse iSMSC training manual. p. 17.

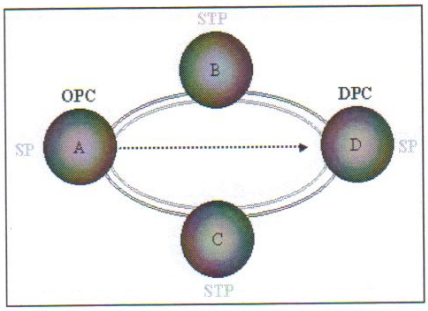
2.1.3.6.3. Ruta

Una ruta se define como la relación código de punto destino (DPC) hacia código de punto origen (OPC) en un enlace SS7, donde ambas partes, tanto origen como destino tienen la misma ruta definida complementariamente.

2.1.3.6.4. Grupo de ruta

Cuando un mensaje es generado en un SP y enviado a otro se le llama punto de origen u OPC y punto de destino o DPC respectivamente. En la figura 23 se muestran los puntos de origen y de destino.

Figura 23. **Relación origen-destino en código punto**



Fuente: Comverse iSMSC training manual. p. 17.

2.1.3.6.5. Código de punto

Dentro del SS7, cada punto de señal (Signalling Point) está identificado por un código de punto numérico. Los códigos de punto son transportados dentro de señales de mensajes intercambiados con puntos de señales (Signalling Point) para identificar la fuente y el destino de cada mensaje. Cada punto de señal utiliza una tabla de rutas para seleccionar el camino adecuado para cada mensaje.

2.1.3.6.6. Punto de señalización

Existen 3 tipos de puntos de señalización (Signalling points) dentro de la red del SS7:

- Punto de conmutación Service Switching Point (SSP)
- Punto de transferencia (STP) (Signal Transfer Point)
- Punto de control (SCP) (Service Control Point)

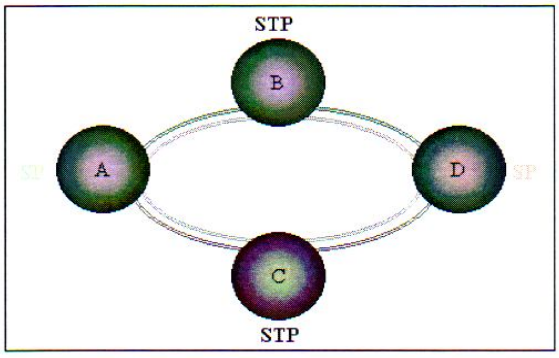
La información de la ruta se encuentra dentro del Routing Label (etiqueta del mensaje) del mensaje.

2.1.3.6.7. Código de punto origen y destino

Signalling Transfer Part (STP): punto de transferencia o STP (Signalling Trasfer Point) son SP dentro de la red que no procesan mensajes únicamente los trasladan a otro SP.

Dentro del SS7, el STP existe únicamente para encaminar los mensajes al destino apropiado. No ofrece servicios y no posee una parte del usuario. Utiliza las características del MTP para asegurarse que los mensajes lleguen al destino correcto. Éste toma como referencia la base de datos o la tabla de rutas para determinar la ruta correcta para cada mensaje en particular. Generalmente las STP se encuentran en pares, ya que esto asegura la redundancia. Conectando el ISMSC a un par asegura la resistencia de la ruta. En la figura 24 se muestra la trasferencias por medio de STP de conexión.

Figura 24. **Comunicación A-D vía STP**



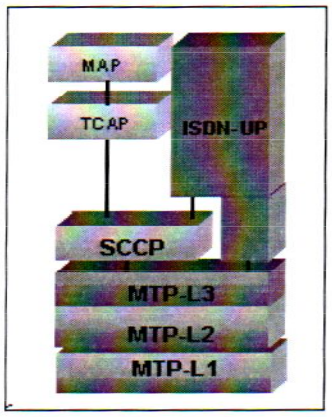
Fuente: Comverse iSMSC training manual. p. 17.

2.1.3.7. SS7 y capas MTP

El MTP está alternadamente dividido en 3 capas distintas según su funcionalidad, cada una de ellas posee una tarea específica. Todas ellas están relacionadas con la seguridad del trayecto de los mensajes y del manejo de los links del SS7.

El modelo de referencia OSI proporciona un marco para las capas arquitectónicas de entidades funcionales, cada una le da funcionalidad a las otras capas. La unión de estas capas del protocolo SS7 provee una arquitectura que es, en muchos aspectos, similar al modelo OSI, las cuales cambian, principalmente, en las capas superiores. Por lo tanto, en las 3 capas inferiores, la funcionalidad es similar al modelo OSI y por lo tanto le es familiar a cualquier persona con conocimiento del mismo. En la figura 25 se muestra el modelo de las capas SS7 y MTP.

Figura 25. **Modelo de capas SS7**

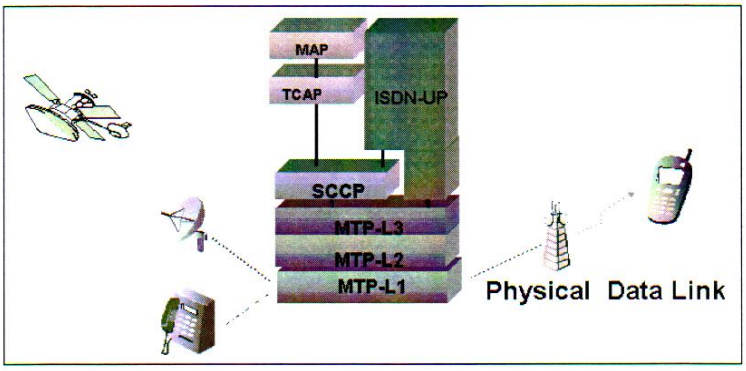


Fuente: Comverse iSMSC training manual. p. 18.

2.1.3.7.1. MTP1

La capa 1 MTP representa a la capa física. Esta es la responsable de la conexión del SS7 Signalling Points con la red de transmisión desde la cual se comunican entre sí. Esto implica, principalmente a la conversión de los mensajes en señal eléctrica y el mantenimiento de los links físicos por los cuales pasan éstos. De esta forma, éste es análogo a la capa 1 del ISDN u otros protocolos. En la figura 26 se muestra el MTP capa 1.

Figura 26. **Función de MTP1**



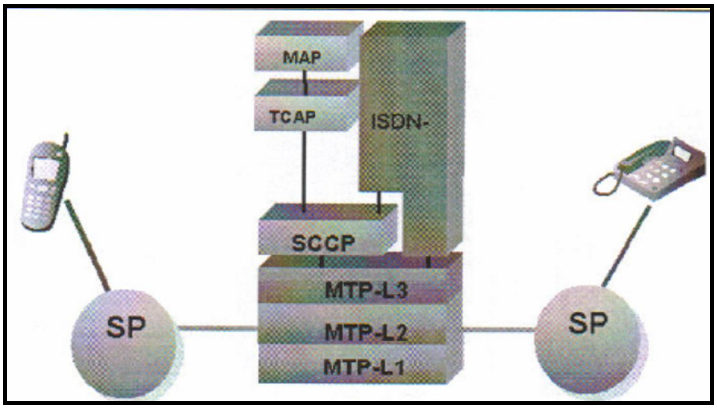
Fuente: Comverse iSMSC training manual. p.18.

2.1.3.7.2. MTP2

La capa 2 MTP está diseñada para proporcionar una transferencia segura de la señal de información entre SPs. En este paso se examinan los datos transmitidos para chequear posibles errores y corregirlos, si es posible, cuando sean descubiertos. Con potencial de transmitir una gran cantidad de información, la capa 2 MTP, también debe monitorear el control del flujo de mensajes, clasificando los mensajes basados en colas y buffers.

Todos los mensajes SS7 son transmitidos a través del SS7 links de señalización. El control del flujo es de vital importancia, ya que el ancho de banda disponible en el link es usualmente 64,000 bits por segundo o 56,000 bits por segundo. Por lo tanto, el monitoreo del link es esencial para que el sistema SS7 trabaje adecuadamente. En la figura 27 se muestra el MTP capa 2.

Figura 27. **Función MTP2**



Fuente: Comverse iSMSC training manual. p. 19.

2.1.3.7.3. MTP3

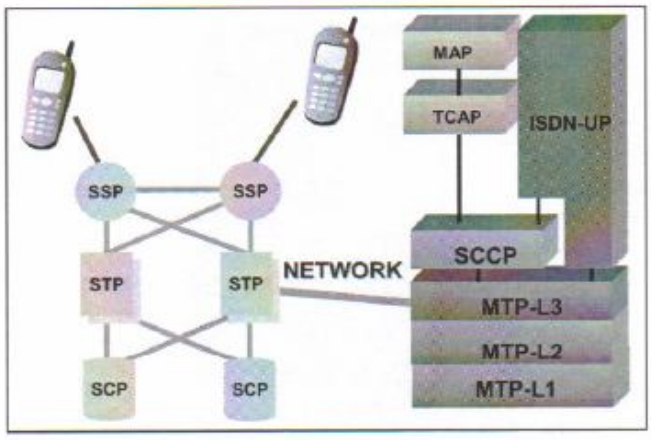
La capa 3 del MTP tiene dos funciones básicas:

- Traslado de mensajes: está relacionado con el envío de mensajes recibidos al destino apropiado, ya sea arriba o abajo.

- Manejo de la red: está relacionado al control de tráfico de los traslados, a los links que controlan el tráfico y al manejo de errores.

Cada una de las capas sobre la capa 3 del MTP pueden ser considerados como usuarios. Las capas superiores confían en el MTP capa 3 para la entrega correcta de los mensajes que ellos le envían y para la recepción correcta y el encaminamiento de los mensajes que reciben. En la figura 28 se puede apreciar el MTP capa 3.

Figura 28. **Función MTP3**

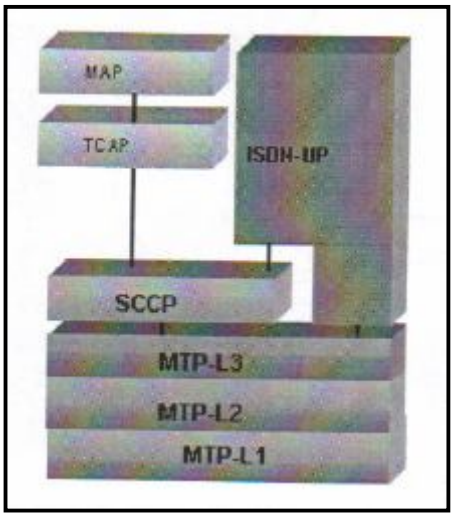


Fuente: Comverse iSMSC training manual. p. 19.

2.1.4. Parte de control de señalización de conexión o SCCP

La parte de control de señalización de conexión (Signalling Connection Control Part) provee un servicio de red sin conexión y una orientación de la conexión en las capas superiores al MTP capa 3. El MTP capa 3 provee puntos de códigos que permite que los mensajes sean enviados a direcciones SP específicas. En la figura 29 se muestra la relación de SCCP con las capas inferiores y superiores del modelo de capas de SS7.

Figura 29. **Interacción SCCP**

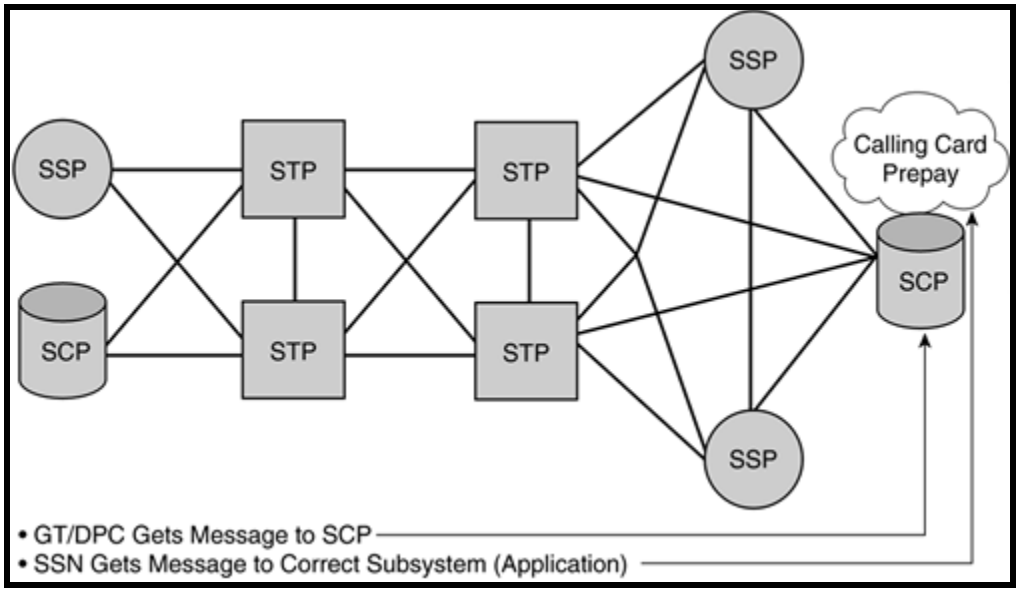


Fuente: Comverse iSMSC training manual. p. 22.

2.1.4.1. Definición del número de subsistema

EL SCCP es utilizado como una capa de transporte para el TCAP, basado en servicios tales como: llamadas gratis (0800/0888), roaming inalámbrico, servicios de comunicación personal (PCS) y Global Title Translation (GTT) o traslación por título o nombre. Este no proporciona ningún reconocimiento ni procedimiento de recuperación. La figura 30 muestra la relación de llamadas GTT y código de punto en el SCP.

Figura 30. **Relación GT-PC-SSN**



Fuente: BERTONI, Henry. Red SS7. p. 30.

2.1.4.2. Definición de título global

El SCCP provee números del subsistema que permiten que los mensajes se dirijan hacia aplicaciones específicas.

2.1.5. Parte de aplicaciones de capacidad de traducción o TCAP

La parte de aplicaciones de capacidad de traducción o TCAP (Translation Capabilities Application Part), permite el despliegue de los servicios en red inteligentes, apoyando el intercambio de información entre los circuitos no relacionados con los puntos de señal (Signalling Points) utilizando el servicio sin conexión del SCCP. Un SP utiliza TCAP para solicitarle al SCP que determine

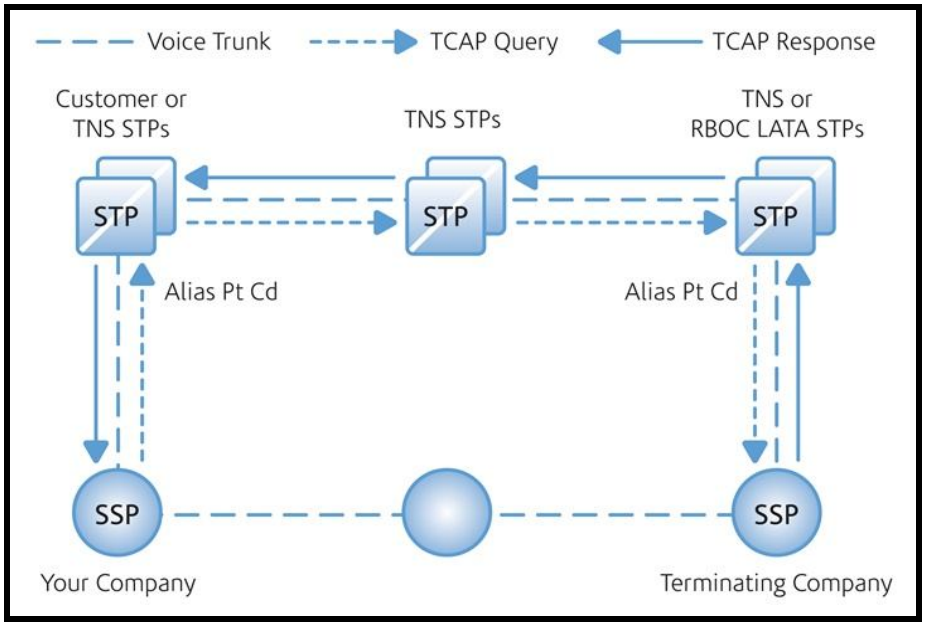
los números de la ruta asociada con los números pulsados 800, 888 o 900. El SCP utiliza el TCAP para devolver la respuesta de regreso al SP, el cual contiene el número de la ruta, o ya sea el error o el componente de rechazo. Las llamadas realizadas con tarjetas de llamadas, también pueden utilizar el TCAP para la solicitud y el mensaje de respuesta.

Cuando un usuario de telefonía móvil utiliza el roaming e ingresa a un área con un nuevo centro de servicio móvil o MSC, el registro integrado de la localización del visitante solicita la información del perfil de la empresa que le provee los servicios al usuario (HLR), utilizando información del Mobile Application Part (MAP) transportada a través del los mensajes del TCAP (ver figura 31).

Los mensajes del TCAP se encuentran dentro de una parte del SCCP del MSU. El mensaje TCAP está compuesto de:

- Porción de transacción
- Porción de componente

Figura 31. **Mensajes TCAP**



Fuente: KORHONEN, Juha. Introduction to 3G mobile communications. p. 203.

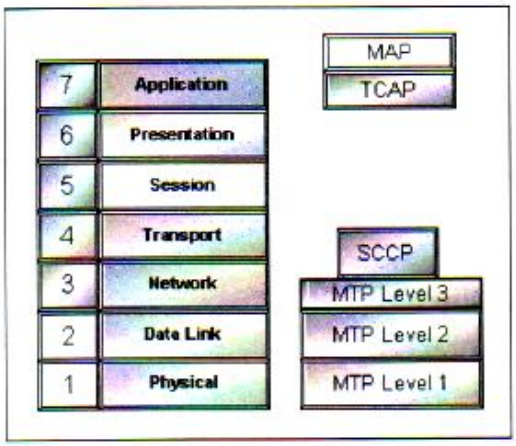
2.1.6. Parte de aplicación móvil o MAP

En telefonia la capa de aplicación para GSM estra construida sobre el protocolo MAP.

2.1.6.1. Definición

MAP está diseñado, especialmente, para soportar GSM en el modelo OSI. El MAP se encuentra sobre el TCAP, ambos pertenecen a la capa 7. Éste utiliza el servicio sin conexión del SCCP y los servicios del TCAP. La figura 32 muestra la parte de aplicación móvil o MAP

Figura 32. **Parte MAP en pila SS7**



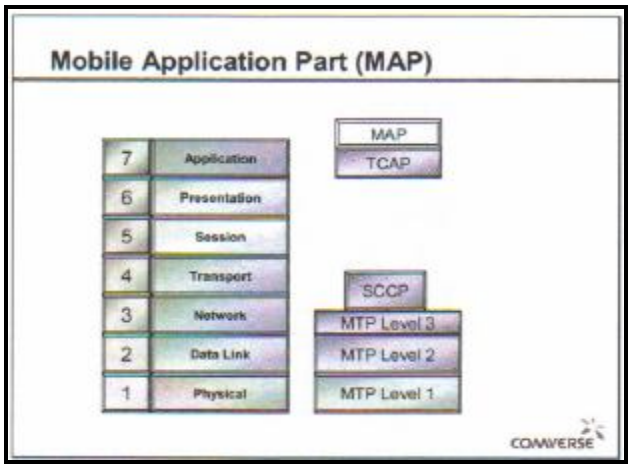
Fuente: Comverse iSMSC training manual. p. 23.

El GSM MAP (ver figura 33), está especificado en la Norma ETSI (ETS GSM 09.02) y es muy utilizada alrededor del mundo. Una de las razones de su éxito es la innovación que separa un aparato móvil con una tarjeta inteligente que identifica al usuario y a su perfil de suscripción; esta es la tarjeta SIM. La tarjeta SIM contiene la identidad del usuario móvil, un dato que puede ser transmitido por un aparato y utilizado para comprobar la autenticidad en cualquier red de GSM. Este requerimiento introduce la autorización y el registro de los usuarios, especialmente si se mueven entre estaciones de radio base o RBS. Por lo tanto, una red de GSM requiere bases de datos sofisticados que soporten todos los datos de usuarios.

El Global Title Translation tiene un papel importante dentro de este proceso, ya que las redes necesitan localizar información fuera de su propia infraestructura de base de datos.

Es más importante aún, cuando se trata de la entrega de SMS ya que ésta es la única forma que un usuario pueda ser localizado globalmente, es decir, saber en qué área del MSC se encuentran. El IS41 es el estándar utilizado en los Estados Unidos. Éste está especificado por la ANSI.

Figura 33. **Aplicación móvil**



Fuente: Comverse iSMSC training manual. p. 24.

Cuando se hace necesaria la transferencia de información específica entre entidades de Public Land Mobile Network (PLMN), el Signalling System No. 7 especificado por el CCITT es usado para la transferencia de esta información, utilizando el GSM MAP.

2.1.6.2. Capacidad de transacción o TC

El MAP utiliza los servicios ofrecidos por la capacidad de transacción o TC (Transaction Capabilities) del Signalling System No. 7. Para especificaciones más completas del TC se debe consultar la Norma ETS 300 287, el cual está basado en el CCITT.

El MAP utiliza todos los servicios proporcionados por el TC, exceptuando los relacionados a los diálogos no estructurados. Desde la perspectiva del modelo, el MAP es visto como un solo elemento de aplicación de servicio. (Ver figura 34).

La capacidad de transacción se refiere a una estructura de protocolo sobre la capa de red de interface (servicio de interface del SCCP), hasta la capa de aplicaciones, incluyendo elementos de servicio de aplicaciones comunes, pero no los elementos de servicios de aplicaciones específicos usados por ellos.

El TC está estructurado como un componente de la sub-capa superior a la sub-capa de transacciones. La sub-capa componente tiene 2 tipos de servicios de aplicaciones: el servicio para el control de fin al fin (end-to end) diálogos y servicios para manejar operaciones remotas.

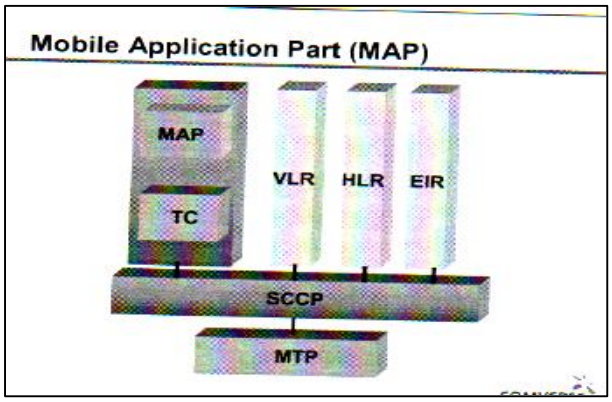
Se puede acceder a estos servicios utilizando el diálogo TC de manejos primitivos y el componente TC de manejos primitivos, respectivamente. Los servicios para el control del diálogo incluyen la habilidad de intercambiar información relacionada a la negociación del contexto de aplicación, así como datos de inicio.

Servicios para el manejo de una operación remota, le proporciona al intercambio del protocolo de unidades de datos una solicitud de tareas (operaciones) y le reporta sus resultados (resultados o errores), además de cualquier error del protocolo en cualquier aplicación no específica, detectada por la sub capa componente.

Los reportes de los errores del protocolo de aplicaciones específicas por el usuario TC diferentes al proceso de aplicaciones de errores, también son reportados.

La sub capa transacciones proporciona una simple asociación en el servicio de conexión de punta a punta (end-to-end), desde la cual se pueden intercambiar varias unidades de datos del protocolo relacionadas, es decir, construidas por la sub capa componente. La finalización de una transacción puede ser pre organizada (el usuario no recibe indicación) o básica (se recibe indicación).

Figura 34. **Capa de transacciones**

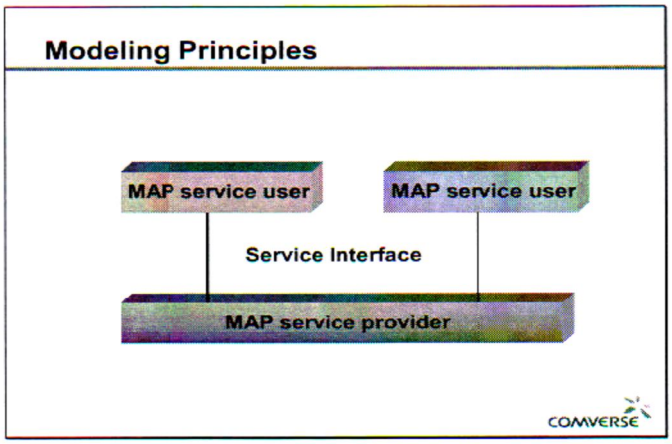


Fuente: Comverse iSMSC training manual. p. 26.

2.1.6.3. Principios de modelaje

El MAP es un grupo de servicios, que el proveedor del servicio le proporciona al usuario según se presenta en la figura 35. .

Figura 35. **Relación de servicios y modelo MAP**



Fuente: Comverse iSMSC training manual. p. 28.

3. FLUJO DE MENSAJES CORTOS O SMS

3.1. Introducción

La parte de aplicación móvil o MAP (Mobil Application Part) está diseñada para trabajar con GSM en el modelo OSI. Éste se encuentra arriba del TCAP en el modelo OSI. Ambos pertenecen a la capa 7, la capa de aplicación, proporcionando servicio y soporte.

Se puede encontrar el protocolo MAP en el ISMSC, MSC, HLR, VLR, EIR, y en el centro de autentificación o AUC, ayudando a la comunicación de nudos en los siguientes casos:

- Registro de localización
- Cancelación de localización
- Cancelación de la matricula
- Envíos y manejo y recuperación de información del suscriptor
- Entrega
- Transferencia de datos asegurados y auténticos

3.2. Entrega exitosa

Se refiere a un envío de mensaje por la red el cual completa las validaciones y termina en el móvil destino exitosamente. Ver figura 36 para literales:

(a). ISMSC le envía al HLR: sendroutinginfoforSMrequest. La dirección en el HLR es manejada por el MDD.

(b). HLR le responde al ISMSC: sendroutinginfoforSMconfirmation. La cual contiene la siguiente información:

- Dirección MSC
- Número IMSI

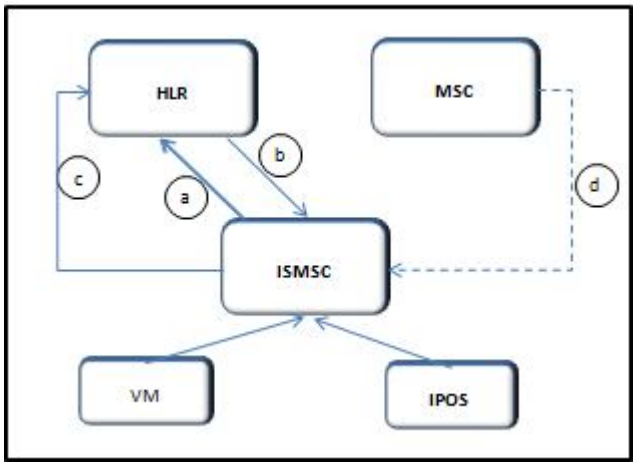
(c). ISMCC le envía al MSC: forwardSMrequest**.** El mensaje forwardSM contiene lo siguiente:

- Dirección MSC (vía título global)
- Número IMSI
- Datos del usuario definidos por el GSM 03.40.

(d). MSC responde: forwardSMconfirmation. Lo cual significa una entrega exitosa.

(e). Falla de entrega debido a falla temporal en MSC/ GSM.

Figura 36. **Entrega exitosa de un mensaje**



Fuente: Comverse iSMSC training manual. p. 32.

3.3. Fallas de entrega del MSC debido a error-GSM temporal

Se refiere a un envío de mensaje por la red el cual no completa las validaciones y termina y terina en un error temporal. Ver figura 37 para literales:

(a). ISMSC le envía al HLR: sendroutinginfoforSMrequest. La dirección en el HLR es manejada por el MSISDN. Ver figura 37 para referencia de flujo.

(b). HLR le responde al ISMSC: sendroutinginfoforSMconfirmation. La cual contiene la siguiente información:

- Dirección MSC
- Número IMSI

(c). ISMCC le envía al MSC: forwardSMrequest**.** El mensaje forwardSM contiene lo siguiente:

- o Dirección MSC (vía título global)
- o Número IMSI
- o Datos del usuario definidos por el GSM 03.40

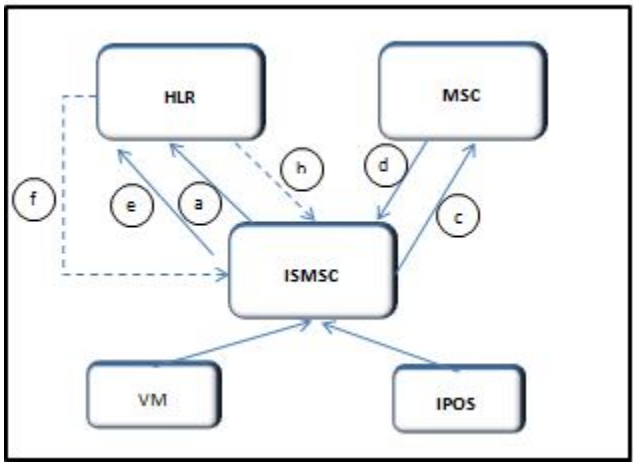
(d). MSC responde con error temporal, e.g. suscriptor ausente

(e). ISMSC responde una solicitud al HLR: report SMdeliverystatus**.** El cual contiene la siguiente información:

- o MSISDN

(f). HLR responde con un reconocimiento al ISMSC

Figura 37. **Falla de entrega por error temporal en GSM**



Fuente: Comverse iSMSC training manual. p. 35.

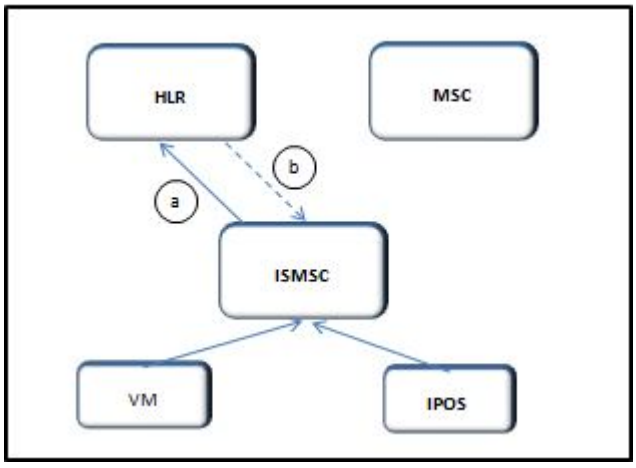
3.4. Falla de entrega debido a falla temporal en HLR/GSM

Se refiere a un envío de mensaje por la red el cual no completa las validaciones y termina con error por mensajes en HLR. Ver figura 38 para literales:

(a). ISMSC le envía al HLR: sendroutinginfoforSMrequest. La dirección en el HLR es manejada por el MSISDN. Ver figura 37 para referencia de flujo.

(b). HLR le responde con un error temporal en el routinginfoforSMconfirmation**.** Si está configurado, el HLR puede enviar un mensaje informSC que le notifica al ISMSC que se ha registrado para una alarma futura cuando el MS se encuentre disponible.

Figura 38. **Falla de entrega por error temporal en HLR**



Fuente: Comverse iSMSC training manual. p. 35.

3.4.1. Definición de registro de localización base o HLR

El registro de localización base o HLR (Home Location Register), o registro de ubicación base es una base de datos que almacena la posición del usuario dentro de la red, si está conectado o no y las características de su abono (servicios que puede y no puede usar, tipo de terminal, etcétera). Es de carácter permanente; cada número de teléfono móvil está adscrito a un HLR determinado y único, que administra su operador móvil.

Al recibir una llamada, el MSC pregunta al HLR correspondiente al número llamado si está disponible y dónde está (es decir, a qué BSC hay que pedir que le avise) y direcciona la llamada o da un mensaje de error.

El registro de ubicación de visitante o VLR (Visitor Location Register) es una base de datos más volátil que almacena, para el área cubierta por un MSC, los identificativos, permisos, tipos de abono y localizaciones en la red de todos los usuarios activos en ese momento y en ese tramo de la red. Cuando un usuario se registra en la red, el VLR del tramo al que está conectado el usuario se pone en contacto con el HLR de origen del usuario y verifica si puede o no hacer llamadas según su tipo de abono. Esta información permanece almacenada en el VLR, mientras el terminal de usuario está encendido y se refresca periódicamente para evitar fraudes (por ejemplo: si un usuario de prepago se queda sin saldo y su VLR no lo sabe, podría permitirle realizar llamadas).

Tomar en cuenta que el sistema GSM permite acuerdos entre operadores para compartir la red, de modo que un usuario en el extranjero, por ejemplo: puede conectarse a una red (MSC, VLR y capa de radio) de otro operador.

Al encender el teléfono y realizar el registro en la red extranjera, el VLR del operador extranjero toma nota de la información del usuario, se pone en contacto con el HLR del operador móvil de origen del usuario y le pide información sobre las características de abono para permitirle o no realizar llamadas. Así, los distintos VLRs y HLRs de los diferentes operadores deben estar interconectados entre sí para que todo funcione. Para este fin existen protocolos de red especiales, como SS7 o IS-41; los operadores deciden qué estándar escoger en sus acuerdos bilaterales de roaming (itinerancia) e interconexión.

3.5. Falla de entrega debido a error permanente en GSM

Se refiere a un envío de mensaje por la red el cual no completa las validaciones y termina con error permanente por mensajes en MSC. Ver figura 39 para literales:

(a). ISMSC le envía al HLR: sendroutinginfoforSMrequest. La dirección en el HLR es manejada por el MSISDN. Ver figura 39 para referencia de flujo.

(b). HLR le responde al ISMSC: sendroutinginfoforSMconfirmation.La cual contiene la siguiente información:

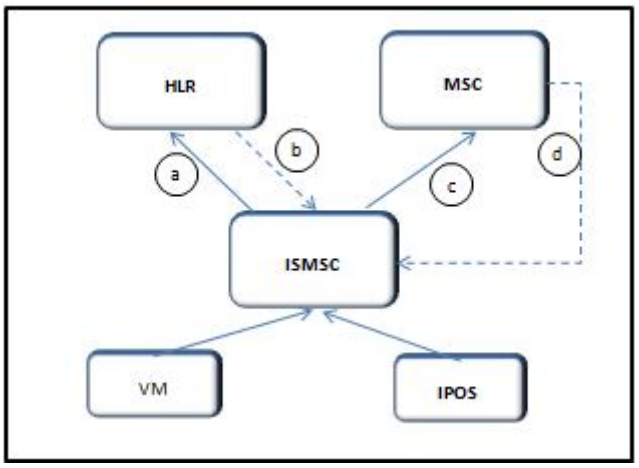
- Dirección MSC
- Número IMSI

(c). ISMCC le envía al MSC: forwardSMrequest**.** El mensaje forwardSM contiene lo siguiente:

- o Dirección MSC (vía titulo global)
- o Número IMSI
- o Datos del usuario definidos por el GSM 03.40#

(d). MSC responde con error permanente con el mensaje forwardSMconfirmation. Como resultado, el ISMSC no trata de entregar el SM de nuevo, y el SM es borrado de la base de datos.

Figura 39. **Falla de entrega debido a error permanente en GSM**



Fuente: Comverse iSMSC training manual. p. 36.

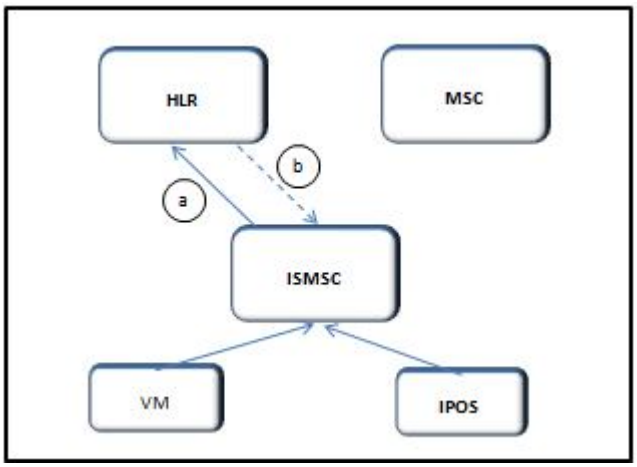
3.6. Error permanente debido a HLR/GSM

Se refiere a un envío de mensaje por la red el cual no completa las validaciones y termina con error permanente por mensajes en HLR y es borrado del almacenamiento. Ver figura 40 para literales.

(a). ISMSC le envía al HLR: sendroutinginfoforSMrequest**.** La dirección en el HLR es manejada por el MSISDN. Ver figura 40 para referencia de flujo.

(b). HLR le responde le responde con un error permanente en él: sendroutinginfoforSMconfirmation. El ISMSC no trata de entregarlo y el SM es removido de la base de datos.

Figura 40. **Errores debido a HLR**



Fuente: Comverse iSMSC training manual. p. 36.

3.7. Alerta seguida de entrega exitosa

Una alerta es una actualización de estado del destinatario, en el que los componentes de la red notifican la disponibilidad del mismo.

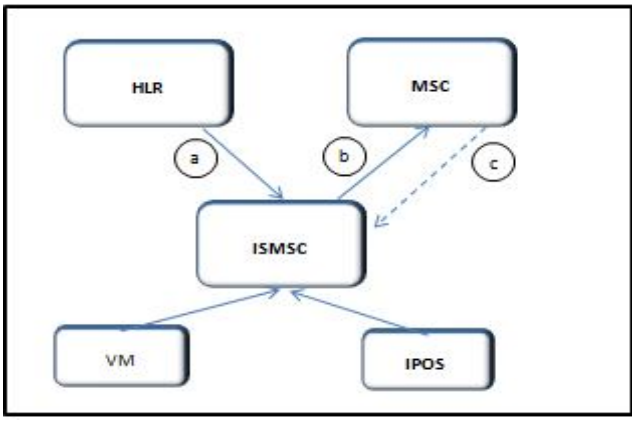
Una alerta seguida por una entrega GSM exitosa. Se refiere a una notificación desde el HLR de disponibilidad del abonado. Ver figura 41 para literales:

(a). Ahora está disponible el suscriptor móvil y el mensaje Message Waiting Dataset en el HLR envía un mensaje SC de alerta al ISMSC para notificar que el MS ya está disponible. Ver figura 41 para referencia de flujo.

(b). Todos los mensajes pendientes en la base de datos del ISMSC son enviados y entregados.

(c). El MSC envía el mensaje**:** forwardSMconfirmation

Figura 41. **Falla debido a error permanente en HLR**



Fuente: Comverse iSMSC training manual. p. 37.

3.8. Flujo de mensaje originado o MO

Se refiere a un envío de mensaje de un usuario local, por la red el cual completa las validaciones y termina exitosamente. Ver figura 42 para literales:

(a). Vía MSC, el suscriptor móvil A envía al SMSC: SMS_submit.

(b). El MSC envía el SMS al ISMSC con un mensaje: MAP_forward_SM.

(c). El ISMSC formatea el mensaje corto y lo guarda en la base de datos. Ahora éste reconoce el mensaje MAP_forward_SM y lo envía de regreso al suscriptor móvil a través del MSC. Ver figura 42 para referencia de flujo.

(d). ISMSC envía al HLR: sendroutinginfoforSMrequest. La dirección en el HLR es manejada por el MSISDN

(e). HLR le responde al ISMSC: sendroutinginfoforSMconfirmation**.** La cual contiene la siguiente información:

- Dirección MSC
- Número IMSI

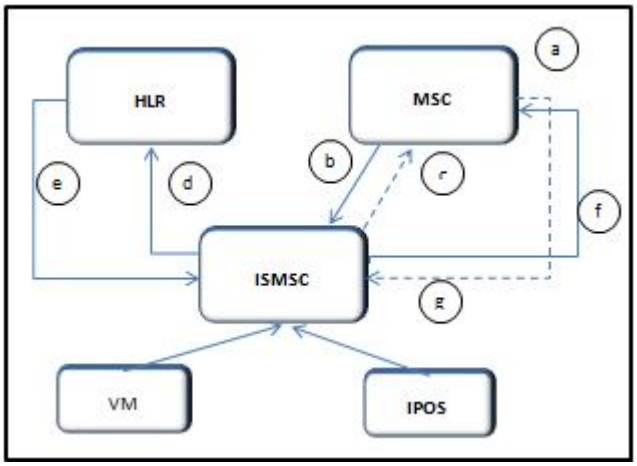
(f). ISMCC le envía al MSC: forwardSMrequest**.** El mensaje forwardSM contiene lo siguiente:

- Dirección MSC (vía titulo global)
- Número IMSI
- Datos del usuario definidos por el GSM 03.40

(g). MSC responde con: forwardSMconfirmation, lo cual indica una entrega exitosa.

(h). El MSC formatea un SMS _status_report y si está previsto, lo envía al suscriptor móvil como un último mensaje móvil estándar.

Figura 42. **Flujo de mensaje originado en el móvil, MO**



Fuente: Comverse iSMSC training manual. p. 38.

4. INFORMACIÓN GENERAL DE LA EMPRESA

4.1. Antecedentes de la Secretaria Nacional de Ciencia y Tecnología, SENACYT

La institución por excelencia de apoyo a crecimiento del interés por la aplicación y reforzamiento de la ciencia, es descrita a continuación como parte de proyecto realizado en unión con una empresa de telecomunicaciones.

4.1.1. Reseña histórica

El Decreto Gubernativo número 63-91 del Congreso de la República de Guatemala, por medio de la Ley de Promoción del Desarrollo Científico y Tecnológico Nacional, crea la Secretaría Nacional de Ciencia y Tecnología, SENACYT, que tendrá la función de apoyar al Consejo Nacional de Ciencia y Tecnología.

La SENACYT su objetivo principal es apoyar, coordinar y ejecutar las decisiones del Consejo Nacional de Ciencia y Tecnología y dar seguimiento a sus respectivas acciones, constituye un vínculo entre las instituciones que integran el sistema nacional de ciencia y tecnología.

4.1.2. Misión de la Secretaría Nacional de Ciencia y Tecnología, SENACYT

"Coordinar y ejecutar las políticas nacionales de ciencia, tecnología e innovación, con responsabilidad y excelencia continua, facilitando su articulación, aplicación y seguimiento por medio de mecanismos ágiles y efectivos para impulsar el desarrollo científico y tecnológico del país y coadyuvar al bienestar económico-social de los guatemaltecos".

4.1.3. Visión de la Secretaría Nacional de Ciencia y Tecnología, SENACYT

"Ser la institución por excelencia que promueve el desarrollo de la ciencia, la tecnología y la innovación, para mejorar la competitividad y el nivel de vida de los guatemaltecos, con altos estándares de calidad".

4.2. Tecnologías utilizadas por la empresa de telecomunicaciones TIGO

TIGO parte del grupo Millicom Internacional, con operaciones en Guatemala desde 1989, es una empresa de telecomunicaciones, con cobertura en todo el pais, con servicios de voz y datos.

4.2.1. Tecnología del sistema global para las comunicaciones móviles GSM

El sistema global para las comunicaciones móviles o GSM (Groupe Special Mobile) es un sistema estándar, completamente definido, para la comunicación mediante teléfonos móviles que incorporan tecnología digital. Por

ser digital cualquier cliente de GSM (Global System for Mobile Communications) puede conectarse a través de su teléfono con su ordenador y puede hacer, enviar y recibir mensajes por e-mail, faxes, navegar por Internet, acceso seguro a la red informática de una compañía (LAN/Intranet), así como utilizar otras funciones digitales de transmisión de datos, incluyendo el servicio de mensajes cortos o SMS (Short Message Service).

GSM se considera, por su velocidad de transmisión y otras características, un estándar de segunda generación (2G). Su extensión a 3G se denomina sistema universal de telecomunicaciones móviles o UMTS (Universal Mobile Telecommunications System) y difiere en su mayor velocidad de transmisión, el uso de una arquitectura de red ligeramente distinta y sobre todo en el empleo de diferentes protocolos de radio como el acceso múltiple por división de código de banda ancha o W-CDMA (Wide-Code Division Multiple Access).

4.2.2. Tecnologías de mensajes cortos punto a punto, entidades externas de mensajes cortos y servicio de mensaje de texto

Los mensajes cortos punto a punto o SMPP (Short Message Peer-to-peer Protocol), es un protocolo estándar de telecomunicaciones pensado para el intercambio de mensajes de texto o SMS entre equipos que gestionan los mensajes, como pueden ser los SMSC (Short Message Service Center) o los GSM USSD (Unstructured Supplementary Services Data Server) y el sistema de solicitud de SMS como puede ser un servidor WAP (protocolo de aplicaciones inalámbricas) o cualquier puerto o sistema de mensajería.

Se utiliza, normalmente, para permitir a terceros enviar mensajes (como pueden ser los proveedores de contenido).

SMPP fue desarrollado por Aldiscon, una pequeña firma irlandesa comprada posteriormente por Logica. En 1999, SMPP pasó formalmente a manos del SMPP Developers Forum, posteriormente rebautizado como el SMS Forum.

SMPP es el interfaz que permite que entidades de envío de SMS s que subyacen fuera de la red móvil de las Entidades Externas de Mensajes Cortos o ESME (External Short Message Entities) puedan interconectar con los elementos internos como la SMSC.

SMPP define básicamente:

- El conjunto de operaciones para el intercambio de SMSs entre los ESME y el SMSC.

- Los datos que los ESME debe intercambiar con el SMSC durante la conexión.

El protocolo se basa en el intercambio, petición, respuesta de pares de unidades de datos del protocolo o PDUs (Protocol Data Units), éstos se intercambian sobre la capa 4 OSI (sesiones TCP/IP o X.25). El intercambio de datos puede realizarse de manera síncrona, esperando cada parte la respuesta/petición del otro para enviar la correspondiente petición/respuesta, o asíncrona, donde cada envío y la recepción van a través de distintos hilos.

Actualmente, las versiones más utilizadas, y las más comúnmente soportadas por los operadores son por orden, SMPP v3.3 y v3.4.

Esta última soporta el modo transceptor o transceiver (una misma conexión puede enviar y recibir al mismo tiempo). La última versión disponible es la v5.0.

4.3. Ejemplos de servicios ya existentes de mensajería corta

Los mensajes cortos de texto son usados en una amplia variedad de aplicaciones e interacion con sistemas de comunicación a continuacion se describe algunas de estas aplicaciones o usos.

4.4. Promociones

Las promociones vía mensajes cortos son unas de las más difundidas y comunes en el aspecto de aplicaciones o presentación al cliente final, como las programaciones de radio, encuestas, subscripciones, rifas; aplican una interacción activa entre el usuario y la entidad promotora o receptora, que puede utilizar tanto el contenido del mensaje como el número telefónico de origen, para generar una respuesta o tener un registro de los mensajes recibidos y enviados.

4.4.1. Chat

La aplicación de Chat o plática activa entre dos o más personas vía teléfono, son ampliamente difundidas de manera sofisticada hasta llegar al punto de interactuar, también con ordenadores y aplicaciones web y hacen grupos virtuales de usuarios y virtualizan, también, salones de plática y conversación vía mensajes de texto.

4.4.2. Descarga de tonos para teléfonos

Las descargas de contenido son otra opción de las aplicaciones vía SMS , éstas interactúan con un repositorio de contenidos como los tonos de teléfono, los cuales se dividen usualmente en monofónicos y polifónicos; monofónicos que tiene un menor peso en función de los datos transmitidos y un menor precio y polifónicos con un mayor peso en los datos, pero que también, significa mayor calidad de sonido y variedad pudiendo ser trozos musicales en formato de audio digital comprimido o MP3.

5. PROCESO DE PROGRAMACIÓN DE INTERFASE ESME EN PERL

Tomando en cuenta el conocimiento de cómo a través de un medio físico, pueden trasportarse datos, formando redes con determinado tipo de transporte, presentándolos y haciendo aplicaciones sobre los anteriores, se definirá ahora una aplicación de mensajes cortos, que utiliza la presentación del aparato telefónico como origen y destino del texto, aplicación que utiliza una red Ethernet extendida a una red privada virtual y con un protocolo de TCP-IP como lo es SMPP. Se definirá cómo se interactúa con las partes desde un modelo de programación abierto como PERL, que es el compilador del programa que efectuará sesiones entre el cliente y servidor e interpreta y dará formato al texto de un repositorio de datos que serán vistos finalmente por el usuario.

Puede no estar por completo claro donde están los niveles del modelo OSI en todo el flujo. Pues puede ser que en un punto de la capa de trasporte sea TCP-IP, pero por otra parte se traduzca a SS7 y por consiguiente a MTP1,2 y 3. El enfoque es ahora en la parte de transporte de la aplicación cliente servidor, y con esto TCP-IP. Siguiendo la figura 43. Básicamente el proceso utilizado en la programación es:

- Conexión de datos vía Internet con una red privada virtual punto a punto o VPN.

- Generación de base de datos general de palabras y significado en Mysql.

- Desarrollo de aplicación de módulo para primera consulta sobre enciclopedia libre Wikipedia.

- Desarrollo de aplicación con módulo asociado para consulta a base de datos.

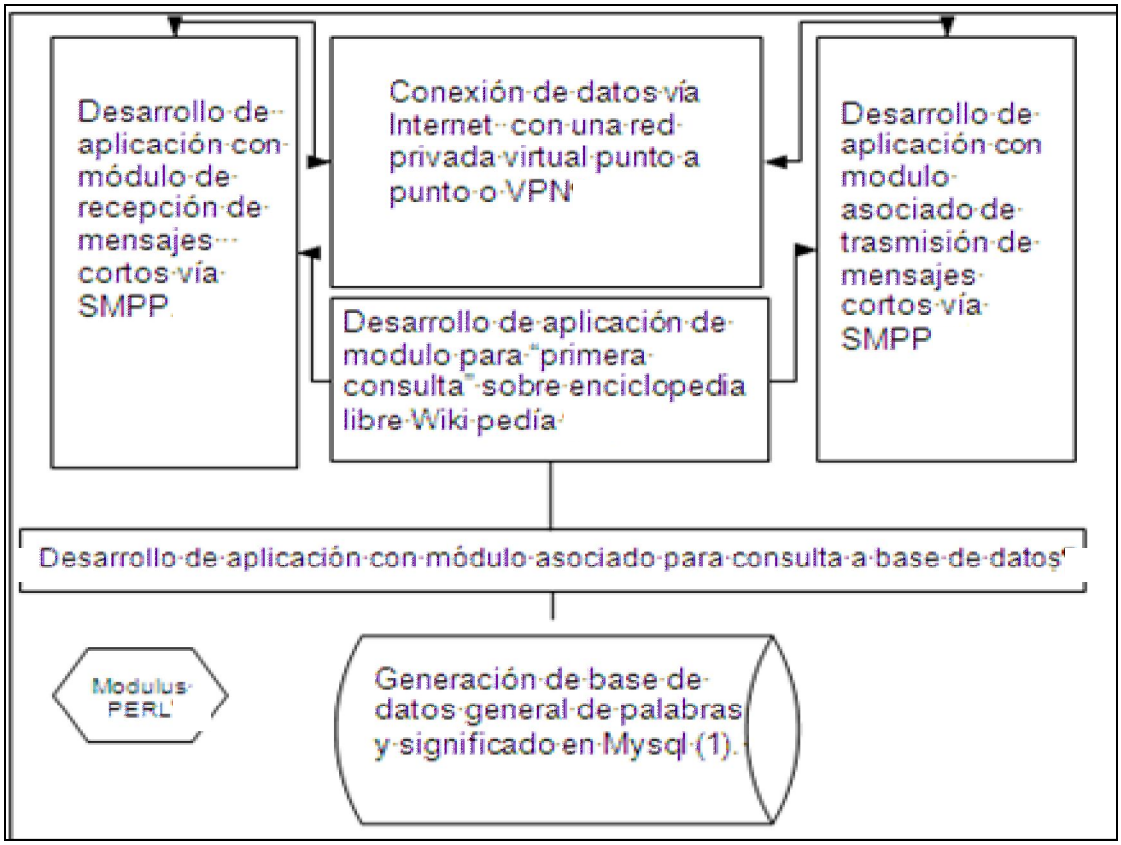
- Desarrollo de aplicación con módulo de recepción de mensajes cortos vía SMPP.

- Desarrollo de aplicación con módulo asociado de transmisión de mensajes cortos vía SMPP.

- Instalación de módulos Perl

    - Net::SMPP, y www::Wikipedia
    - DBI

Figura 43. **Modelo de Programación PERL**



Fuente: elaboración propia.

5.1. Modelado en bloques de la interfaz

El modelado de bloques de la interface se realizó con base en las partes de comunicación o funciones del mismo. Como se expuso anteriormente la modelación general puede dividirse en:

- Parte SMPP (TX, RX)
- Parte de información (DB y conexión a Wikipedía)
- Parte operacional (módulos, scripts, logs)

De esta manera, por ejemplo, la parte de SMPP tiene una estructura como la siguiente:

- Declaración de perl {}
- Declaración de variables
- Declaración de subrutinas
- Funcione o bloque de recepción
- Función o bloque de transmisión
- Llamada a bloque de consulta

5.1.1. Introducción de PERL

Perl es un lenguaje de programación diseñado por Larry Wall en 1987. Perl toma características del lenguaje C, del lenguaje interpretado Shell (sh), AWK, sed, Lisp en un grado inferior de muchos otros lenguajes de programación.

Estructuralmente, Perl está basado en un estilo de bloques como los del C o AWK y fue ampliamente adoptado por su destreza en el procesador de texto y no tener ninguna de las limitaciones de los otros lenguajes de script.

El nombre es descrito ocasionalmente como PERL que significa lenguaje práctico para la extracción e informe (Practical Extraction and Report Language).

Perl es un lenguaje de propósito general, originalmente desarrollado para la manipulación de texto que ahora es utilizado para un amplio rango de tareas incluyendo administración de sistemas, desarrollo web, programación en red, desarrollo de GUI y más.

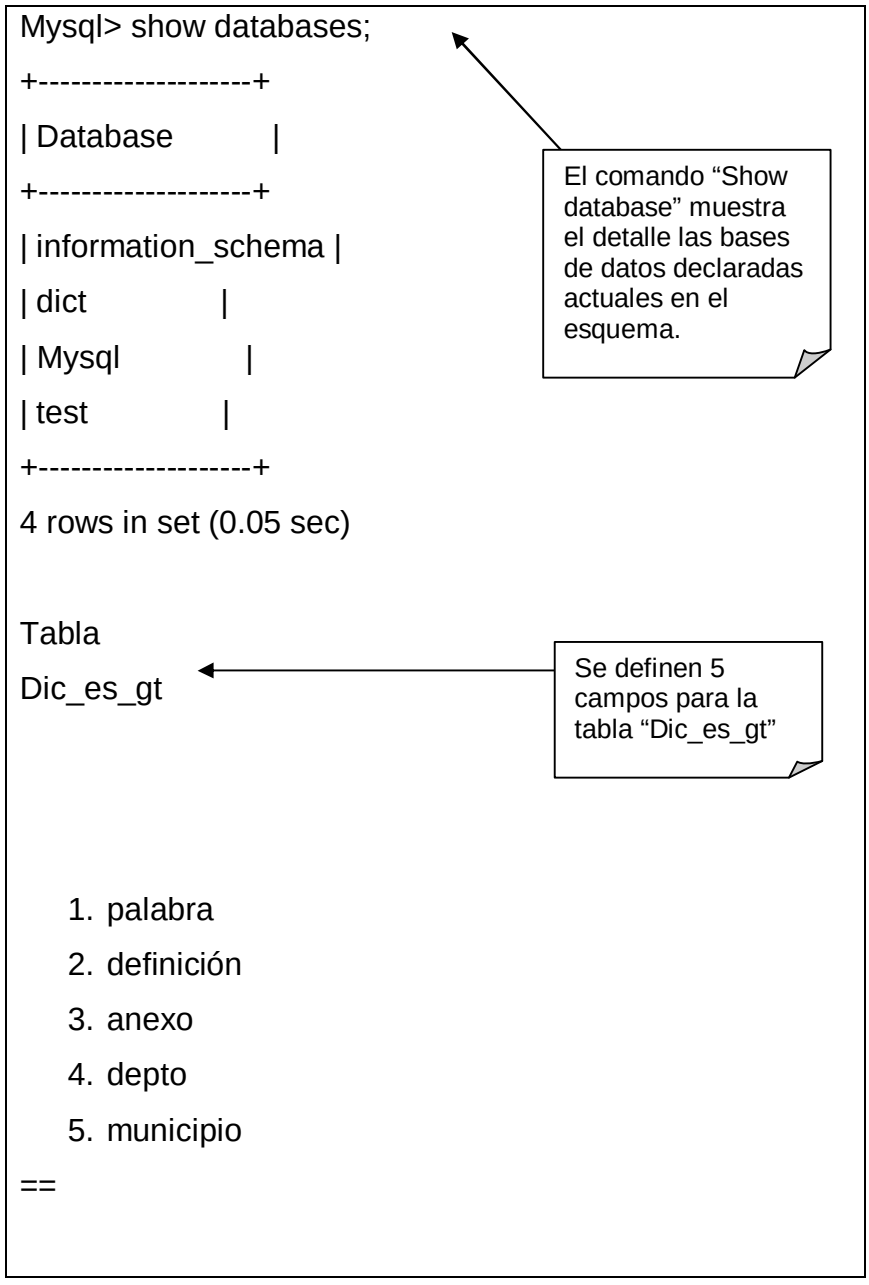
Se previó que fuera práctico (facilidad de uso, eficiente, completo) en lugar de hermoso (pequeño, elegante, mínimo). Sus principales características son que es fácil de usar, soporta tanto la programación estructurada como la programación orientada a objetos y la programación funcional, tiene incorporado un poderoso sistema de procesamiento de texto y una enorme colección de módulos disponibles.

5.1.2. Base de datos

El procedimiento de creación de base de datos parte desde la carga o base de datos, se asigna el nombre dict como identificador del esquema diccionario, a continuación se describe brevemente el procedimiento de creación, con su respectivo comando en SQL (Ver figuras 44, 45 y 46 como referencia)

Mysql es un sistema de gestión de base de datos relacional, multi-hilo y multiusuario con más de seis millones de instalaciones. Mysql AB, desde enero de 2008 una subsidiaria de Sun Microsystems y Oracle Corporation desde abril de 2009, desarrolla Mysql como software libre en un esquema de licenciamiento dual.

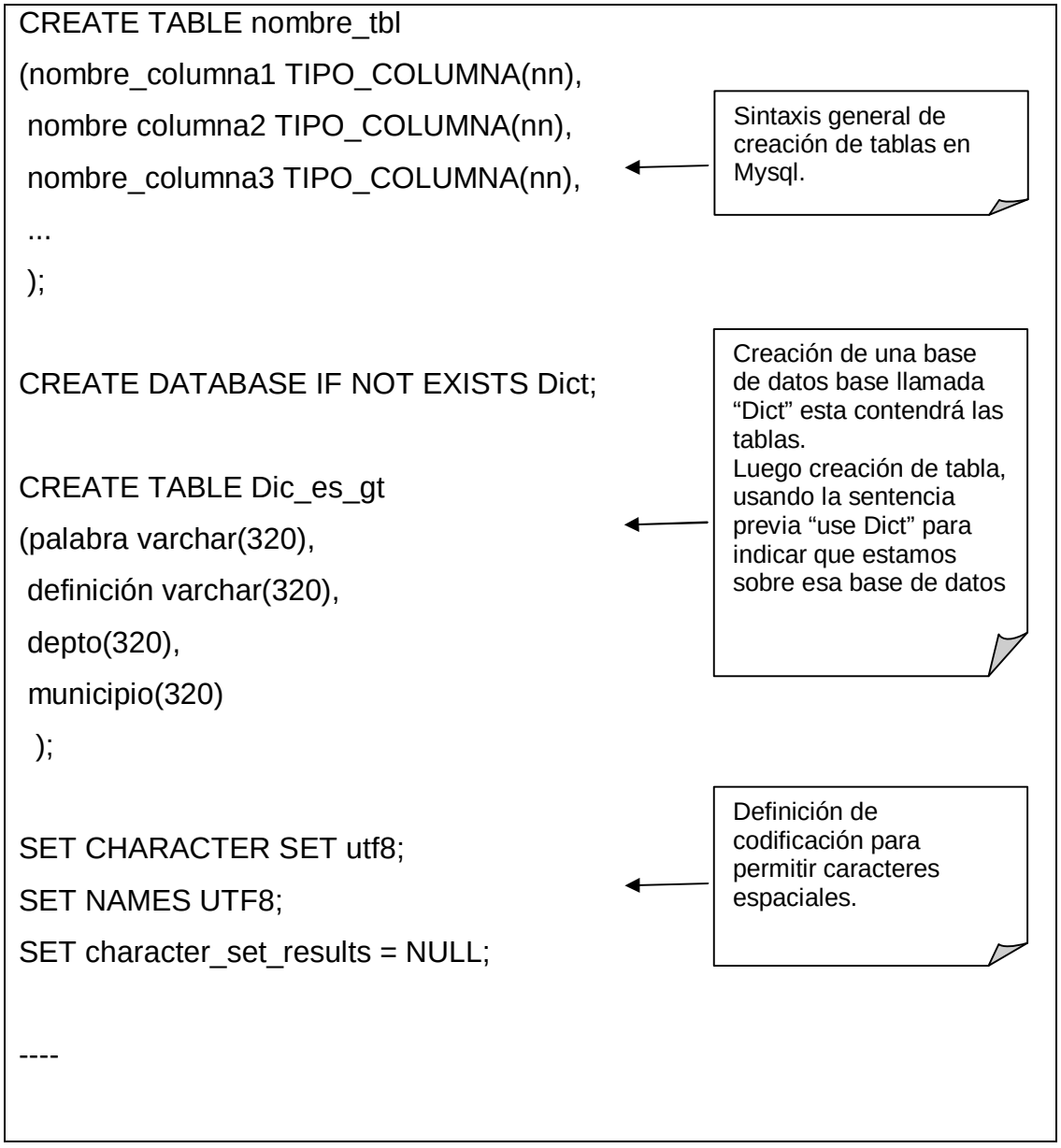
Figura 44. **Uso de base de datos Mysql**



Fuente: elaboración propia.

Sintaxis SQL de proceso de creación de código, la sintaxis descrita en la figura 45, muestra los componentes básicos del código.

Figura 45. **Creación de tabla en una base de datos**



Fuente: elaboración propia.

Ejemplo de consulta (requerimiento) sobre la base de datos, construyendo la consulta con la palabra abatible y consultando en la tabla Dic_es (figura 46):

Figura 46. **Ejemplo de consulta en una base de datos**

```
select * from Dic_es_gt where palabra like '%abatible%';
ALTER DATABASE Dict DEFAULT CHARACTER SET utf8 COLLATE utf8_general_ci;
```

Fuente: elaboración propia.

5.1.2.1. Creación de bases de datos y tablas

Para la creación de nuevas bases de datos, como se describió anteriormente, basta sencillamente usar la orden create database nombre_db que se limita a habilitar un nuevo directorio para los datos de la nueva base. Se puede completar la orden con la cláusula create database if not exists db_nombre en cuyo caso la nueva base de datos sólo se intentará crear si no existe otra con el mismo nombre. Si no usamos IF NOT EXISTS y el nuevo nombre está duplicado, Mysql avisará del error y no ejecutará acción ninguna.

La creación de tablas tiene muchas más opciones, ya que aquí no se limita a reservar un espacio, sino que hay que crear la propia estructura de la tabla. La sintaxis general es create table…. campo, valor

Es decir, para cada columna se debe especificar su nombre, su tipo (char, varchar, int, etc.) y su longitud.

Un buen diseño de la tabla determinará el éxito o fracaso de la base de datos. Existen abundantes estudios acerca de la normalización de las bases de datos, cuya complejidad excede de las posibilidades de este documento. A un nivel mucho más básico se puede indicar que la sola elección del tipo de tabla adecuado y del tipo (y longitud) de datos de cada columna tendrá su reflejo en la rapidez y eficacia del sistema.

La tabla se creará en la base de datos que esté en uso en ese momento. También, se puede crear específicamente, la tabla en otra base de datos del mismo servidor, usando la sintaxis create table bd_nombre.tabla_nombre.

Algunas reglas por recordar son las siguientes:

Longitud: es opcional salvo para los campos tipo decimal numeric char y varchar. Por ejemplo: create table mi_tabla (id_field int(4));.

Las columnas tipo INT pueden albergar desde -2147463846 a 2147483647 (unsigned). Al fijar el rango en 4, se limita desde -999 a 9999. Mysql guardará correctamente el dato fuera del rango especificado, siempre que no esté, además, fuera del rango para ese tipo de columna.

Para datatypes no numéricos, el rango determina el número fijo de caracteres almacenados en cada caso (char) o el número máximo permitido (por. ejemplo. varchar).

Valor decimal, máximo número de decimales para aquellos datatypes que admiten decimales. Si el número a almacenar tiene más, será redondeado:

- Float (5,2)

    - 2.14 se almacena como 2.14.
    - 32.147 se almacena como 32.15 (5 caracteres en total).
    - 232.14 se almacena como 232.1 es decir, un número máximo de 5 carácteres, un número máximo (si caben en el total) de 2 decimales.

El atributo binary puede usarse con char y varchar, con el único efecto de que en caso de búsqueda distinguirá mayúsculas y minúsculas. El atributo zerofill sólo puede emplearse con datos tipo numérico. El atributo unsigned sólo puede emplearse con datos del tipo numérico entero. Cada columna (independientemente de su tipo) puede ser null o not null. Si no especifica nada, se asume que la columna es null.

Las columnas (salvo que sean auto_increment) siempre tienen un valor por defecto. Si la columna es tipo null el valor por defecto es justamente ese, null. Si es not null y la columna numérica, el valor por defecto es 0. Si la columna no es tipo numérica el valor por defecto será "" (cadena vacía). Puede establecerse un valor por defecto propio con default.

Sólo puede existir una columna auto_increment por tabla, que debe ser del tipo entero y además not_null.

La columna auto_increment siempre será considerada como índice primario (primary key).

En Mysql los índices se llaman (indistintamente) key o index. En principio se puede indexar cualquier columna, sea cual sea su tipo, aunque algunas son más idóneas que otras. Un index puede ser unique, en cuyo caso esa columna no podrá tener datos repetidos.

Primary key es un índex sobre una columna not null y unique (que no puede estar vacía ni tener valores repetidos); es decir que la columna no puede tener valores vacíos o duplicados.

Aunque sólo puede haber un primary key por tabla, puede tener tantos índices como se quiera (o debas) y puede crear not null y unique.

Solamente puede haber una columna auto_increment y existir un índice primary key (aunque se puede formar un primary key sobre dos o más columnas).

Es posible indicar la longitud del índice. En ese caso, sólo se indexarán los primeros caracteres de cada campo hasta la longitud indicada. La indicación de longitud es opcional para los campos char y varchar y obligatorio para los campos de las familias text y blob.

Las columnas tipo char, varchar y text pueden ser indexadas además como fulltext.

5.1.3. Interfaz SMPP

El protocolo SMPP, a pesar de su nombre, define a un cliente (ESME) y un servidor (a menudo llamado SMSC en el operador móvil). El cliente por lo general, inicia la conexión TCP y un requerimiento bind para iniciar sesión.

Después del requerimiento, hay una serie de pares respuesta-solicitud llamada PDU, éstas se intercambian entre las partes. La solicitud puede ser iniciada por cualquiera de los extremos (de ahí peer-to-peer) y el otro extremo responde. Las solicitudes son numeradas con una referencia o secuencia y cada respuesta tiene correspondientes sus números de secuencia. Esto permite que varias solicitudes puedan quedar pendientes en el mismo tiempo y puedan convivir. Conceptualmente, esto es similar a IMAP o las identificaciones de mensaje LDAP.

Por lo general, el objeto SMPP mantiene los números de secuencia por sí mismo y el programador no necesita preocuparse por sus valores exactos, el argumento siguiente puede suministrarse a cualquier solicitud o método de respuesta.

Normalmente, el protocolo SMPP funciona en modo síncrono, es decir que un método que envía una solicitud, también se bloqueará hasta que se obtiene la respuesta correspondiente. El comando interno utilizado para esperar la respuesta es según la figura 47.

Figura 47. **Respuesta en el código para SMPP**

```
$resp_pdu = $smpp->wait_pdu($cmd_id, $seq);
```

Fuente: elaboración propia.

Si mientras se espera una respuesta particular, otros PDU's son recibidos éstos son manejados por el manejador configurado por el constructor o descartados.

Ambos, código comando y número de secuencia deben coincidir. Típicamente un manejador para el comando enquire es tomado, mientras otros comandos son rechazados silenciosamente. Esta práctica puede ser no muy recomendable para un modo transceptor y aún menos, para una implementación tipo SMSC.

La operación síncrona hace imposible intercalar operaciones SMPP, de allí que éste debe ser relacionado sólo a modelo de programación de tareas simples. Cualquiera que quiera un control más avanzado debería de usar un modelo asíncrono y de tomarse la tarea de entender e implementar más del flujo del mensaje dentro de su propia aplicación

En el modo síncrono el método de petición devuelven un objeto PDU Net:: SMPP:: PDU representando la respuesta, si todo va bien con el protocolo o undef si hubo un error a nivel de protocolo. Si un undef fue devuelto, la razón se puede extraer de $(*) ($ SMPP SMPPerror) y $(*) ($ SMPP SMPPerrorcode) (los códigos actuales no están documentados en este momento, pero se garantiza que no tendrán cambio) las variables y la variable global $!. Estas variables no tienen sentido si cualquier otra cosa que un undef es devuelta. La respuesta en sí misma puede ser una respuesta de error si hay un nivel de aplicación de error en el extremo remoto. En este caso, la del error a nivel de aplicación puede determinarse a partir del campo $ PDU-> (status). Algunas respuestas, también tienen parámetros opcionales y amplían la explicación de la falla.

Si un error a nivel de protocolo ocurre, probablemente la única acción segura sea destruir el objeto de conexión (por ejemplo un undef $SMPP). Si un error a nivel de aplicación ocurre, entonces depende de cómo fue implementado

El extremo remoto puede ser posible de continuar con la operación. El módulo puede también ser usado asincrónicamente especificando async=>1 en el constructor. En este modo el método de comando o primitiva retorna inmediatamente devolviendo el número de secuencia del PDU y se debe usar una respuesta usando el comando mostrado en la figura 48.

Figura 48. **Respuesta en el código para identificación**

```
$pdu = $smpp->wait_pdu($cmd_id, $seq);
```

Fuente: elaboración propia.

Típicamente el wait_PDU() es utilizado para la espera de un PDU, pero si éste es usado para la espera de un comando, el requirente debe generar una respuesta apropiada como se muestra en la figura 49:

Figura 49. **Lectura de comando SMPP**

```
$pdu = $smpp->read_pdu();
```

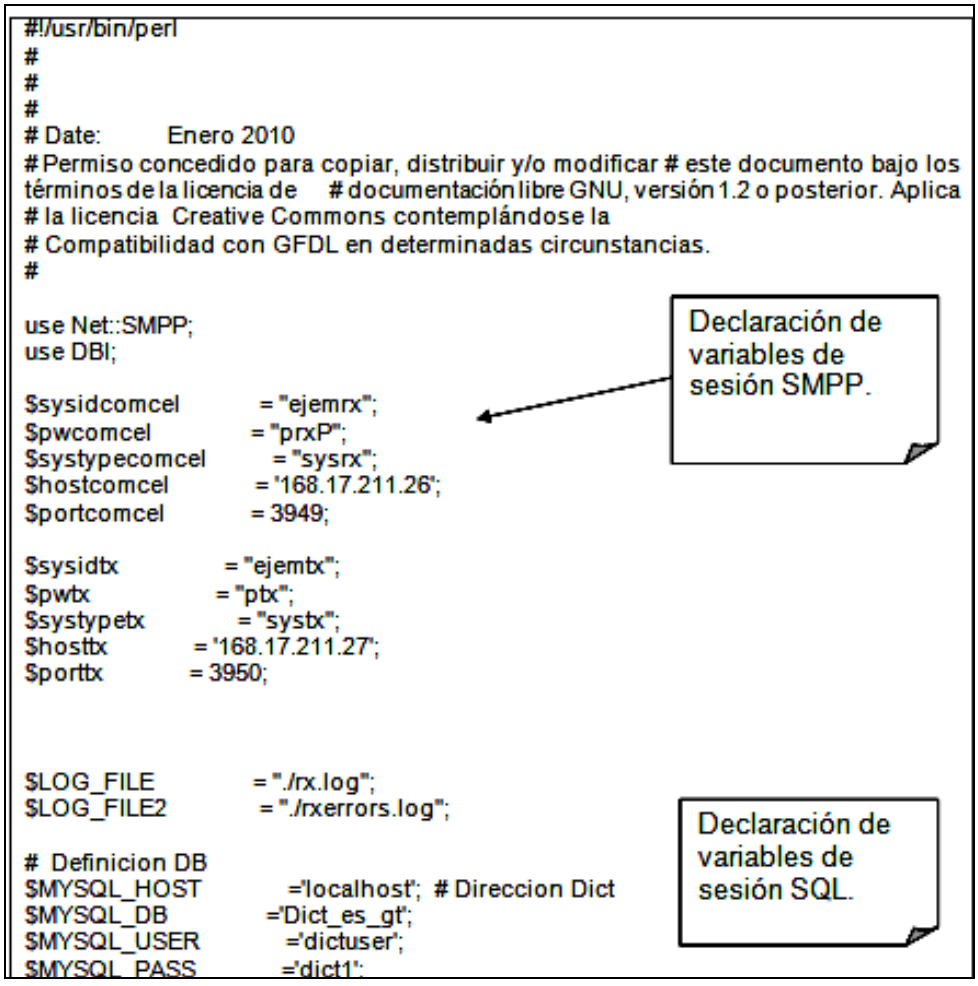
Fuente: elaboración propia.

La cual se bloqueará hasta que un PDU es recibido en la trama. El origen debería entonces, revisar si el PDU es una respuesta o un requerimiento y tomar la acción adecuada. Si el origen no desea bloquear sobre el wait_PDU() or read_pdu(), Éste debería usar un select() para verificar si el puerto está listo para lectura. Aún así, el puerto esté listo para lectura, podría no haber suficientes datos para completar el PDU, entonces la llamada debería ser bloqueada. Actualmente no hay ningún mecanismo efectivo para evitar esto.

El método de respuesta siempre retorna el número de secuencia, no importando si es un modo síncrono, asíncrono o si un error undef sucede.

Tomando lo anterior como base, a continuación se muestra en la figura 50 el código que integra solicitud de conexión y recepción envío y manejo de PDU de mensaje ejemplificando el uso de módulo NET::SMPP.

Figura 50. **Ejemplo de código Perl**



Continuación de la figura 50.

```
sub printlog {
        my $txt         = shift;
        my $fecha       = localtime;
        open (LOG, ">>$LOG_FILE");
        print LOG "$fecha: $txt";
        close LOG;
        return;
}

sub printlog2 {
        my $txt         = shift;
        my $fecha       = localtime;
        open (LOG, ">>$LOG_FILE2");
        print LOG "$fecha: $txt";
        close LOG;
        return;
}

#  Conexion SMSC_Rx
($smpp2, $resp2) = Net::SMPP->new_receiver($hostcomcel,
                    system_id       => $sysidcomcel,
                    password        => $pwcomcel,
                    addr_ton        => 0x01,
                    addr_npi        => 0x01,
                    source_addr_ton  => 0x01,
                    source_addr_npi  => 0x01,
                    dest_addr_ton    => 0x01,
                    dest_addr_npi    => 0x01,
                    system_type      => $systypecomcel,
                    port            => $portcomcel,
                    #..
                    smpp_version => 0x34,
                    )
   or die "No se estableció la conexión Receiver\n";

#  Conexión SMSC_Tx

  ($smpp, $resp) = Net::SMPP->new_transmitter($hosttx,
                    system_id       => $sysidtx,
                    password        => $pwtx,
                    addr_ton        => 0x00,
                    addr_npi        => 0x00,
                    source_addr_ton  => 0x00,
                    source_addr_npi  => 0x00,
                    dest_addr_ton    => 0x00,
                    dest_addr_npi    => 0x00,
                   #async            => 1,
                    system_type      => $systypetx,
                    port            => $porttx,
                    smpp_version => 0x34,
                    )
```

Conexión Rx, ésta recibe cada mensaje proveniente desde el operador de telefonía.

Continuación de la figura 50.

```
printlog "\n\tENVIANDO de esme A COMCEL\n";

while (1){
      $pdu = $smpp2->read_pdu() or die"$$: PDU not read\n";

   $nombre_pdu =  Net::SMPP::pdu_tab->{$pdu->{cmd}}{cmd};
                  $seq_pdu    =  $pdu->{seq};
                  $tipo_pdu   =  $pdu->{cmd};
                  $celular    =  $pdu->{source_addr};
                  $msg_id     =  $pdu->{message_id};
                  $destino    =  $pdu->{destination_addr};
                  $mensaje    =  $pdu->{short_message};

if($tipo_pdu == 5){
            $smpp2->deliver_sm_resp(message_id => "1234567", seq =>$seq_pdu);

        if (($celular eq 'agw') || ($celular eq '50255999998')){
            printlog2 "MO: $celular\tMT: $destino\n";
        }else{
            $resp = $smpp->submit_sm(  source_addr => $destino,
                                       destination_addr =>$celular,
                                       short_message=>$mensaje,
                                       service_type => '',       # default ok
                                       source_addr_ton => 0x00, # default ok
                                       source_addr_npi => 0x00, # default ok
                                       dest_addr_ton => 0x00,    # default ok
                                       dest_addr_npi => 0x00,    # default ok
                                       esm_class => 0x00,        # default ok
                                       protocol_id => 0x00,      # default ok on CDMA,TDMA
                                       priority_flag => 0x00,    # default ok
                                       schedule_delivery_time => '', # default ok
                                       validity_period => '',        # default ok
                                       registered_delivery => 0x00,  # default ok
                                       replace_if_present_flag => 0x00, # default ok
                                       data_coding => 0x00,      # default ok
                                       sm_default_msg_id => 0x00,    # default ok

                                    )
            or printlog "ERROR No se envío el SMS a $destino\n";
            $resultado = $resp->{message_id};
            if($resultado){
                  #$resultado = "OK";
            }else{
                  $resultado = "ERROR  $resp->{status}";
            }
            printlog  "MO: $celular\t MT: $destino\t Msg_id: $resultado\n";
            #printlog  "Terminated: $destino\n";
            #printlog  "Msg_id: $resultado\n\n";
        }
      }
```

Lectura y asignación de campos de PDU de mensaje a variables

Continuación de la figura 50.

```
    if($tipo_pdu == 21){
        $smpp2->enquire_link_resp (seq => $seq_pdu);
        $smpp->enquire_link();
        printlog2 "Enquiry_link_resp $seq_pdu \n\n";
    }
}
$smpp2->unbind();
$smpp->unbind();
#EOF
```

Fuente: elaboración propia.

5.1.4. Carga y modificación de datos

Para el proyecto se utilizaron dos métodos de extracción de datos, evitando cualquier conflicto de derechos de autor, utilizando el diccionario de OPENOFFICE programa de uso libre y gratuito bajo licencia opensource (ver figura 52), se creó un archivo de texto, agregándole formato y separación de campos para una fácil lectura de línea por línea y su posterior carga a una tabla.

Como complemento y previendo la actualización de términos, también se ha agregado un módulo de consulta tipo texto en línea hacia wikipedia, enciclopedia libre. Se hace mención que todo el contenido tomado de wikipedia se hace bajo el uso de licencia GNU (ver figura 51) y Creative commun, no se copia ninguna imagen y el resultado podrá ser redistribuido y usado en estos mismos términos.

Figura 51. **Nota de licencia GNU**

The licenses Wikipedia uses grant free access to our content in the same sense that free software is licensed freely. Wikipedia content can be copied, modified, and redistributed if and only if the copied version is made available on the same terms to others and ACKnowledgment of the authors of the Wikipedia article used is included (a link bACK to the article is generally thought to satisfy the attribution requirement; see below for more details). Copied Wikipedia content will therefore remain free under appropriate license and can continue to be used by anyone subject to certain restrictions, most of which aim to ensure that freedom. This principle is known as **copyleft** in contrast to typical copyright licenses.

To this end,

- **Permission is granted** to copy, distribute and/or modify Wikipedia's text under the terms of the Creative Commons Attribution-ShareAlike 3.0 Unported License and, unless otherwise noted, the GNU Free Documentation License. Unversioned, with no invariant sections, front-cover texts, or bACK-cover texts.

Fuente: Wikipedia. Wikipedia_Copyright. Consuta: 12 de enero de 2010.

Figura 52. **Nota de licencia código abierto**

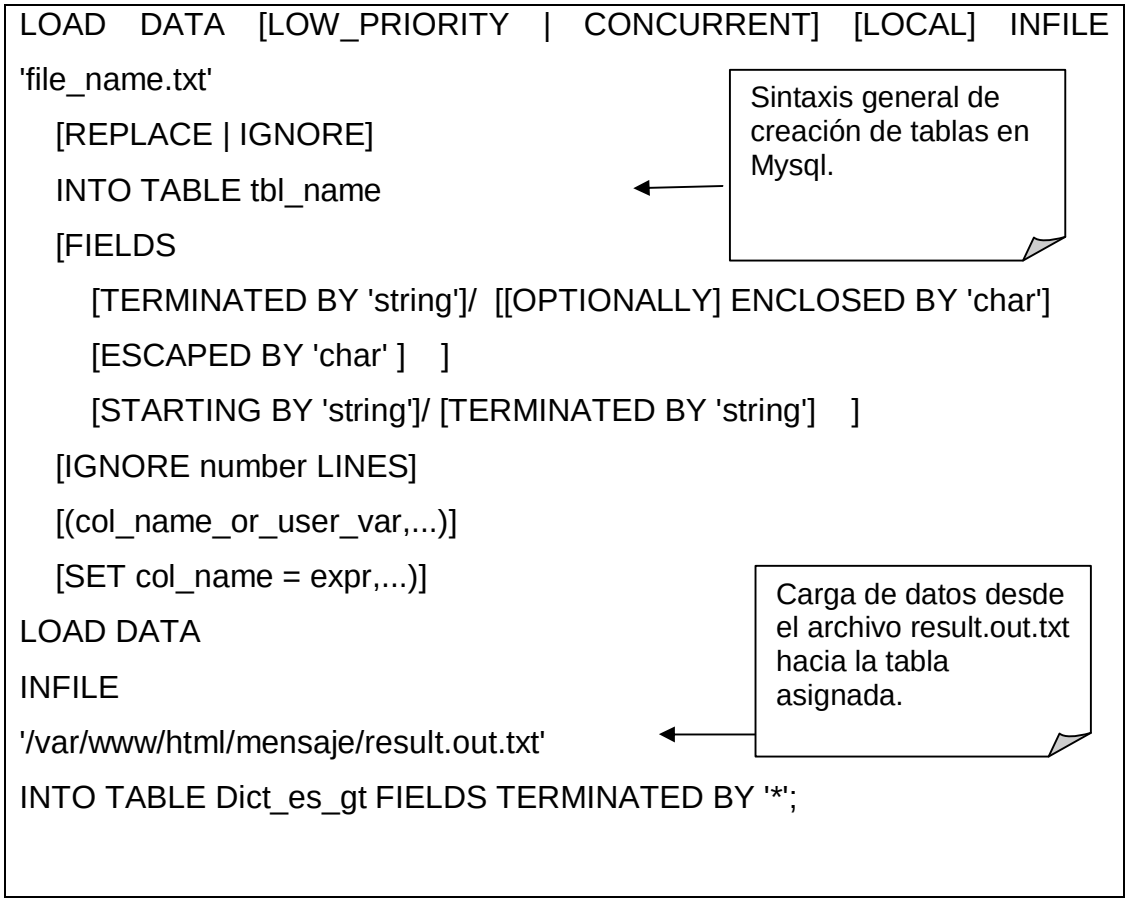
1. Free Redistribution

The license shall not restrict any party from selling or giving away the software as a component of an aggregate software distribution containing programs from several different sources. The license shall not require a royalty or other fee for such sale.

Fuente: Open source consorcio. Consuta: 12 de enero de 2010.

La carga datos desde un archivo de texto a los campos de la tabla (comúnmente conocidos como tuplas) se muestra en la figura 53.

Figura 53. **Carga masiva de datos Mysql**



Fuente: elaboración propia.

6. REALIZACIÓN DE ANÁLISIS ECONÓMICO Y APLICATIVO EN EL ÁMBITO DE APLICACIONES DE SMS

¿Qué parámetros se utilizaron para decidir si el proyecto era viable económicamente y en qué medio se desarrolla?

¿Quién es el usuario final y qué utilidad tiene para la empresa, el gobierno y la sociedad en general?

Para responder estas interrogantes, se presentan a continuación los pasos básicos de análisis y decisión utilizados y una breve explicación.

6.1. Racionalidad económica del proyecto

A continuación se definen conceptos que apoyan el desarrollo del proyecto:

- Forecast o proyección en el tiempo de cantidad de transacciones en un tiempo determinado.

- Costos de VPN: se conoce como un costo hundido, ya que tanto CONCYT como TIGO, ya poseen infraestructura y enlaces para este fin, esto quiere decir, que en el costo total no hay un costo fijo o variable para este proyecto, considerando que ya se paga por este servicio.

- Costos de mantenimiento y operación de servidores, este costo tampoco se agrega ya que no hay nuevos servidores ni se contratará nuevo personal para operar los ya existentes.
- Costo operativo en salarios y suministros: tampoco varía ni los costos operativos, red, medio, personal; ni tampoco varía o se agregan suministros nuevos o más cantidad de los ya existentes.

6.2. Contexto macroeconómico y sectorial

Siendo éste, un ámbito de tecnología y comunicaciones el efecto macroeconómico podría influir en una mejor forma de producir (mejora de productividad) y mejor acceso de información.

6.3. Acercamiento integral del análisis económico

El alcance económico social es limitado al escenario medios vs. acceso y facilidad de uso del medio, eso quiere decir, que se le da más facilidad de uso y en cualquier parte a un usuario aplicando la funcionalidad de este proyecto.

6.4. Framework o marco de aplicación

Se puede establecer entonces, un marco para sostener el análisis, como sigue:

- Entrada – Salida: la entrada se identifica como la necesidad o posibilidad de información inmediata, la salida como facilidad de acceso y la satisfacción de la necesidad de información inmediata.

- ¿Qué afecta?: el proyecto afecta la forma de hacer una consulta o búsqueda de información y probablemente la percepción de uso de los mensajes cortos como entretenimiento.

- ¿Cómo, cuánto?: el proyecto se desarrolla en una red GSM con 5,5 millones de usuarios como lo es TIGO, se agrega y designa un número corto destino por parte del operador telefónico, se establecen los datos técnicos de conexión punto a punto, se asignan también por parte del proveedor los parámetros de conexión SMPP, con lo anterior se establece la aplicación y verifica el cobro por parte del proveedor así como el flujo de entrega de respuesta al usuario. El operador concilia la cantidad de mensajes por aplicación y así verifica el ingreso neto de la aplicación por semana o mes y la cantidad de mensajes recibidos.

6.5. Análisis financiero y económico

En el análisis financiero se estiman las ganancias del proyecto, operativamente hablando.

El análisis económico mide el efecto del proyecto de forma integral o nacional, para que un proyecto sea económicamente viable debe ser financieramente posible así como económicamente eficiente.

El análisis financiero entonces, se dedica a la verificación de las ganancias o ingresos derivados del proyecto y su costo beneficio, en cambio el análisis económico se ocupa de términos monetarios, pero tomando en cuenta la sociedad completa y su disposición a pagar un producto o servicio y mide también, los efectos positivos y negativos del proyecto.

6.5.1. Identificación y cuantificación de costos y beneficios

Pera cuantificar el proyecto se sigue el proceso básico de: identificar los costos y beneficios económicos; costos y beneficios pueden dividirse en software o aplicación y hardware o infraestructura, cuantificar los costos y beneficios lo más posible (ver tabla XIX), valuar los costos y beneficios.

Tabla XIX. **Relación costo beneficio**

Aspecto	Costo	Beneficio
Aplicación (software)	Operadora (costo hundido) CONCYT Q.0,00	Comercial Operadora = Q.0,40 por mensaje corto. No comercial CONCYT = Palanca de servicio móviles y tecnológicos.
Infraestructura (hardware)	Operadora (costo hundido) CONCYT Q.0,00 (costo hundido)	
Comparación	Costo ya adquirido en infraestructura y servicios (el concepto de hundido es el costo ya adquirido valuado o pagado.)	Beneficio con mínima inversión y adquisición de ventajas en conocimiento y diversidad. A mayor cantidad de mensajes mayor ingreso incremental

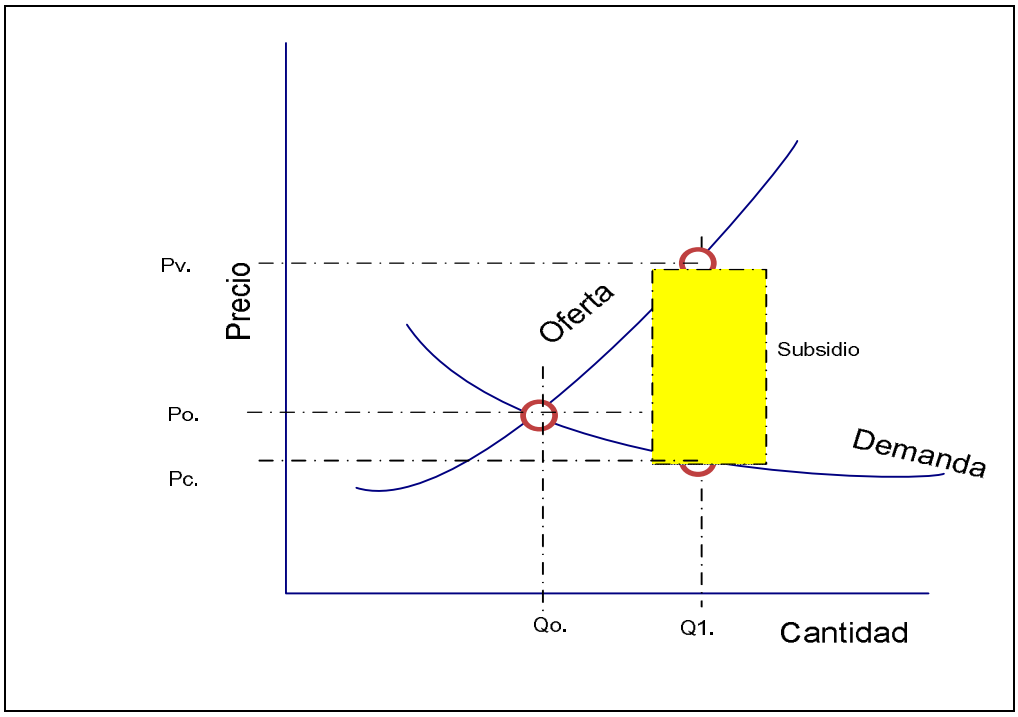
Fuente: elaboración propia.

6.5.2. Valuación de los costos y beneficios financieros

- Consideraciones generales: tomar en cuenta qué factor afecta los beneficios financieros, considerando qué costos y beneficios potenciales se tienen y cuáles beneficios son económicos y cuáles no comerciales o económicos.

- Rol del precio: el precio afecta la oferta y la demanda, si se considera como un subsidio el que CONCYT no perciba ningún ingreso se podría afirmar que el precio al cliente final o usuario potencial del servicio podrá usar la aplicación a un precio más bajo que si fuera un producto comercial 100 por ciento. (ver figura 54)

Figura 54. **Relación del precio contra la oferta y la demanda**



Fuente: elaboración propia.

- Precio económico comercial y no comercial: el precio comercial, como se mencionó antes será de Q.0,40 y el precio no comercial podría definirse como el aporte de valor a lo que el usuario está dispuesto a pagar por no tener un diccionario impreso cerca o inmediato del servicio y respuesta.

- Del precio económico a la base común: en este paso se puede determinar si hay algún precio de frontera o de cambio que pueda influir directa o indirectamente al precio real, en este caso podría variar por la tasa de cambio.

- Viabilidad Económica: el proyecto es viable aún así tenga crecimiento limitado, por el bajo nivel de inversión requerida.

6.5.3. Menor costo y análisis costo efectivo

Este paso se realiza haciendo los supuestos de mínimo precio y precio de equilibrio, de allí que el mínimo precio sería cero, pero no justifica el riesgo de una nueva conexión y utilización de recursos y licencias del lado del operador, el precio de equilibrio, entonces es el de costo mínimo del operador con un descuento máximo del lado de CONCYT, es decir, que el precio normal de un mensaje corto es de Q.0,40 que es el precio mínimo del operador.

6.5.4. Criterio de inversión: viabilidad económica

Los criterios incluyen variables como:

- Decisión de proyecto: un número corto con conexión básica.

- Decisión de alternativas: cuando los beneficios no son valorables y cuando lo son, indica el valor social y de conocimiento por el lado no valorable cuantitativamente y el análisis de crecimiento de cobro de servicio por el lado cuantificable y medible económicamente.

Prueba de la viabilidad económica de la mejor alternativa: la mejor alternativa se considera como aquella en la que le valor presente neto es mayor que cero o que representa un aprovechamiento de costo oportunidad, de esta forma el valor presente neto para el operador telefónico se puede considerar como mayor que cero y para CONCYT como cero pero con un costo oportunidad importante, tomando esto en cuenta el proyecto es viable económicamente.

Escogencia de tasa de descuento: la tendencia de descuento debería ser verificada luego del lanzamiento, pudiendo aplicar promociones limitadas en tiempo o en uso.

Inversión del proyecto y presupuesto: considerando valores de horas hombre en el mercado dos ingenieros trabajando 4 horas diarias durante 3 meses de desarrollo y evaluación. En la tabla XX se muestra un estimado.

Tabla XX. **Relación horas vs. costo del proyecto**

Horas hombre	Costo promedio de horas hombre
90 horas (desarrollo)	Q.62,5 = Q.5 000,00 En desarrollo y pruebas

Fuente: elaboración propia.

Se debe incluir el costo de publicidad y mercadeo. El costo de desarrollo se diluye en el tiempo de EPS y el de publicidad en la promoción de tecnología probablemente programado y proyectado por CONCYT.

6.5.5. Análisis de incerteza y riegos

Para el análisis de incertezas y riegos se tomaron factores que podían afectar el proyecto. Los posibles riesgos son:

- Productos substitutos.
- Necesidades de ilustración o imágenes del usuario.
- Productos alternos que puede escoger el usuario prefiriéndolos antes que la aplicación.

6.5.6. Sustentabilidad de los efectos del proyecto

Los efectos esperados del producto incluyen incremento gradual de uso de tecnología en el conocimiento, facilidad de acceso, rapidez de respuesta. ¿Cómo se espera sustentar en el tiempo? incluyendo nuevas alternativas del producto que puedan hacer uso de necesidades no satisfechas del usuario.

En la tabla XXI se incluye un resumen de valores económicos, cuantitativos y cualitativos tomados para el proyecto.

Tabla XXI. **Valores económicos, cuantitativos y cualitativos del proyecto**

Fecha	29/06/2010			Tipo de Servicio	SMS
Nombre de proveedor	CONCYT			Tipo de Solicitud	Apertura
Nombre de la mecánica	Diccionario en Linea				
Número corto, URL o Asterisco	258				
Fecha Planificada de Inicio de Uso	10 de Julio 2010				
Descripción del contenido que se ofrece	Diccionario de contenido, palabras y definiciones en linea.			Categoría	Comunidad *
				Tipo de Servicio	Juegos *
Porcentaje de crecimiento esperado	3%				
Revenue Sharing (Proveedor)	0%			Tipo de Cobro	MO
Precio Quetzales (IVA 12% Incluido)	Q0.40				
				Utilice un escenario conservador	
	Mes 1	Mes 2	Mes 3		
Cantidad esperada (mensajes, descargas, llamadas) *	20,000	20,600	21,218		
Precio	Q0.40	Q0.40	Q0.40		
Costo	0	0	0		
Ingreso	8,000	8,240	8,487		
Costo	0	0	0		
utilidad esperada	8,000	8,240	8,487		

* Se debe de llenar toda la información en celdas amarillas.
* En caso no se encuentre la categoría o tipo de servicio seleccione otr@ y escríbalo en la casilla que aparecerá abajo
* Puede crear varias hojas en este mismo documento para solicitar varios destinos, cada hoja deberá llevar el numero de destino.

Indicar Mecánica a Realizar (explicación de cómo se utilizará el servicio)	Envio de un mensaje corto con una palabra que se necesite el concepto o definicion, la aplicación respondera es concepto o definicion.
Medios de Comunicación que se Utilizarán	ATL limitado a WEB, BTL Afiches educativos y promocionales.
EN CASO SE ESTE APERTURANDO UN ASTERISCO: NUMERO DE TELEFONO AL QUE SE VA A ENRUTAR EL ASTERISCO	+502 xxxx-xxxx

Fuente: ORRIOLS PÉREZ, Alejandro. TIGO Departamento de Valor Agregado.

6.6. Definición del nombre de producto

El producto será designado como: diccionario en línea con número corto asignado 258, éste ofrecerá contenido y significado de palabras bajo demanda de usuarios TIGO.

6.7. Definición de estrategia de promoción resumen

La estrategia será promover el servicio vía página de CONCYT y esquema no masivo o btl (Below the line) en carteles y comunicados de tecnología, como foco inicial en converciencia 2010.

Converciencia: es un encuentro en Guatemala de científicos nacionales que trabajan en investigación fuera el país. Con esto se busca lograr varios objetivos:

- Interesar y estimular a jóvenes estudiantes de secundaria y de universidad, en el trabajo de investigación y en la ciencia en general.

- Hacer patente, ante diferentes sectores (académico, privado y público), así como al público en general, la necesidad y la urgencia de desarrollar la ciencia y la investigación en Guatemala, para alcanzar el bienestar anhelados.

- Dar a conocer el importante y apasionante trabajo que realizan en sus laboratorios, así como lo que está ocurriendo en la frontera del conocimiento en otros países.

- Dar a conocer que en Guatemala se forman profesionales de alto valor y capacidad, reconocidos internacionalmente y que es necesario que el país genere los espacios y oportunidades para que en el futuro, las personas que estén en ese caso, puedan permanecer en Guatemala y dar su valioso aporte al desarrollo científico, económico y social.

- Propiciar un intercambio de los científicos visitantes con sus pares residentes en el país.

- Mantener activa la red internacional de científicos guatemaltecos, en la que participen todos los investigadores nacionales, tanto los que radican en el país, como quienes trabajan en el exterior.

- Recibir ideas para desarrollar con éxito algunas de las actividades del plan nacional de ciencia, tecnología e innovación 2005-2015

El programa incluye conferencias y talleres ofrecidos por los científicos visitantes sobre temas de ciencia, dirigidos a estudiantes y a público en general e intercambio de científicos visitantes con investigadores que radican en Guatemala.

En el 2005, primer año en que se celebró converciencia, acudieron a Guatemala once doctores, científicos que hacen investigación en diferentes países. En los años subsiguientes, hasta la fecha, han participado 43 científicos guatemaltecos, que no solamente han presentado conferencias y propuestas de investigaciones y proyectos, sino que han promovido el establecimiento de importantes programas de cooperación con los científicos locales, especialmente en el campo de la formación de recursos humanos de alto nivel.

6.8. Definición de tarifa resumen

Se definió una tarifa de mensaje normal Q0,40, esto por ser en un esquema de cobro total para TIGO y se cobra al origen, quiere decir el usuario que genera la consulta paga la misma.

Usualmente el esquema de negocio en las operadoras el compartir el cobro con el proveedor de contenido, entiéndase proveedor de contenido como el ESME que responde a un requerimiento de contenido o información como lo es en este caso la aplicación de diccionario.

6.9. Alcance del proyecto resumen

El proyecto como fue definido tiene un enfoque educativo e informativo, no gratis por lo atractivo para las operadoras y con un lanzamiento en TIGO.

El proyecto, aunque aplicativo, es también, documental dando las bases para que entendiendo el mundo de telecomunicaciones básicas se pueda desarrollar aplicaciones similares siguiendo los pasos de análisis, desarrollo y seguridad expuestos.

7. DOCUMENTACIÓN DE PRUEBA Y FUNCIONALIDAD DEL PROYECTO

7.1. Documentación técnica

En funcion de mantener la operación a lo largo del tiempo, una vez instalado y probado el software, se define a continuacion la documentacion base para entrega a CONCYT.

7.1.1. Documento de datos de conexión virtual

Para poder acceder a una red privada virtual punto a punto, se intercambia usualmente información para los concentradores de redes virtuales privadas o corta fuegos, esta información incluye las direcciones IP de cada corta fuegos, las direcciones del servidor o equipo de ambos lados que contienen las conexiones del protocolo SMPP, la encriptación e información de túnel seguro sobre el cual la comunicación de cliente servidor podrá ser enviada de forma segura y privada.

A continuación de muestra en la tabla XXII un ejemplo de la información intercambiada entre las partes para el establecimiento de la VPN.

Tabla XXII. **Datos de conexión VPN**

VPN Technical Contacts	TIGO	Customer VPN
Technical Support 24*7		
Name	Nombre ejemplo1 TIGO	Nombre ejemplo proveedor
Direct Phone Number	(502) 55555500	44444400
Email	Ejemplo1@TIGO.gt	Ejemplo@concyt.gob
Network Engineer		
Name	Nombre ejemplo2 TIGO	
Direct Phone Number	(502) 55555501	
Email	Ejemplo2@TIGO.gt	
VPN Gateway Device Information	**COMCEL VPN Device**	**Customer VPN Device**
VPN MODEL	ASA 5550	Watchguard X 1000 + Fireware Pro
VPN Peer IP	201.xxx.xxx.xxx	169.xxx.xxx.xxx
Encryption Domain (e.g. 12.41.110.100)	168.x.x.x	172.x.x.x
Tunnel Properties		
Phase 1	Authentication Method	Pre-Shared Key
	Encryption Scheme	IKE
	Diffie-Hellman Group	Group 2
	Encryption Algorithm	3DES
	Hashing Algorithm	SHA-1
	Main or Aggressive Mode	Main mode
	Lifetime (for renegotiation)	86400 seconds, no volume limit
Phase 2	Encapsulation (ESP or AH)	ESP
	Encryption Algorithm	3DES
	Authentication Algorithm	MD5
	Perfect Forward Secrecy	NO
	Lifetime (for renegotiation)	3600 seconds
	Lifesize in KB (for renegotiation)	Not used
	Key Exchange For Subnets	

Fuente: ORRIOLS PÉREZ, Alejandro. VPN, Plantilla de conexión de proveedores.

Se asigna internamente en TIGO una IP NAT: 172.xx.xx.xx. (dirección IP interna donde NAT indica un traslación de dirección de red, traslada una IP publica a una privada), así la llave es Pre-Shared Key: “ #jj$ddddas@123 (llave de conexión para fase 1).

7.1.2. Documentación de datos SMPP

Luego de establecer la comunicación VPN, se debe configurar en el programa de conexión del cliente en CONCYT los parámetros de conexión SMPP, ésta se muestra en la tabla XIII, estos valores son los necesarios para hacer funcionar el programa del lado del cliente para realizar una autenticación exitosa, además de valores que se usan solamente en la parte servidor, a continuación se describe brevemente haciendo referencia a la taba XXIII, cada variable:

- Nombre de conexión: se refiere al identificador del grupo de paramentos para una conexión específica, en este caso CONCYT.

- Activa: designa del lado del servidor si la conexión con estos parámetros esta activa y lista para ser usada.

- Máximo TPS: asigna transacciones por segundo a la conexión descrita en este grupo, en este caso 5 transacciones máximo.

- Número de conexiones: asigna cantidad de conexiones a esta conexión, esto es, cuántas sesiones simultáneas se permiten para el cliente.

- System ID: identificado de sistema con el que se liga la sesión a nivel SMPP.

- Password: contraseña de sesión SMPP.

- System type: tipo de sistema, cadena de conexión que liga password y System ID.

- Host: IP del cliente.

- Address range: parámetro opcional en el servidor.

- SMPP versión: versión de protocolo SMPP utilizada en la conexión, las opciones son 3.3, 3.4.

a. Número corto asociado 258.

Tabla XXIII. **Variables de conexión a nivel SMPP**

Variable	Valor
Nombre de conexión	eConcyt1
Activa	Yes
Máximo TPS	5
Número de conexiones	2
System id	Concyt
Password	Concyt1
System type	Concyt
Host	10.10.10.99
Address range	Range
SMPP version	SMPP 3.4
Outbind port	10000

Fuente: TIGO Departamento de Valor Agregado. Datos técnicos de conexión.

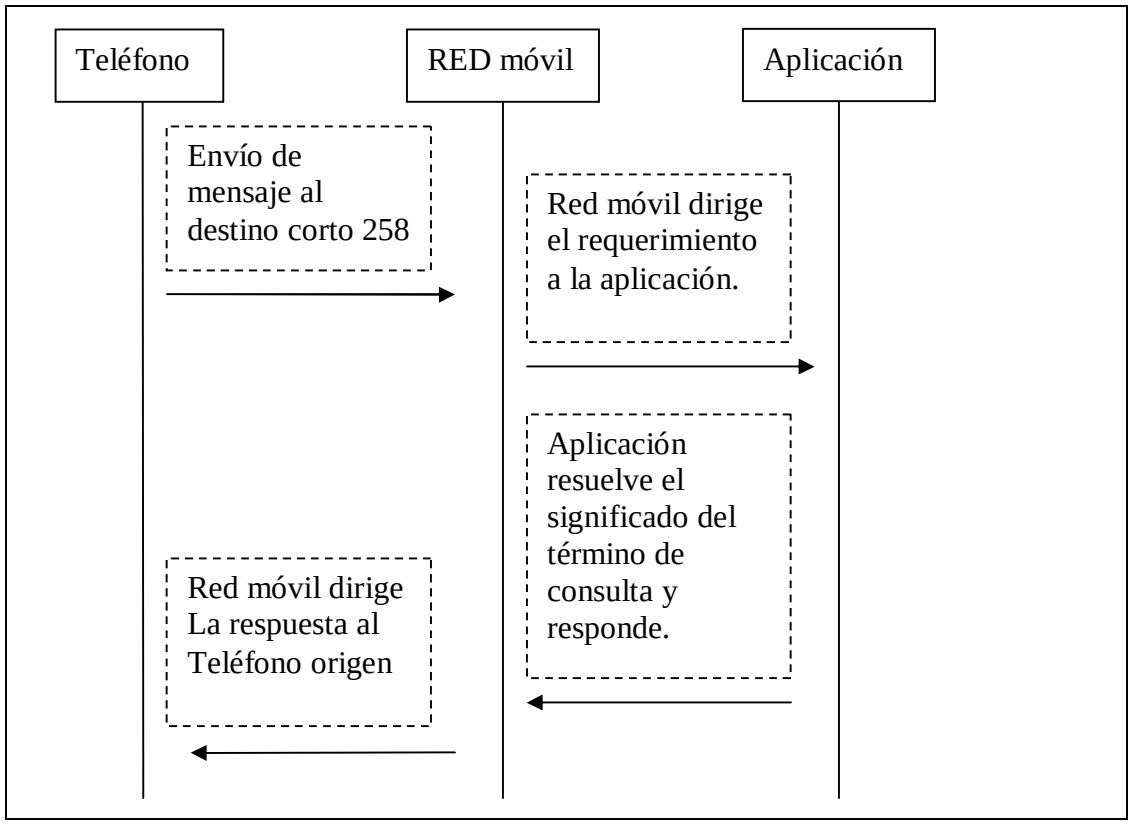
7.2. Documentación de la aceptación y prueba en entidad del CONCYT

A continuacion se detalla le funcionamiento de la interfaz y los modulos de aplicación intalados en CONCYT.

7.2.1. Manual de usuario

Un usuario final de la aplicación diccionario deberá seguir el siguiente flujo cuando requiera información de una palabra o término:

Figura 55. **Diagrama de mensajes en aplicación**

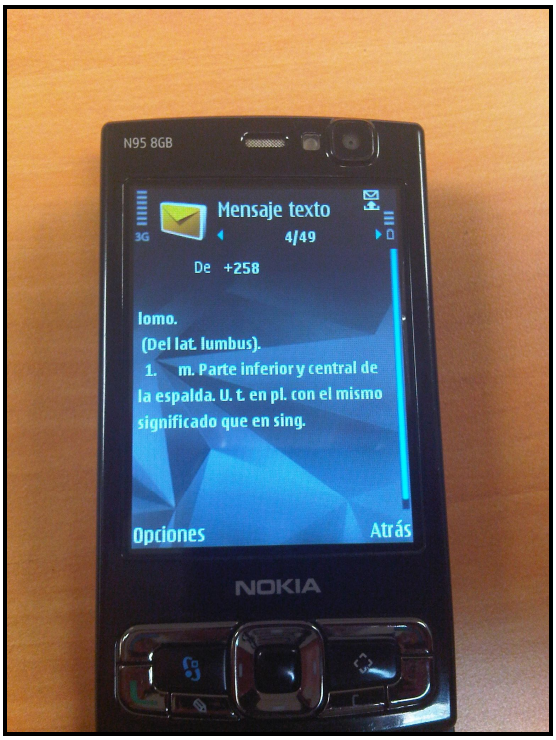


Fuente: elaboración propia.

De esta manera, como se muestra en el flujo de la figura 55, el origen será un número de celular con destino al número corto 258, al llegar a la aplicación el destino ahora será el número de celular y el origen el número corto 258.

En la figura 56 se muestra el resultado y el formato final de la respuesta, ésta tiene un encabezado que es la palabra y el resultado como cuerpo del mensaje.

Figura 56. **Resultado de envío de mensaje**



Fuente: elaboración propia.

7.2.2. Operación y mantenimiento básico

La operación y mantenimiento básico se compone de dos partes:

- Verificación de VPN: la VPN cómo alcanza un servidor al otro y determina la disponibilidad de alcanzar la red destino (ver tabla XIV) y usar el protocolo SMPP. Los pasos básicos de verificación son:

    - Ping si está habilitado en el origen y en el destino, debería mostrar algo como el ejemplo siguiente.

Tabla XXIV. **Conexión a nivel TCP-IP vía VPN**

Ejemplo “ping 10.10.10.99” PING 10.10.10.99 (10.10.10.99) 56(84) bytes of data.
64 bytes from 10.10.10.99: icmp_seq=1 ttl=63 time=0.340 ms
64 bytes from 10.10.10.99: icmp_seq=2 ttl=63 time=0.290 ms
64 bytes from 10.10.10.99: icmp_seq=3 ttl=63 time=0.284 ms
64 bytes from 10.10.10.99: icmp_seq=4 ttl=63 time=0.290 ms
64 bytes from 10.10.10.99: icmp_seq=5 ttl=63 time=0.277 ms

Fuente: elaboración propia.

    - Telnet hacia la IP destino 168.0.0.2 puerto 5610. Como se muestra en la tabla XV Este puerto es el puerto destino que determina la disponibilidad de puerto en escucha en la parte del SMSC, el Telnet lo que muestra es que se pudo establecer un vínculo sobre la VPN ya verificada, pero a un nivel más específico.

Tabla XXV. **Prueba de conexión telnet**

[root@linux ~]# telnet 168.0.0.2 5016 Trying 168.0.0.2...	Connected to 168.0.0.2 (168.0.0.2). Escape character is '^]'.

Fuente: elaboración propia Documentación y pruebas de funcionalidad.

- Ejecutar la aplicación en el cliente (servidor de CONCYT). La ejecución de la aplicación usa de los anteriores pasos la conexión y el puerto, el nivel de la aplicación envía entonces, por esos medios los datos de conexión y mantiene comunicación constante vía el protocolo SMPP.

- Verificación de aplicación: ejecuta un script Perl y le asigna una identificación de proceso (PID como se ve en la tabla XVII) al mismo, la ejecución es de la manera como se muestra en la tabla XVI:

Tabla XVI. **Ejecución en segundo plano de programa**

Perl Concyt.pl &	& indica segundo plano

Fuente: elaboración propia.

De esta forma, la aplicación corre en él un modo de no desplegado a la consola y no es dependiente de la sesión de usuario de shell.

Tabla XVII. **Verificación de proceso del programa**

UID PID PPID C STIME TTY TIME CMD	root 31370 1 0 00:40 ? 00:00:02 perl Concyt1.pl

Fuente: elaboración propia.

Ya ejecutándose la aplicación, en el mismo directorio donde reside, se crean dos archivos:

- Mensajes.log : archivo de registro de mensajes que guarda todo mensaje exitoso o fallido (ver la tabla XVIII), con este archivo se puede identificar la fecha y hora de reinicio de la aplicación, que palabra no se encontró, el numero de celular originarte y si existió algún error en el envío de la respuesta, contiene la siguiente información:

    - Día, mes, hora y año de recepción de mensaje.
    - Número Origen MO en formato internacional 502xxxxxxx.
    - Número Destino MT.
    - Identificación del mensaje, que puede contener un número hexadecimal de identificación único del mensaje o el error a nivel de de protocolo SMPP.
    - Palabra o término de búsqueda.
    - Resultado de la búsqueda, este resultado puede tener dos alternativas que son: OK que es un resultado exitoso y NOK que es un resultado no exitoso.

Tabla XVIII. **Muestra de archivo de registro**

Wed Nov 17 13:03:49 2010:	MO: 50253600004	MT: 258	Msg_id: 00e0bc8c	Busqueda: Roca	resultado: OK
Wed Nov 17 15:04:20 2010:	MO: 50257746597	MT: 258	Msg_id: 20e6648a	Busqueda: Aaaa	resultado: NOK

Fuente: elaboración propia.

- Eventos.log: archivo que contiene los eventos en ejecución del programa, (ver la tabla XXIX), usualmente éste contiene la requisiciones y respuestas de la primitiva enquiry link del protocolo SMPP en la fecha y hora de la respuesta. Con este archivo se puede identificar que la sesión esta activa y respondiendo a la comunicación Cliente-servidor.

Tabla XXIX. **Muestra de archivo de eventos**

Thu Jul 29 18:57:22 2010: Enquiry_link_resp 3
Thu Jul 29 18:57:52 2010: Enquiry_link_resp 5
Thu Jul 29 18:58:22 2010: Enquiry_link_resp 7
Thu Jul 29 18:59:04 2010: Enquiry_link_resp 10

Fuente: elaboración propia.

La aplicación genera, cuando está en modo ejecución, un archivo adicional de tipo temporal con el nombre del PID (identificación del proceso mismo) este archivo es utilizado para un reinicio en caso de una excepción en el programa que cause su interrupción, este archivo con formato 12088.pid se declara en un proceso tipo demonio en la utilería de unix cronjob que revisa

cada media hora si existe un archivo de proceso, en caso exista se mantendrá corriendo hasta que no encuentre el mismo en cuyo caso reinicia la aplicación asegurando la continuidad de la misma.

CONCLUSIONES

1. Los mensajes cortos a través de las redes celulares en Guatemala tienen una penetración cerca de 75 por ciento, lo que hace importante el desarrollo de aplicaciones educativas que utilicen este tipo de servicio tecnológico y que posibiliten el fácil acceso y uso a la mayor parte de la población.

2. La interacción de empresas de telecomunicaciones con entidades que apoyen ya sea la educación o la tecnología como es el caso de El Consejo Nacional de Ciencia y Tecnología (CONCYT), se hace cada vez más importante en un mundo donde la brecha de países en desarrollo y las potencias mundiales pueden acortarse más rápidamente haciendo uso de herramientas tecnológicas con infraestructura móvil para potenciar el conocimiento y el desarrollo.

3. La juventud en Guatemala, es cada día más hábil en el uso de tecnología y aplicaciones, lo que hace este ambiente un terreno fértil para incentivar a los jóvenes no solo a utilizar aplicaciones educativas, sino alentar a corto o mediano plazo que ellos mismos desarrollen aplicaciones y herramientas útiles e interesantes para toda la sociedad guatemalteca.

4. La Universidad de San Carlos de Guatemala y por ende la Facultad de Ingeniería, como la institución por excelencia donde se divulga la educación, es un ente potenciador para la industria y la sociedad de nuevas posibilidades de hacer un país cada día más cercano a la tecnología y sus egresados más enfocados al compromiso de contribuir en este rol de trasmisión de conocimientos y trabajo en conjunto.

5. El desarrollo de una aplicación en la que se integra conocimiento técnico, económico, empresarial e institucional en el ámbito del Ejercicio Profesional Supervisado (EPS), hace que el desafío haya sido y sea interesante y productivo de realizar dando como resultado este diccionario de la lengua española consultado a través de mensajes cortos en la red de telefonía celular.

RECOMENDACIONES

1. Desarrollar en el futuro un programa permanente de cooperación: Universidad de San Carlos de Guatemala y CONCYT, que establezca posibles proyectos de aplicación de Ejercicio Profesional Supervisado (EPS) esto sería una relación de ganar entre entidades y futuros egresados de ingeniería como de otras áreas del conocimiento.

2. La aplicación del diccionario podría ser empleada para traducciones en el futuro, utilizado en el módulo ya existente el protocolo DICT definido actualmente como un estándar en línea y que tiene traducciones español a inglés y del mismo inglés al rededor de 30 idiomas distintos.

3. El diccionario y contenido puede ser adecuado y poblado en el futuro con terminología de tecnología o contenido social guatemalteco, indistintamente, ya que bastaría crear un archivo adicional con el nuevo término o contenido.

4. Incluir en el futuro, revisiones periódicas lingüísticas y semánticas del contenido actualmente incorporado al diccionario, que fortalezcan aún más el detalle de las palabras y definiciones sobre las cuales el usuario haga una búsqueda.

5. Con la experiencia y resultados de esta interacción CONCYT – TIGO en el ámbito de mensajes cortos, pueden en el futuro ser integrados con facilidad a otras compañías de telefonía celular, cuando éstas estén dispuestas a abrir sus puertas y montar aplicaciones educativas, ya que la mecánica y protocolos usados son estándares en la industria.

6. CONCYT podría proporcionar contenido para toda Centroamérica, utilizando la estructura cliente-servidor y el protocolo SMPP, compartiendo así esta ventaja con países hermanos.

BIBLIOGRAFÍA

1. 3GPP. *The 3rd Generation Partnership Project* (3GPP) [en linea]. [ref. 03 de julio de 2008]. Disponible en Web: http://www.3gpp.com.

2. BAKER, Paul. ISMSC*. Manual de entrenamiento*. Primera parte. Estados Unidos: Comverse Training Services, 2002. 100 p.

3. BERTONI, Henry L. *Radio propagation for modern wireless systems*. Estados Unidos de América: Prentice Hall, 2000. 276 p. ISBN-10: 0130263737.

4. CARDAMA, Aznar, et. al. *Antenas.* 2a ed. México, D.F: Alfaomega, 2002. 470 p. ISBN: 8483016257.

5. *Comverse* ISMSC *training manual*; *PN 10-133-001*. Estados Unidos: Comverse, 2001. 120 p.

6. Consejo Nacional de Ciencia y Tecnología. *Reglamento Orgánico Interno de la Secretaría Nacional de Ciencia y Tecnología. Guatemala:* CONCYT*; SENACYT,* 2006. 20 p.

7. DESAI, Vishvanath. *Guidelines for the Economic analysis of projects.* India: Economics and Development Resource Centre, 1997. 215 p.

8. Enciclopedia Wikipedía. *Sistema Global para las Comunicaciones* [en linea]. [ref. 15 de enero de 2009]. Disponible en Web: http://www.wikipedia.com.

9. Equipo de Arquitectura de Internet. RFC 793/1700/2018/2501 [en linea]. [ref. 12 de agosto de 2008]. Disponible en Web: http://www.rfc-es.org.

10. European Telecommunications Standardization Institute. *Digital cellular telecommunications system (Phase 2+). Alphabets and language-specific information*. Norma GSM 03.38 version 7.2.0. 1998.

11. European Telecommunications Standardization Institute. *Digital cellular telecommunications system (Phase 2+).* ETSI TS 100 900. Versión 7.2. Valbonne – France: ETSI, 1998. 230 p.

12. HAYT, William H.; BUCK, John A. *Teoría electromagnética*. 7a ed. México D.F : McGraw-Hill, 1991. 582 p. ISBN: 9701056205.

13. JUNQUERA, Rafael A. *Servicios de Valor Agregado en las Redes Móviles de Latinoamérica*. Tele-Semana y Signals Consulting, Mexico: SCT, 2005. 57 p.

14. KELLOMAKI, Sampo. *Modulo Net::*SMPP. [en linea]. [ref. 2 de agosto de 2008]. Disponible en Web: http://search.cpan.org/~sampo/Net-SMPP-1.03/SMPP.pm.

15. KORHONEN, Juha. *Introduction to 3G mobile communications*. 2a ed. Estados Unidos: Artech House, 2003. 544 p. ISBN: 1580535070.

16. Logica. *Mobile Networks Limited. SMPP Protocol Specification v3.4 Issue 1.0 [en linea]. [ref. 01 de diciembre de 2008]. Disponible en Web: http://www.openSMPP.logica.com.*

17. REY VEIGA, Eugenio. *Telecomunicaciones móviles.* 2a ed. España: Marcombo, 1998. 261 p. ISBN: 8426711499.

18. Simplewire. *Short message Peer to Peer Error Code*.[en linea]. [ref. 3 de agosto de 2008]. Disponible en Web: http://www.simplewire.com.

19. SMPP FORUM. *SMPP 3.4*. [en linea]. [ref. 02 de agosto 2008].Disponible en Web: http://www.smsforum.net/.

20. SPURGEON, Charles. *Redes Lan del tipo Ethernet. Ethernet the definitive guide*. Estados Unidos: O'Reilly Media, 2000. ISBN-10: 1565926609.

21. STREMLER, Ferrel G. *Introduction to Communication System*. 3a ed. Estados Unidos: Addison Wesley, 1990. 757 p. ISBN: 0201184982.

22. TOMASI, Wayne. *Sistemas de comunicaciones electrónicas*. 4a ed. Mexico: Prentice Hall, 2003. 935 p. ISBN: 9702603161.