El sistema GSM

Introducción

Los sistemas de comunicación basados en tecnologías celulares son, a día de hoy, uno de los sectores que mayor demanda y crecimiento ha experimentado. Actualmente, existen más de 45 millones de usuarios en todo el mundo, y se calcula que para el año 2005 dicha cifra ascienda a 100 millones. Incluso, en algunos países, el número de teléfonos móviles ha superado al de teléfonos fijos en el año 2000, cosa que favorecerá el establecimiento de dichos sistemas como método universal de comunicación.

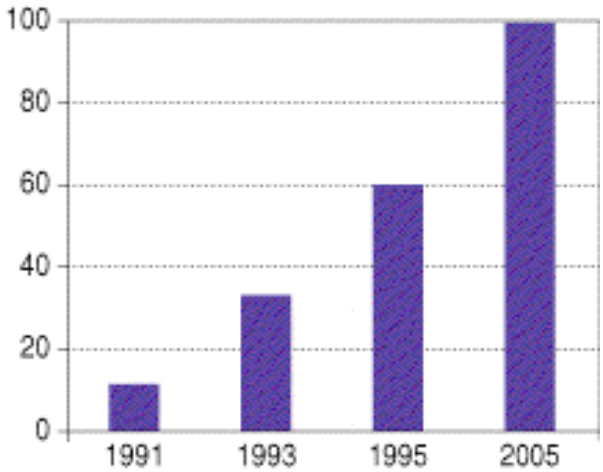

Figura 1: Usuarios de telefonía móvil (millones)

La base de los sistemas celulares radio, la reutilización de frecuencias por zonas geográficas, fue formulada en los Estados Unidos por los laboratorios Bell hacia el año 1970, pero sin embargo, fueron los países nórdicos quienes introdujeron el primer sistema celular comercial, con la puesta en marcha del sistema NMT (Nordic Mobile Telephone), en el año 1981.

En Estados Unidos, los sistemas celulares aparecieron como tales con el desarrollo del sistema AMPS (Advanced Mobile Telephone System), en 1983. El sistema AMPS fue adoptado en Asia, Latino América y Australia, creándose así un potente mercado dentro del mundo de las telecomunicaciones.

También cabe destacar el desarrollo del sistema TACS (Total Access Communications System) en Gran Bretaña, que empezó a ser operativo a partir de 1985 y que fue creado como una evolución del sistema AMPS.

Por otra parte, hasta el año 1980, los sistemas celulares se basaron mayormente en tecnologías analógicas, no obstante, las dificultades de éstas para incrementar la capacidad de los sistemas de forma eficiente y económica, provocó la progresiva evolución hacia tecnologías digitales, que introdujeron numerosas ventajas y facilidades, tanto a nivel de capacidad como de señalización, transmisión o robustez de los sistemas frente a interferencias.

Dentro de este nuevo marco es donde aparece el sistema celular digital GSM (Global System for Mobile Communication), que será el centro de estudio en este Proyecto Fin de Carrera.

A continuación se detallan los principales sitemas celulares analógicos y digitales, que han aparecido:

Tabla 1: Sistemas celulares analógicos

C-450	Instalado en Sur Africa en 1980. Actualmente se conoce como Motorphone y es utilizado por Vodacom.
NMT-450	Nordic Mobile Telephones-450. Desarrollado especialmente por Ericsson y Nokia para dar un servicio robusto que no se viera afectado por la accidentada orografía de los países nórdicos. Opera en la banda de los 450MHz. (año 1981)
AMPS	Advanced Mobile Phone System. Desarrollado por los laboratorios Bell en 1970 y comercializado por primera vez en Estados Unidos en el año 1983. Opera en la banda de 800MHz.
C-NEZT	Tecnología celular utilizada en Alemania. Opera en la banda de los 450MHz.
N-AMPS	Narrowband Advanced Mobile Phone System. Desarrollado por Motorola como una tecnología intermedia entre la analógica y la digital. Tiene una capacidad tres veces mayor que el sistema AMPS y opera igualmente en la banda de 800MHz.
NMT-900	Nordic Mobile Telephones-900. Opera en la banda de los 900 Mhz, y es una evolución del sistema NMT-450 que proporciona mayor capacidad. (año 1986)
NTT	Nippon Telegraph and Telephone. El antiguo estándar analágico japonés.
HICAP	Versión de mayor capacidad del sistema NTT.
TACS	Total Access Communications System. Desarrollado por Motorola a partir del sistema AMPS. Se usó por primera vez en Gran Bretaña en 1985, aunque también se usa en Japón, donde se conoce como JTAC. Opera en la banda de los 900MHz.
ETACS	Versión mejorada del sistema TACS.

Tabla 2: Sistemas celulares digitales

D-AMPS	Versión digital del sistema AMPS. Opera en la banda de los 800MHz.
GSM	Global System for Mobile Communications. Primer estándar digital europeo, desarrollado para establecer una compatibilidad celular en Europa. Opera en la banda de los 900MHz. (año 1991)
DCS-1800	Digital Cordless Standard. Versión de GSM operando en la banda de 1800MHz. Incompatible con GSM-900. (año 1994)
PCS-1900	Personal Communications Service. Versión americana de GSM, incompatible con el sistema GSM europeo. Opera en la banda de 1.900MHz.
PHS	Personal Handy System. Sistema japonés que ofrece una elevada velocidad de datos y una alta calidad de voz.

Introducción a GSM

A lo largo de la evolución de las comunicaciones celulares fueron apareciendo diversos sistemas, pero al principio cada país desarrolló su propia tecnología, lo que provocó la aparición de incompatibilidades, que limitaron el uso de los equipos y redujeron el mercado a zonas concretas.

Para resolver estos problemas, la CEPT (Conference of European Post and Telecommunications) formó, en 1982, la organización GSM (Group Special Mobile, que más tarde pasaría a conocerse como Global System for Mobile communications), cuyo objetivo sería desarrollar un sistema celular estandarizado dentro de Europa. Dicho sistema debería cumplir los siguientes requisitos:

- Eficiencia espectral.
- Roaming internacional.
- Costes económicos de los móviles y las estaciones base.
- Calidad de voz.
- Compatibilidad con otros servicios como los ISDN. (Integrated Services Digital Network)
- Capacidad de soportar nuevos servicios.

En 1989, la responsabilidad de las especificaciones GSM pasaron de la CEPT a la ETSI (European Telecommunications Standards Institute). El objetivo de las especificaciones GSM siguió centrándose en describir la funcionalidad y los interfaces de cada componente, proporcionando así una guía para el diseño global del sistema. Estas especificaciones, una vez estandarizadas, asegurarían la interconexión entre los diferentes elementos de la red. En 1990, fue publicada la fase I de las especificaciones, pero el uso comercial no empezó hasta mediados del año 1992.

Especificaciones GSM

El sistema GSM fue diseñado, como se ha comentado anteriormente, para ser una plataforma independiente. Las especificaciones GSM no especifican requerimientos de tipo hardware, sino que describen las funcionalidades de las que debe disponer la red. Esto permite a los proveedores diseñar distintos productos que proporcionen las funcionalidades requeridas, y a la vez hace posible que los operadores puedan elegir entre diversos equipos.

Las especificaciones GSM consisten en doce series, que fueron redactadas por diferentes grupos de trabajo (GSM, ETSI). Actualmente, es la ETSI quien coordina a los distintos grupos que trabajan en las futuras especificaciones.

Tabla 3: Series GSM

Serie	Contenido
01	Especificaciones generales.
02	Características del servicio.
03	Características de la red.
04	Protocolo e interfaz entre el terminal móvil y la estación base.
05	Capa física del canal radio.
06	Codificación de la información.
07	Especificaciones del terminal móvil.
08	Interfaz entre la estación base y el terminal móvil.
09	Modo de funcionamiento de la red.
10	Modo de funcionamiento del servicio.
11	Aprobación de las especificaciones.
12	Operación y mantenimiento.

El lanzamiento del sistema GSM fue realizado en distintas fases, dado que las especificaciones no fueron finalizadas en el tiempo establecido. Cada fase fue introduciendo mejoras y nuevos servicios basándose en la anterior.

Fase 1

La fase 1 contiene los servicios básicos del sistema GSM:

- Telefonía.
- Roaming internacional.
- Servicios de datos (9.6 kbits/s).
- Servicio de mesajes cortos (SMS).
- Desvío de llamada.

Fase 2

Las características adicionales que fueron introducidas fueron:

- Cobro revertido.
- Identificación del abonado.
- Llamada en espera.
- Grupo cerrado de usuarios.
- Capacidades adicionales para las comunicaciones de datos.

Fase 2+

Dicha fase añade nuevos servicios de valor añadido para los usuarios:

- Planes de numeración privados.
- Interconexión con los sistemas DCS-1800 y DECT, entre otros.
- Servicios de datos suplementarios.

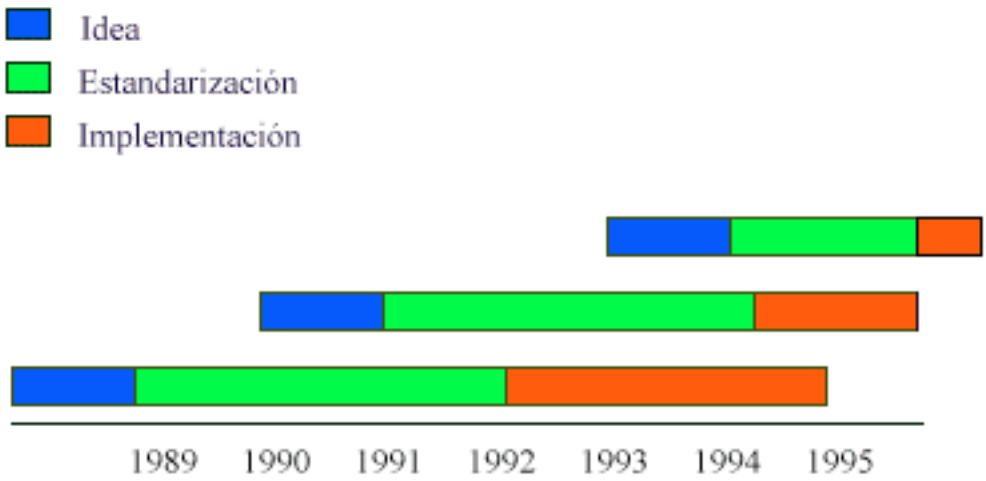

Figura 2: Fases del sistema GSM

Por último, se destacan los hitos más importantes en la historia del sistema GSM:

Tabla 4: Hitos en la historia de GSM

1982	La CEPT establece el grupo GSM para desarrollar un estándar Europeo de sistema celular en la banda de los 900 MHz.
1985	Elección de las recomendaciones a ser desarrolladas.
1986	Realización de distintas pruebas para la elección de la tecnología a usar en el interfaz radio.
1987	Se escoge como técnica de acceso al medio, TDMA, aunque en realidad se usará combinada con FDMA. Doce operadores de telecomunicaciones, representando a 12 países, firman el MoU (Initial Memorandum of Understanding), comprometiéndose a utilizar el nuevo estándar.
1988	El grupo GSM empieza a desarrollar las especificaciones. Otros cinco países se unen al MoU.
1989	La responsabilidad de las especificaciones GSM pasa a la ETSI.
1990	Se publica la fase I de las especificaciones y se empiezan a producir equipos.
1991	Crece el MoU.
1992	Comercialización del sistema GSM. Se dota de servicio a las principales ciudades y aeropuertos.
1993	Aumentan las zonas con cobertura y el servicio se extiende fuera de Europa.
1994	Aparece la fase 2 de las especificaciones. Se dota de cobertura a las zonas rurales.
1995-1997	Aumenta el número de usuarios y de redes GSM. Se empieza a trabajar en la Fase 2+.
1998	A principios de 1998 el MoU lo componen un total de 253 miembros y el mercado GSM abarca el 31% de la telefonía celular.

La red GSM

La red GSM se suele dividir, generalmente, en tres sistemas principales. A su vez, cada uno de ellos, está compuesto por distintas unidades funcionales que actúan como componentes individuales dentro de la red. Los tres sistemas: Sistema de Conmutación (SS, Switching System), Sistema de Estación Base (BSS, Base Station System) y Sistema de Operación y Soporte (OSS, Operation and Support System), quedan reflejados en la siguiente figura.

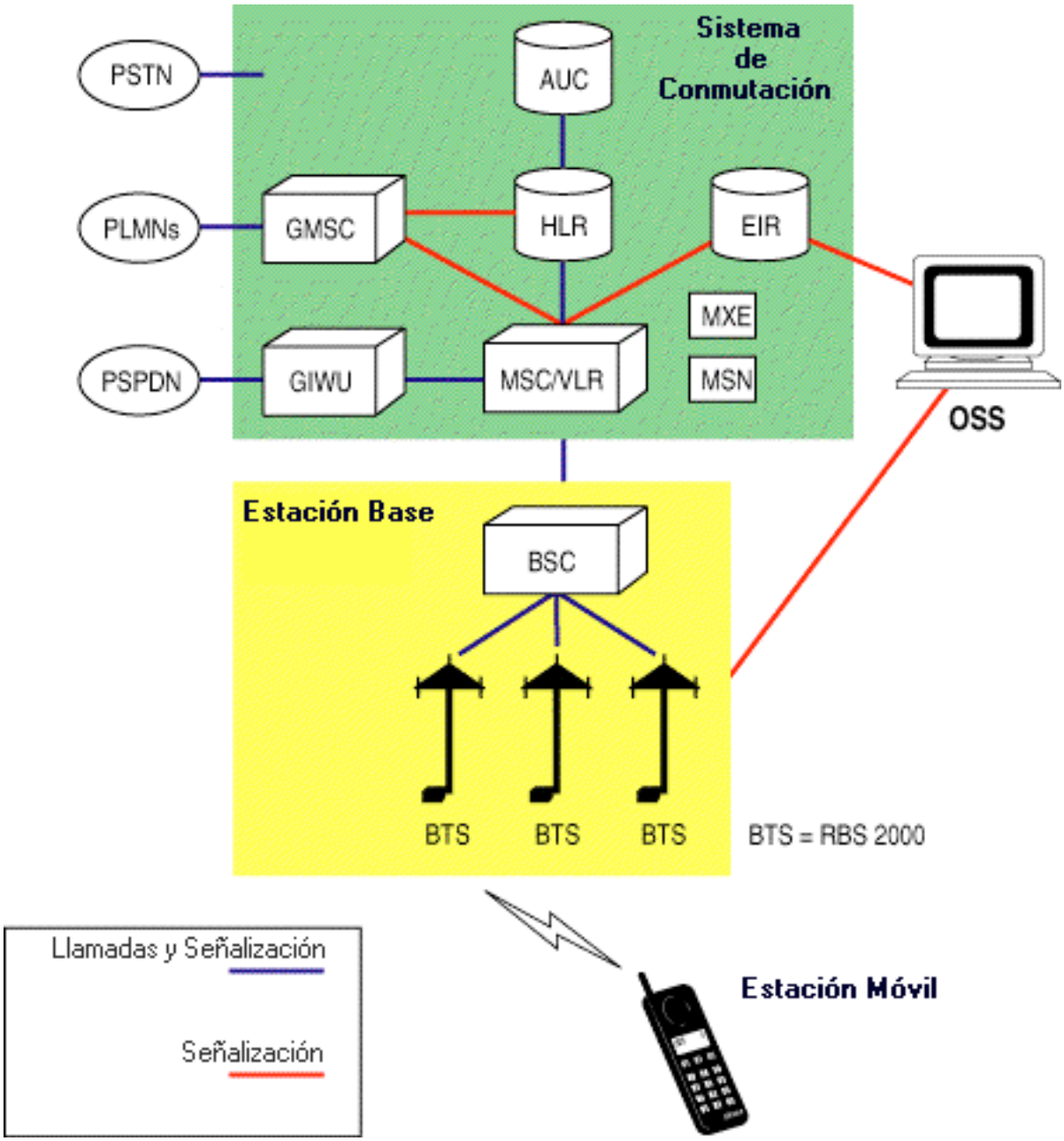

Figura 3: Estructura de la red GSM

La red GSM de un operador, por razones de capacidad y cobertura, estará formada por distintas replicas de los tres sistemas anteriores (nodos), que se comunicarán a través del Centro de Conmutación de Servicios Móviles. (MSC, Mobile services Switching Center). Comúnmente, al nodo se le denomina simplemente MSC, por ser este su componente más importante.

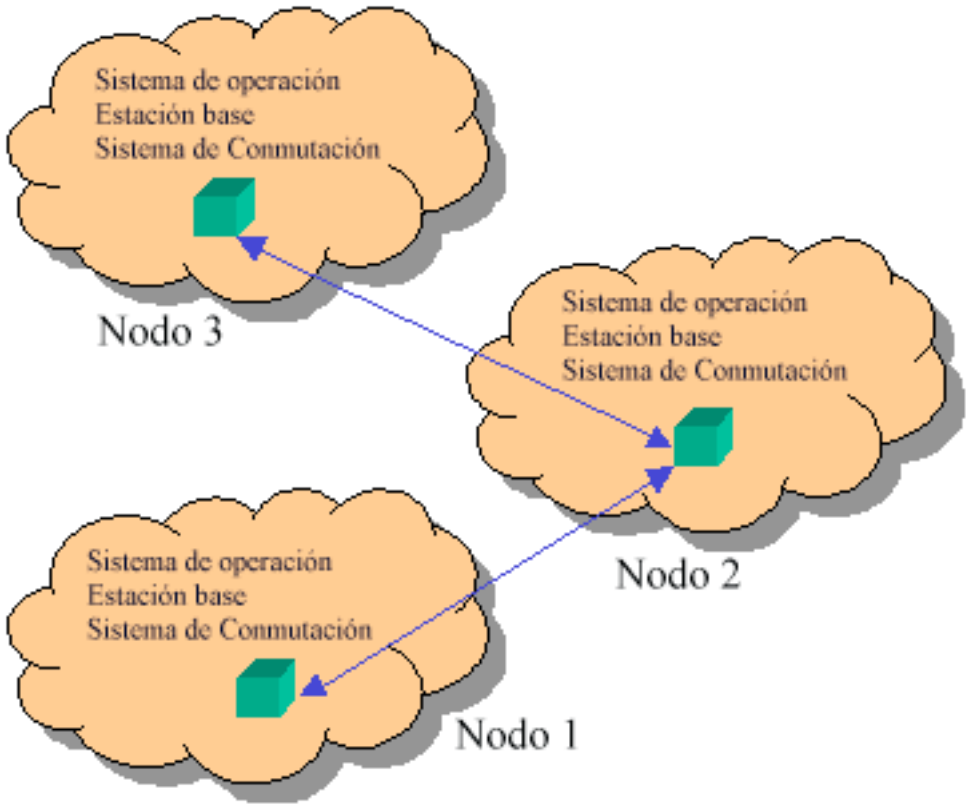

Figura 4: Nodos de la red GSM

Tabla 5: Abreviaturas

AUC	Centro de autentificación	AUthentification Center
BSC	Controlador de estación base	Base Station Controller
BTS	Estación base	Base Transceiver Station
EIR	Registro de identificación del equipo	Equipment Identity Register
HLR	Registro de localización local	Home Location Register
MSC	Centro de conmutación de servicios móviles	Mobile service Switching Center
NMC	Centro de administración de red	Network Management Center
OMC	Centro de operación y mantenimiento	Operation and Maintenance Center
VLR	Registro de localización de visitantes	Visitor Location Register

SS - Sistema de Conmutación

El Sistema de Conmutación es el responsable del procesado de las llamadas y de las funcionalidades relacionadas con el usuario. Incluye los siguientes componentes:

MSC - Centro de conmutación de servicios móviles

El MSC implementa las funciones de conmutación dentro de la red móvil, ya que controla las llamadas provenientes o dirigidas a otros sistemas de telefonía o datos, como la red telefónica pública (PSTN), la red de servicios integrados (RDSI), las redes de datos públicas y privadas o las redes móviles no propias del operador.

Obviamente, el MSC también controla las llamadas que se producen dentro de la red del operador, para ello precisa comunicarse con los MSC's del resto de nodos y con el HLR perteneciente a su nodo. En todas las acciones que realiza el MSC para encaminar los distintos tipos de llamadas, éste se comporta como una especie de pasarela dentro de la red, por ello se dice que dicho componente incorpora la funcionalidad de Gateway, y comúnmente se le suele denominar GSMC. (Gateway MSC).

HLR - Registro de localización local

El HLR es una base de datos que almacena y administra toda la información perteneciente a los usuarios de la red. Generalmente, dicho componente, contiene la información de los usuarios que se han dado de alta dentro de la zona geográfica que abarca el nodo en el que se encuentra ubicado.

Los datos almacenados se pueden agrupar en las siguientes categorías:

- Identificación del abonado.
- Servicios adicionales contratados por el abonado.
- Información para su localización.
- Información para la autentificación del abonado.

VLR - Registro de localización de visitantes

El VLR es una base de datos que contiene información sobre los abonados que, en un momento determinado, se encuentran localizados en el área de acción de un nodo que no se corresponde con el nodo donde fueron dados de alta. El MSC correspondiente es el que se percata de tal situación e incluye al abonado en el VLR. Además, contacta con el MSC propia del usuario para que éste actualice la información correspondiente en su HLR. Así, las llamadas dirigidas a dicho usuario podrán ser redirigidas adecuadamente.

AUC - Centro de autentificación

Su principal función es autentificar a los usuarios que intentar usar la red, para evitar posibles fraudes. Consiste en una base de datos, conectada con el HLR, que permite decodificar y comparar la información cifrada de autentificación que es enviada por el móvil cada vez que se intenta acceder a la red a través de él.

EIR - Registro de identificación del equipo

El EIR es una base de datos que permite comprobar el número de identificación de cada equipo móvil. Mediante dicha comprobación, el operador puede saber a que fabricante pertenece el equipo o si este ha sido robado o es defectuoso, por ejemplo. En función de dicha información la llamada será cursada o no. No hay que confundir el número de identificación del equipo con la información de autentificación del usuario, que es la que comprueba en el AUC. Por otra parte, destacar que el EIR es un componente opcional dentro de la red GSM.

BSS - Sistema de Estación Base

Los componentes que incluye dicho sistema son:

BSC - Controlador de estación base

La BSC es un centro de conmutación de canales de alta capacidad que controla todos los aspectos radio relacionados con la red GSM. La BSC es la que se encarga de la asignación de frecuencias y de la realización de los handover s. Cada BSC controla a varias estaciones base y a su vez una MSC controla a varias BSC.

BTS - Estación base

La estación base es el componente que proporciona el interfaz radio a los equipos móviles a través de distintos transceptores y antenas. La BTS recoge en primera instancia la información de dichos equipos y la transfiere a la BSC, que es quien actuará en función de ella.

OSS - Sistema de Operación y Soporte

Los componentes que incluye dicho sistema son:

OMC - Centro de operación y mantenimiento

El OMC es un centro computerizado de monitorización que está conectado a distintos componentes de la red, como el MSC o la BSC, a través de conexiones X.25 generalmente. De estos componentes el OMC recibe distinta información que le permite conocer el estado de la red (trafico, caída de enlaces) y actuar en función de ella modificando distintos parámetros. Generalmente, suele existir un OMC por cada nodo, que se encarga del control de la red que abarca éste.

NMC - Centro de administración de red

El NMC es el encargado del control total de la red, suele existir uno por red que se conecta a los distintos OMC.

Terminal móvil (MS)

El último componente de la jerarquía de la red GSM, y tal vez el más importante, sea el terminal móvil. Básicamente el terminal consta de dos elementos básicos:

- Tarjeta de Identidad de Usuario (SIM, Suscriber Idenntity Module) Dicha modulo esta implementado en una pequeña tarjeta que se suele insertar en la parte trasera del móvil. Cada vez que se realiza una llamada la información del usuario contenida en la SIM es transferida a la red. Esta información identifica totalmente al abonado, de tal forma que si un usuario inserta su SIM en el terminal móvil de otra persona y realiza una llamada, el coste de ésta le será cargado a el mismo. A través de este sistema de identificación también se puede bloquear el uso de un terminal robado.

- El terminal en si.

Estructura geográfica de la red GSM

Toda red telefónica necesita una estructura específica para enrutar correctamente las llamadas hacia los usuarios. En una red móvil, esto es todavía más importante, ya que los abonados no tienen una localización fija. A continuación se describe la estructura geográfica que usa GSM para mantener localizados a sus usuarios, la disposición celular.

Célula

Una célula es la unidad básica de un sistema celular, y se define como el área de cobertura dada por una estación base (BTS). Cada célula tiene asignado un identificador único denominado CGI, Cell Global System.

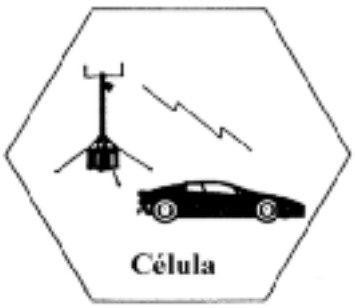

Figura 5: Célula

Area de Localización

El área de localización (LA) se define como un conjunto de células. Dentro de la red, la localización de un usuario se conoce por el LA (Location Area) donde se encuentra. Este identificador de LA es el que se almacena en el VLR y en el HLR. Cuando un usuario pasa de un LA a otro LA, su localización deberá ser actualizada (esto no ocurre si pasamos de célula a célula dentro de un mismo LA, o si se cambia de LA mientras se cursa una llamada). Cuando exista una llamada dirigida al usuario, se propagara un mensaje de localización a través de todas las células pertenecientes al LA actual para localizarlo de forma concreta.

Area de MSC

El área de MSC está formada por varias LA y representa la zona geográfica controlada por un MSC (nodo). En su VLR se almacena el LA de los abonados que se encuentran en su campo de acción, pero que no fueron dados de alta en dicho nodo, y en el HLR se almacena el LA actual de los abonados dados de alta ese nodo, sea cual sea su posición.

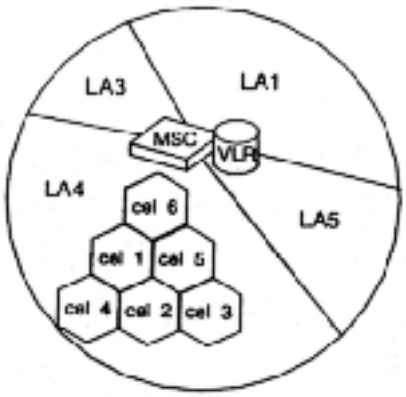

Figura 6: LA - Area de MSC

Area PLMN

Se entiende por área PLMN (Public Land Mobile Network) al conjunto de células totales controladas por un operador o al área donde el operador ofrece cobertura y acceso a su propia red. En un país existen varias PLMN, una por cada operador de telefonía móvil.

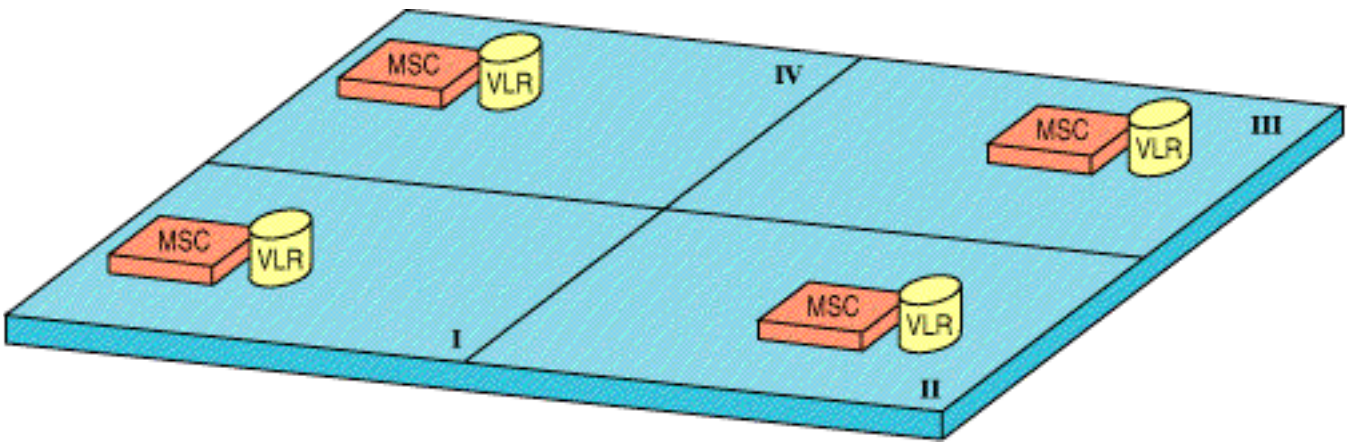

Figura 7: Area del operador - PLMN

Area GSM

Dicho termino se refiere al área geográfica total desde donde se puede tener acceso a la red GSM. Esta zona está creciendo gracias a los acuerdos entre los distintos operadores. El termino roaming international se refiere al hecho de cambiar de PLMN, es decir un usuario está en roaming cuando la red GSM en la que se encuentra no pertenece al operador con el que se dio de alta.

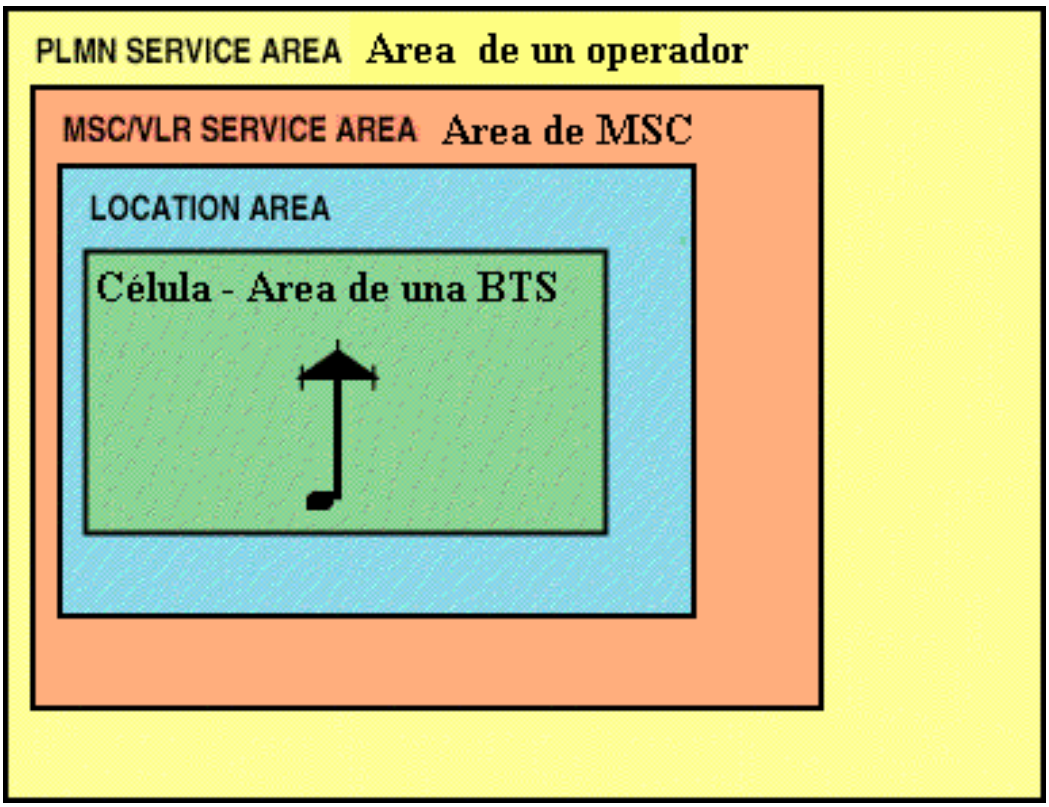

Figura 8: Estructura geográfica de una red GSM

Bandas de frecuencia en GSM

A lo largo de su evolución el sistema GSM se ha extendido y desarrollado en tres bandas de frecuencia distintas.

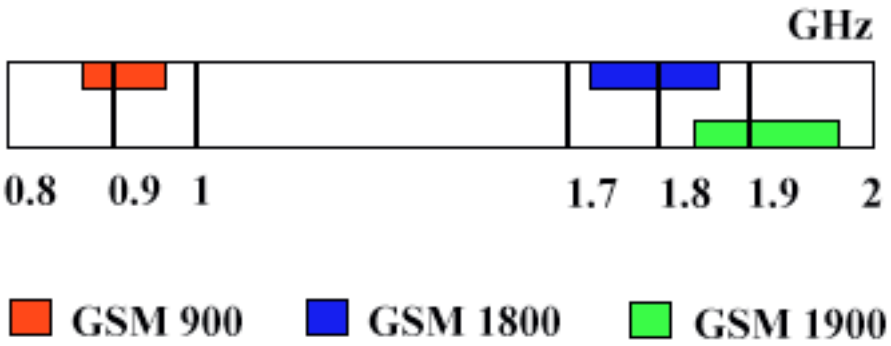

Figura 9: Bandas de frecuencia

GSM 900

La banda de frecuencias original que se especificó para el sistema GSM fue la de los 900MHz, y es la que utilizan la mayoría de las redes GSM actuales. En algunos países se ha desarrollado una versión de GSM 900 de mayor capacidad que recibe el nombre de E-GSM, mientras que la primera versión se denomina P-GSM.

GSM 1800

En 1990, para incrementar la competencia dentro del sector, el Reino Unido propuso el desarrollo de una nueva versión de GSM adaptada a la banda de los 1800MHz, lo que supuso la aparición de nuevos operadores. Este sistema recibió el nombre de DCS 1800 (Digital Celular System), aunque más tarde, en 1997, pasó a denominarse GSM 1800.

GSM 1900

Alrededor de 1995, fue especificado en Norte América el sistema PCS (Personal Communications Services). El sistema PCS, que potencia la idea de comunicación “persona a persona”, no precisa de una tecnología celular, pero se comprobó que a través de dicha tecnología se obtenían los mejores resultados. Las frecuencias disponibles estaban en la banda de 1900MHz, por lo que se decidió desarrollar el sistema PCS, que más tarde pasaría a llamarse GSM 1900, en dicha banda de frecuencias. En Norte América el sistema GSM 900 no podía ser usado porque su banda de frecuencias ya estaba ocupada.

Conceptos radio

Frecuencia

Un terminal móvil se comunica con una BTS mediante la transmisión y recepción de ondas de radio, que consisten en energía electromagnética. La frecuencia de una onda de radio se define como el número de veces que ésta oscila por segundo, y se mide en Herzios (Hz), donde un herzio indica una oscilación por segundo (Hz=1/s). Actualmente, multitud de aplicaciones usan las ondas de radio, a distintas frecuencias, para transportar información:

- Televisión: 300MHz
- FM Radio: 100MHz
- Redes móviles: 300-2000Mhz

Longitud de onda

Todo onda electromagnética puede ser descrita a través de una función sinusoidal que se caracteriza por una determinada longitud de onda. La longitud de onda es la longitud de una oscilación completa medida en metros (m). Para calcular dicho parámetro se puede usar la siguiente formula.

$$\lambda = (vp)/f$$

Donde:

- vp es la velocidad de propagación en el medio, en nuestro caso dicha velocidad coincide con la velocidad de propagación de la luz, $3x10^8$ m/s.
- f es la frecuencia de la onda.

Así, para el caso del sistema GSM 900, tenemos que:

$$\text{Longitud de onda} = \frac{3x10^8(m/s)}{900MHz} = 0,33m$$

De esta formula se puede deducir que a mayor frecuencia, menor longitud de onda y viceversa. Las frecuencias bajas (mayor longitud de onda) son más apropiadas para la transmisión a largas distancias, ya que son reflejadas por la superficie de la tierra y las capas de la atmósfera. Las televisión y la radio FM son ejemplos de aplicaciones que usan bajas frecuencias.

Las frecuencias altas (menor longitud de onda) son apropiadas para la tranmisión a distancias cortas, ya que son más sensibles a los obstáculos que existan entre el transmisor y el receptor. Generalmente se usan en aplicaciones donde el área de cobertura es relativamente pequeño.

Así, las frecuencias usadas por los sistemas móviles son un compromiso entre las ventajas que ofrecen las altas y las bajas frecuencias.

Ancho de banda

El ancho de bada es el rango de frecuencias totales usadas por una aplicación. Dicho parámetro es importante dentro de un sistema móvil, ya que determina la capacidad del mismo, influyendo en el número de llamadas que podrán ser cursadas.

Canales

Un canal es una frecuencia o un conjunto de frecuencias dentro del ancho de banda total, que se utiliza para la transmisión o recepción de información. Los canales de comunicación pueden ser de distintos tipos:

- Simplex: Se trata de un canal unidireccional. Lo usan aplicaciones como la televisión o la radio FM.
- Half duplex: Se trata de un canal bidireccional, pero sólo se transmite en un sentido simultáneamente, ya que se usa la misma frecuencia tanto para recibir como para transmitir. Lo suelen usar sistemas de radio privados como el de la policía.
- Duplex: Se trata de un canal bidirecional, donde se transmite simultáneamente en ambos sentidos, porque las frecuencias usadas para recibir y transmitir son distintas. Es el empleado en telefonía móvil.

El sentido terminal móvil-red se denomina Uplink, mientras que el opuesto recibe el nombre de Downlink. Las frecuencias que se usan en el Uplink siempre son menores, ya que se requiere menor potencia para transmitir a tales frecuencias. De esta forma se aprovecha mejor la autonomía del terminal móvil.

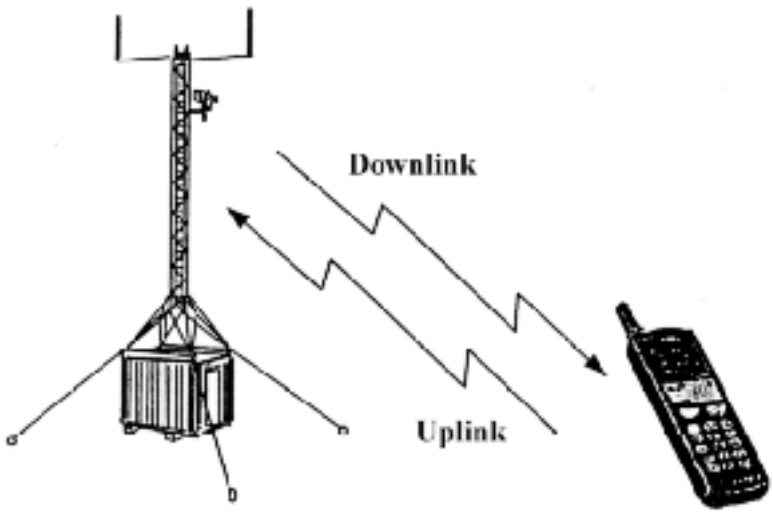

Figura 9: Enlaces Uplink y Downlink

En el sistema GSM 900 los sentidos uplink y downlink abarcan las siguientes frecuencias:

- Sentido Uplink (Móvil-Estación Base): 890 - 915MHz
- Sentido Downnlink (Estación Base - Móvil): 935 - 960MHz

Distancia duplex

EL uso de un canal full duplex requiere que los sentidos uplink y downlink estén separados en frecuencia por una distancia mínima. Esta es la distancia duplex, y sin ella los dos sentidos podrían interferirse. Para el caso de GSM 900 tenemos:

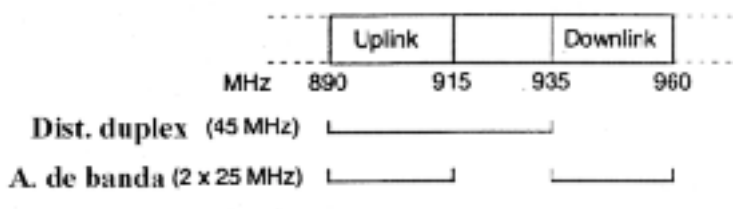

Figura 10: Distancia duplex

Separación entre canales

Además de la distancia duplex, todo sistema móvil incluye una separación entre canales. Dicha separación es la distancia en frecuencia que existe entre uplinks o downlinks consecutivos, y se utiliza para evitar el solape de la información entre sentidos idénticos de transmisión que se encuentran en canales distintos.

La separación entre canales depende de la cantidad de información que vaya a ser transmitida a través de ellos. A mayor cantidad de información, mayor separación será necesaria.

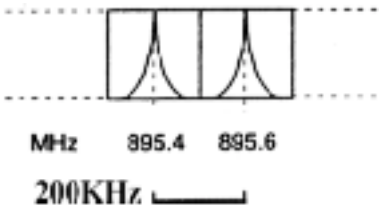

Figura 11: Separación entre canales

En la figura observamos dos canales adyacentes. En uno, la información se modula en la portadora de frecuencia 895.4 MHz, y en el otro en la portadora de frecuencia 895.6MHz. Como se puede observar, entre ambas portadoras existe una separación de 200KHz, necesaria para que no exista interferencia entre ambos canales.

Capacidad

La capacidad es el número de frecuencias del que se dispone dentro de una célula. Cada operador dispone de un número limitado de frecuencias, y debe distribuirlas adecuadamente por todas las células de su red en función del tráfico de cada zona.

No obstante, para proporcionar cobertura a un país entero es necesario reutilizar las frecuencias en diferentes zonas geográficas, consiguiendo así una red con suficiente capacidad para todos los abonados. Un aspecto importante a la hora de reutilizar dichas frecuencias es evitar las interferencias entre ellas, ya que a mayor interferencia menor calidad de la llamada, por lo que se debe evitar reutilizar las mismas frecuencias en células vecinas o próximas.

Así, se establecen patrones de reutilización de frecuencias, que se repiten a lo largo de toda la red del operador evitando las interferencias entre las mismas frecuencias. El termino distancia de reutlización se refiere a la distancia entre dos frecuencias idénticas dentro del patrón de reutilización.

Ratio de transmisión

La cantidad de información transmitida sobre el canal durante un período de tiempo se denomina ratio de transmisión. El ratio de transmisión se expresa en bit/s. En el sistema GSM tiene un valor de 270kbit/s.

Método de modulación

En GSM 900, la frecuencia que se usa para transmitir la información sobre el interfaz radio está alrededor de los 900 MHz, sin embargo, esta no es la frecuencia con la que se genera la información a transmitir. Las técnicas de modulación, en amplitud, frecuencia o fase, son usadas para trasladar dicha información a la banda de frecuencias que se usa en la transmisión, es decir, se fuerza a que la frecuencia portadora de la información sea 900MHz.

La técnica de modulación que se utilice está directamente relacionada con el ratio de transmisión del que se dispondrá. Usando una técnica de modulación simple podemos transmitir 1 bit/s, es decir 1 bit "ocuparía" 1Hz. Según esta técnica, en el sistema GSM, que dispone de un ancho de banda por canal de 200kHz, se podrían transmitir tan solo 200kbits/s. No obstante, existen técnicas de modulación avanzadas que permiten transmitir más de un bit en 1Hz. En GSM se utiliza la modulación GMSK (Gaussian Minimum Shift Keying), que permite la transmisión de 270kbits/s en 200kHz.

La capacidad de transmisión del sistema GSM es menor que la de otros sistemas de telefonía móvil, que son capaces de alcanzar ratios de transmisión mayores. No obstante, la ventaja de la modulación GMSK, se basa en su gran tolerancia a las interferencias, cosa que permite una mayor reutilización de las frecuencias, y por lo tanto un aumento en la capacidad para cursar tráfico.

Método de acceso al interfaz radio

La mayoría de sistemas celulares usan la técnica TDMA (Time Division Multiple Access) para transmitir y recibir señales de voz. Con esta técnica, cada canal es capaz de cursar varias llamadas, ya que cada llamada usará el canal en determinados periodos de tiempo, que se denominan time slots. A cada terminal móvil, en una llamada, se le asigna un time slot determinado, tanto en el enlace uplink como en el enlace downlink. En GSM, una trama TDMA consta de 8 time slots, es decir, cada canal será capaz de cursar 8 llamadas. La información que se transmite en un time slot se denomina burst.

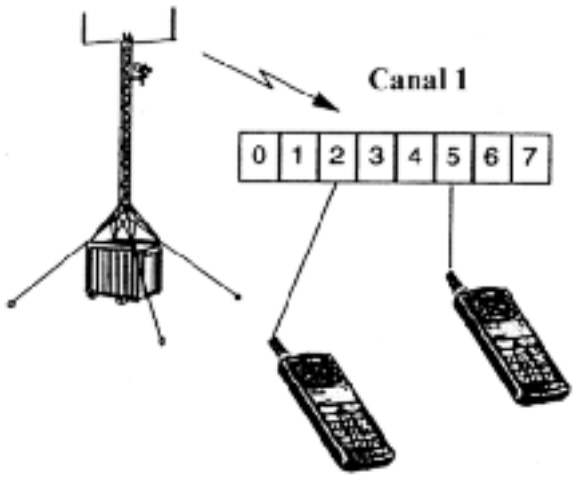

Figura 13: Time slots en un canal GSM

Canales lógicos y físicos

Cada time slot en una trama TDMA se denomina canal físico. Esto significa que hay 8 canales físicos por portadora en el sistema GSM. Los canales físicos pueden ser usados para transmitir voz, datos o información de señalización.

Es decir, un canal físico puede llevar diferentes mensajes dependiendo de las necesidades del momento. Así pues, puede decirse que la información a transmitir se divide en una serie de canales lógicos.

Por ejemplo, un canal físico puede ser usado para enviar trafico. Entonces dicho canal físico está siendo usado como canal lógico de tráfico (TCH-Traffic CHanel). Por otra parte, cuando se precisa transmitir la información necesaria para realizar un handover, el canal físico correspondiente sobre el que se transmite la instrucción está actuando como canal lógico de control (FACCH-Fast Associated Control Chanel).

Existen numerosos tipos de canales lógicos, cada uno designado para transmitir un mensaje diferente desde o hacia el terminal móvil.

Transmisión analógica y digital

Información analógica

La información analógica es continua y no toma valores discretos, es decir, una señal analógica es una forma de onda continua que varia de acuerdo con las propiedades de la información que transmite.

Figura 14: Señal analógica

Información digital

La información digital es un conjunto de valores discretos, es decir una señal digital es un conjunto de formas de onda discretas.

Figura 15: Señal digital

Ventajas de usar señales digitales

La voz humana es un tipo de información analógica, es una señal continua que cambia en amplitud y en frecuencia, por lo que en un principio, las señales analógicas parecían el mejor medio de transmitirla. Si se usaba una señal digital se tendrían que tomar valores discretos en el tiempo, cosa que implicaría una perdida de información.

No obstante, todas las señales, ya sean analógicas o digitales, sufren una distorsión a lo largo de la distancia que recorren. Para las señales analógicas la única solución era amplificar la señal, cosa que a la vez amplificaba la interferencia que se había sumado a ésta. Sin embargo, cuando se dispone de una señal digital, ésta puede ser recuperada totalmente sin ningún tipo de distorsión. Así pues, el sistema GSM escogió la tecnología digital frente a la analógica, ya que ésta presentaba una mayor robustez frente a las interferencias.

Además, si se toman las suficientes muestras, el efecto de la pérdida de cierta información es imperceptible, ya que se consigue una fiel representación de la señal analógica.

Problemas de la transmisión

Perdidas por distancia (Path Loss)

Hablamos de perdidas por distancia cuando la señal recibida se debilita a medida que aumenta la distancia entre el terminal móvil y la BTS, incluso sin existir obstáculos entre ellos. Cuando esto ocurre existe un riesgo muy alto de que la llamada se caiga, por lo que se debe establecer un camino alternativo para la llamada a través de otra BTS.

Efecto sombra (Shadowing)

Este efecto se produce cuando existen obstáculos físicos entre el terminal móvil y la BTS. Dichos obstáculos provocan una disminución en la potencia de la señal recibida. Es muy común que la potencia de la señal recibida desde el móvil fluctúe, dependiendo de los obstáculos que se puedan interferir en el camino hacia la BTS. Las caídas en potencia de la señal reciben el nombre de *fading dips*.

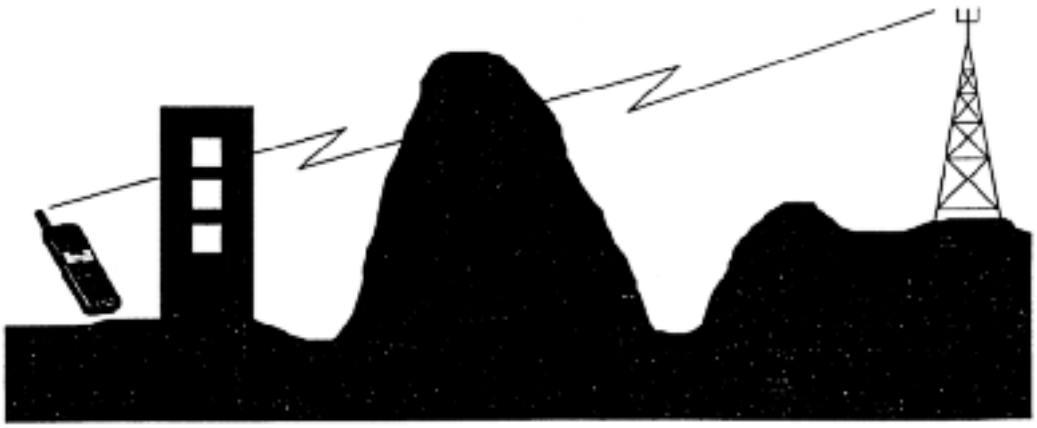

Figura 16: Efecto sombra (Shadowing)

Multipath fading

Este efecto ocurre cuando en la BTS se reciben varias señales provenientes del móvil, debido a las reflexiones que se producen en los diferentes obstáculos con los que se encuentra la señal. Los principales manifestaciones de este tipo de interferencia son el *Rayleigh fading* y la Dispersión en el tiempo (*Time Dispersion*).

Rayleigh fading

El Rayleigh fading tiene lugar cuando la señal llega al móvil a través de varios caminos, debido a las reflexiones en los distintos obstáculos. Así, la señal recibida es la suma de varias señales, que tan solo se diferencian en su fase. Obviamente, esto producirá caídas en la potencia (fading dips) de la señal total cuando las distintas contribuciones se sumen de forma regresiva. Estas caídas de potencia dependen de la velocidad del móvil y de la frecuencia de transmisión. Este fenómeno suele ocurrir cuando los obstáculos se encuentran próximos a la antena receptora.

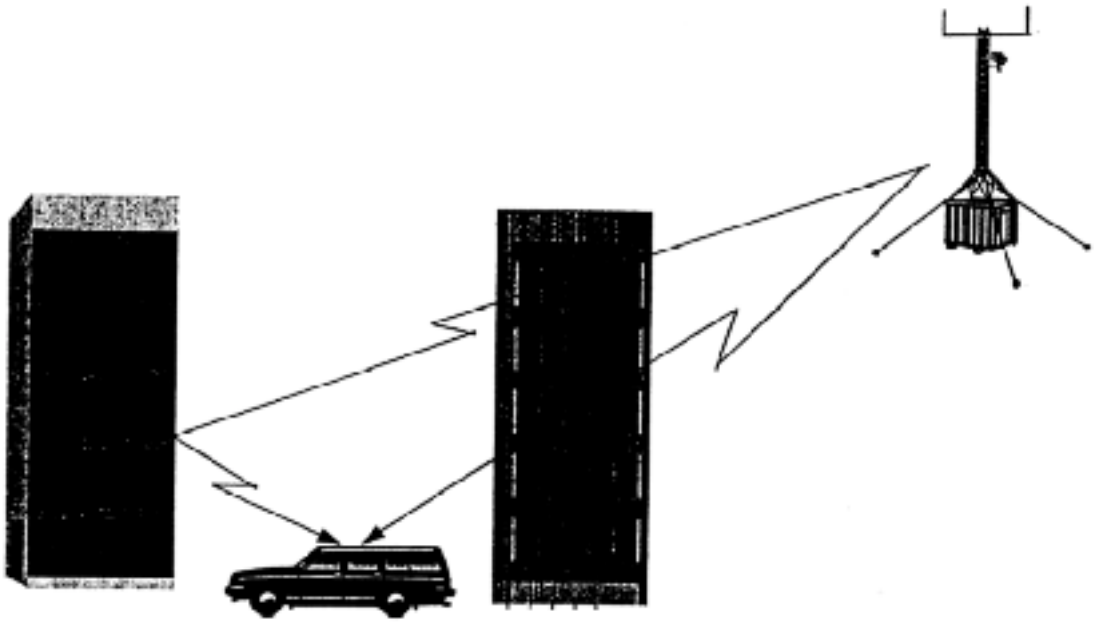

Figura 17: Rayleigh fading

Dispersión en el tiempo (Time dispersion)

La dispersión en el tiempo es otro problema relacionado con la reflexión de la señal en los obstáculos que encuentra en su camino, pero a diferencia del Raleigh fading, éste es provocado generalmente por los obstáculos que se encuentran alejados de la antena receptora.

La dispersión en el tiempo provoca lo que se denomina interferencia inter-simbolo, ya que provoca que símbolos consecutivos interfieran entre si, dificultando así la determinación de los símbolos de forma correcta.

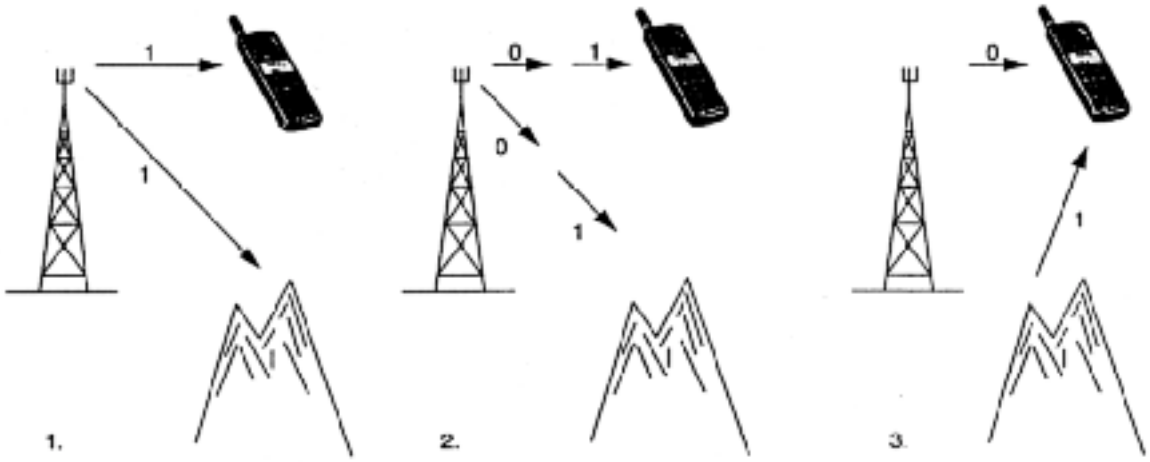

Figura 18: Dispersión en el tiempo (Time dispersion)

Si la señal reflejada llega un periodo de bit después que la señal directa, el receptor detectará simultáneamente un 1 proveniente de la señal reflejada y un 0 de la señal directa, es decir el símbolo 1 esta interfiriendo en el símbolo 0 que es el correcto.

Time alignment

A cada móvil, durante una llamada, se le asigna un time slot dentro de una trama TDMA, durante el cual transmite información hacia la BTS. No obstante, la información no solo debe transmitirse en el time slot adecuado, sino que también debe recibirse en el time slot correcto. El problema del *time aligment* ocurre cuando parte de la información transmitida por un móvil no llega a la BTS en el time slot que le correspondería. Es decir, parte de la información llegará en el siguiente time slot, interfiriendo en la información que está mandando el móvil que usa el time slot consecutivo. La causa principal de este fenómeno es una elevada distancia entre el móvil y la BTS, ya que la información no la puede recorrer en el tiempo establecido.

Por ejemplo, un móvil está cerca de una BTS y se le asigna el time slot 3. Durante la llamada, el móvil se aleja de la BTS, provocando que la información que el móvil envía a la BTS y viceversa llegue cada vez más tarde. Si no se soluciona el problema, reasignando un nuevo time slot, el retraso será tal que la transmisión desde el móvil en el time slot 3 se solapará con la información que la BTS recibe en el time slot 4.

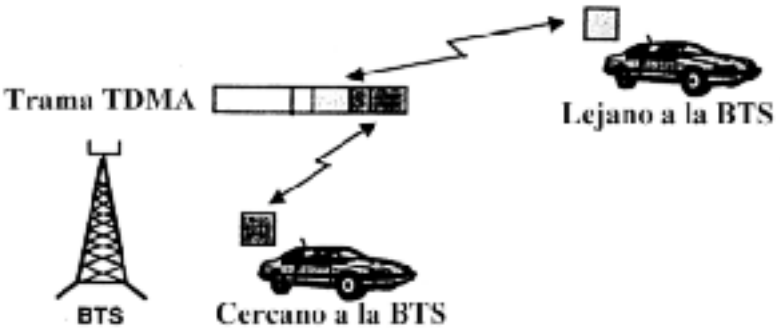

Figura 19: Time alignment

Perdidas conjuntas de la señal

Cada uno de los problemas descritos anteriormente suele ocurrir de forma independiente, aunque en ocasiones aparecen de forma conjunta. En la siguiente figura, donde se muestra la potencia de la señal en la antena receptora del móvil cuando éste se aleja de la antena transmisora de la BTS, pueden observarse los efectos de las perdidas por distancia, por sombra y por Rayleigh fading.

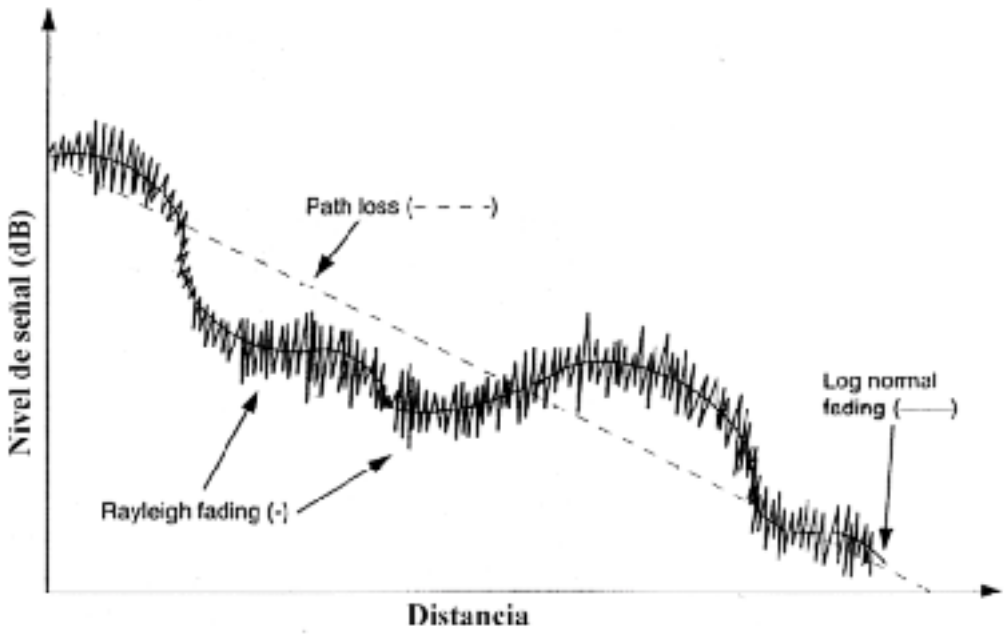

Figura 20: Perdidas conjuntas de la señal

Como puede observarse, la potencia de la señal en valor medio, decrece a medida que el móvil se aleja, provocando finalmente la perdida de la llamada. Las variaciones lentas de la señal se deben a los efectos de la sombra y las variaciones rápidas son debidas al Rayleigh fading.

En la siguiente figura se muestra la señal que se recibiría por parte del móvil en la antena de la BTS.

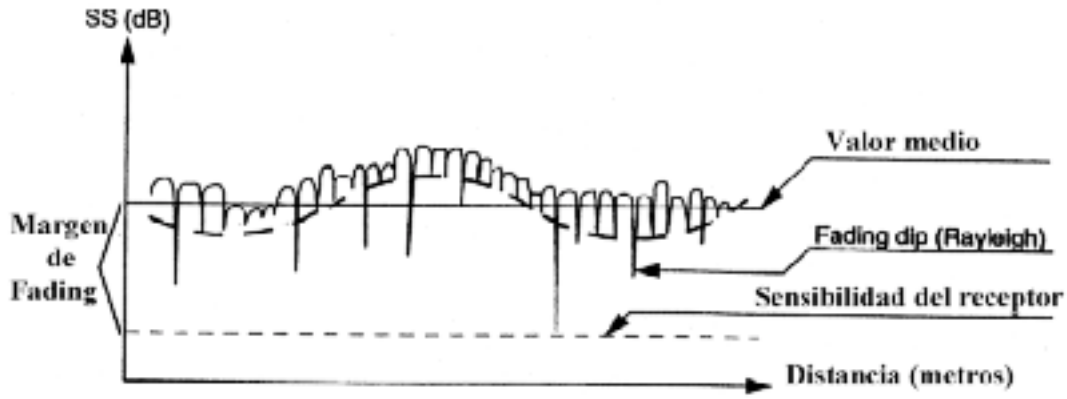

Figura 21: Sensibilidad del receptor y margen de fading

El mínimo nivel de potencia de señal necesario se denomina sensibilidad del receptor. Si la potencia cae por debajo de este nivel la llamada será perdida. Para evitar esto, el nivel medio de señal recibida debe estar por encima de la sensibilidad del receptor un determinado margen. Dicho margen se conoce como margen de fading y en la teoría debe ser igual al mayor decaimiento de la potencia que pudiera producirse. Es la diferencia entre el valor medio de la señal y la sensibilidad del receptor.

Solución a los problemas de la transmisión

Esta sección describe algunas soluciones a los problemas descritos anteriormente. Dichas soluciones no resuelven completamente los problemas, pero si juegan un papel importante en el mantenimiento de la calidad de la llamada durante el mayor tiempo posible.

Codificación del canal

En la transmisión digital, la calidad de la señal transmitida se cuantifica a menudo en función de la cantidad de bits erróneos recibidos. El BER (Bit Error Rate) define que porcentaje del número total de bits recibidos son erróneos.

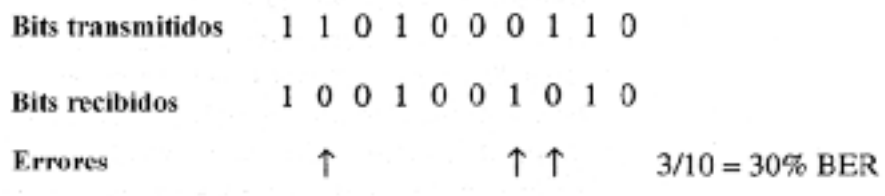

Figura 22: Tasa de error (BER)

Este porcentaje debería ser el mínimo posible, aunque es imposible reducirlo a cero, ya que las propiedades del camino de transmisión dentro de un sistema de telefonía móvil están cambiando continuamente. Esto significa que debe existir cierta tolerancia frente a los errores, y que a la vez debe existir una capacidad de corrección, o al menos de detección de errores, para que estos no sean interpretados como información correcta. Este hecho es especialmente importante en la transmisión de datos, ya que en la transmisión de voz se acepta un mayor BER.

La codificación del canal, en este sentido, se utiliza para detectar y corregir errores en la trama de bits recibidos. Básicamente, consiste en añadir bits de redundancia al mensaje, cosa que permitirá a un decodificador de canal detectar y, potencialmente, corregir ciertos errores.

Interleaving

En realidad, los errores ocurren en secuencia, es decir, afectan a bits consecutivos, como consecuencia, por ejemplo, de un dip fading. La codificación del canal, descrita anteriormente, resulta efectiva en la detección y corrección de errores simples o secuencias de errores cortas, pero no resulta apropiada para tratar los errores que se producen en ráfagas afectando a secuencias largas de bits consecutivos erróneos.

En la siguiente figura se muestra la forma de actuar del interleaving. Supongamos que uno de los bloques de 4 bits se pierde durante la transmisión. Esto supone un BER del 25% sobre el mensaje total, pero implica un BER del 100% para dicho bloque. Ante esta situación, con la perdida de un bloque entero, el mensaje total sería irrecuperable.

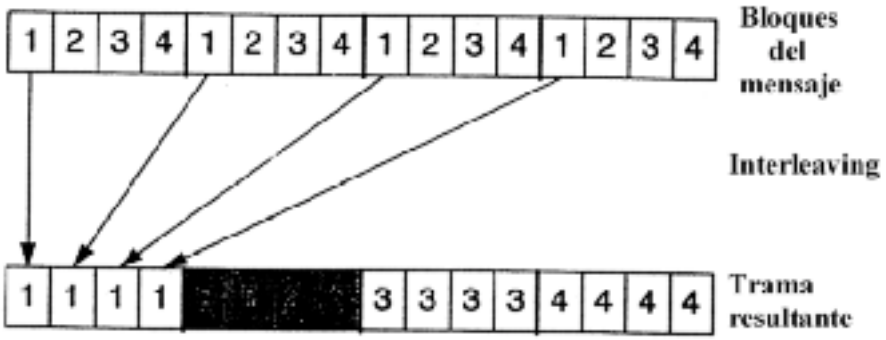

Figura 23: Ráfaga de error sin interleaving

Al aplicar el interleaving, los bits de cada bloque son enviados de forma no consecutiva. Supongamos igualmente que durante la transmisión se pierden los 4 bits de un bloque. Esto implica un BER del 25% sobre el mensaje total, e igualmente un 25% sobre cada uno de los bloques, porque al desaplicar el interleaving en la parte de transmisión hemos distribuido la ráfaga de error entre los distintos bloques. Esta situación es mucho más manejable a lo hora de corregir errores.

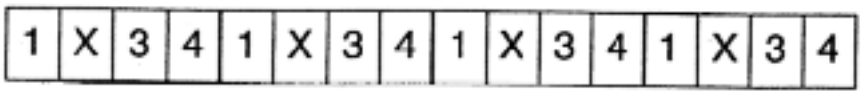

Figura 24: Ráfaga de error con interleaving

Diversidad de la antena

Las técnicas de diversidad aumentan la potencia de la señal recibida en la antena, aprovechando las propiedades naturales de las ondas de radio. Existen dos métodos principales de diversidad: diversidad en el espacio y diversidad por polarización.

Diversidad en el espacio

La potencia de la señal recibida en una BTS puede ser aumentada si se usan 2 antenas receptoras en vez de una, ya que la probabilidad de que ambas se vean afectadas por un dip fading es menor. En el sistema GSM 900 es posible ganar hasta 3dB con una separación de 6 metros entre las antenas, con el simple hecho de escoger la mejor señal, en una antena o en otra, en cada momento. Este método permite un mayor aumento de la ganancia que la diversidad por polarización, pero requiere mayor espacio.

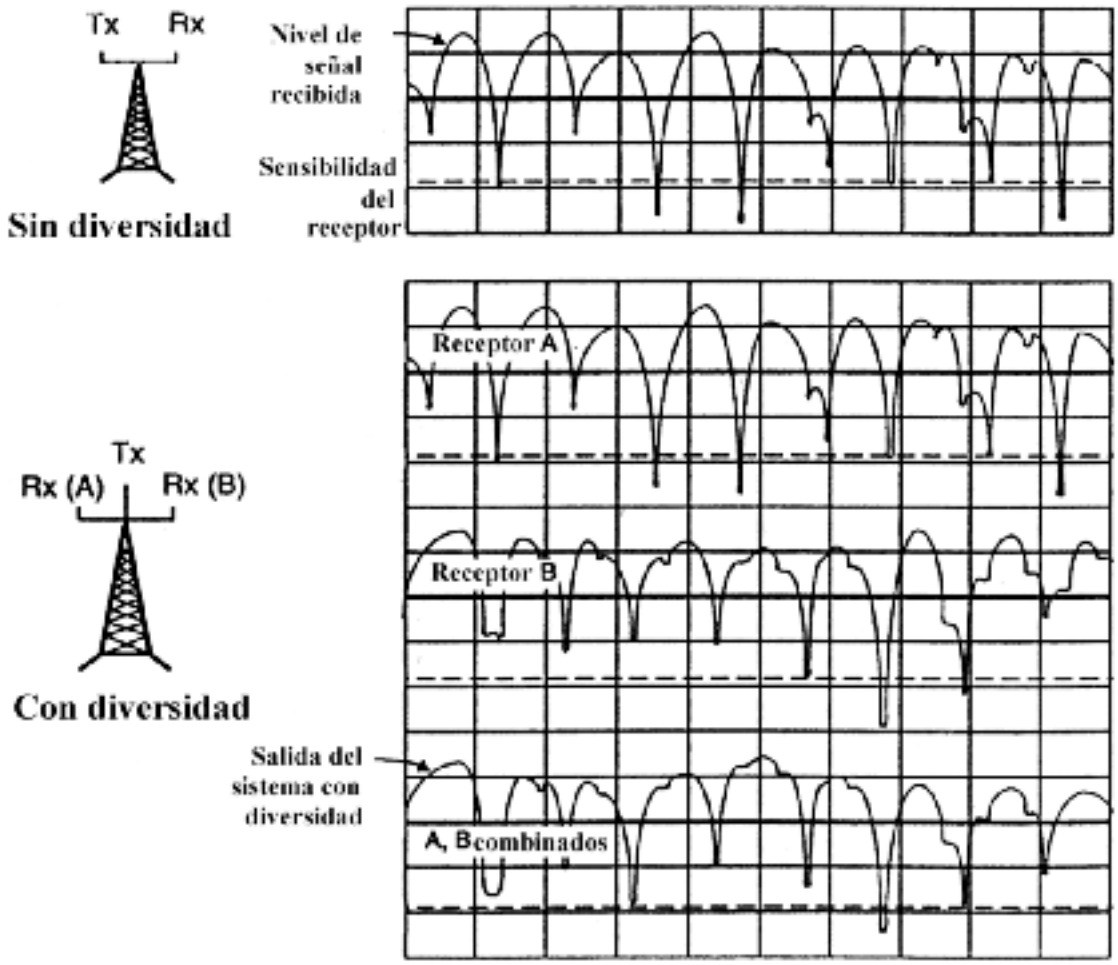

Figura 25: Diversidad en el espacio

Diversidad por polarización

En la diversidad por polarización se usa una antena con polarización dual, es decir, una antena con dos arrays de antenas polarizados de forma distinta. Dichos arrays suelen estar colocados de forma vertical/horizontal o formando ángulos de ±45 grados. Los dos arrays están conectados a la BTS y se escoge, en cada momento, la mejor señal que se reciba en uno de los dos arrays.

Ecualización adaptativa

La ecualización adaptativa es una solución diseñada específicamente para contrarrestar los efectos de la dispersión en el tiempo. Su funcionamiento se basa en el uso de patrones de bits denominados *training secuences*. Estos son conocidos tanto por la BTS como por el terminal móvil, ya que son programados durante el proceso de fabricación. El mecanismo que se sigue es el siguiente:

- La estación base (BTS) indica al terminal móvil que patrón en concreto debe incluir durante la transmisión.
- El terminal móvil incluye dicho patrón (en la figura se representa como “S”) en la transmisión hacia la BTS.
- Cuando la BTS recibe la información del móvil, compara el patrón recibido con el que se acordó usar, si existen diferencias entre ambos es que problemas en el canal radio han provocado errores en la transmisión.
- La BTS asume que los problemas que han afectado al patrón han tenido un efecto similar en el resto de información, e intenta corregirla en base a los errores que ha detectado en el patrón.

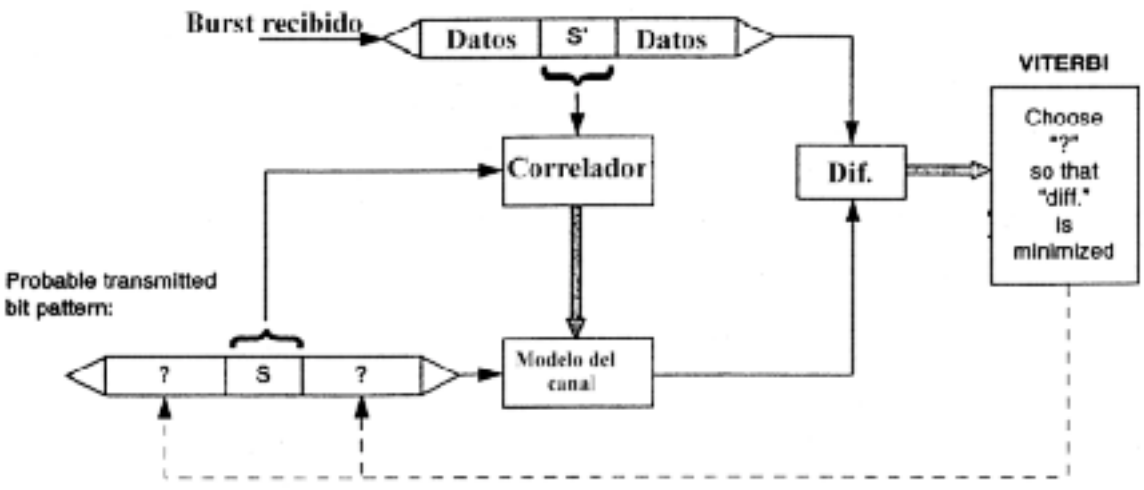

Figura 26: Ecualización adaptativa

Con la ecualización adaptativa se obtienen buenos resultados en cuanto a la corrección de errores, pero no resulta una solución efectiva el 100% de las ocasiones, ya que se realizan ciertas suposiciones sobre el canal radio. El ecualizador de Viterbi es un ejemplo de ecualizador adaptativo.

Saltos en frecuencia

Como se mencionó anteriormente, el efecto Rayleigh fading depende de la frecuencia. Esto significa que si ha una determinada frecuencia tenemos un fading dip elevado, es probable que con otra frecuencia dicho efecto sea mucho menor. Para aprovechar este hecho, la BTS y el móvil usan distintas frecuencias durante la transmisión de forma sincronizada.

En GSM hay 64 patrones de saltos de frecuencia, uno de ellos es cíclico y los 63 restantes son patrones pseudo-aleatorios que el operador puede elegir.

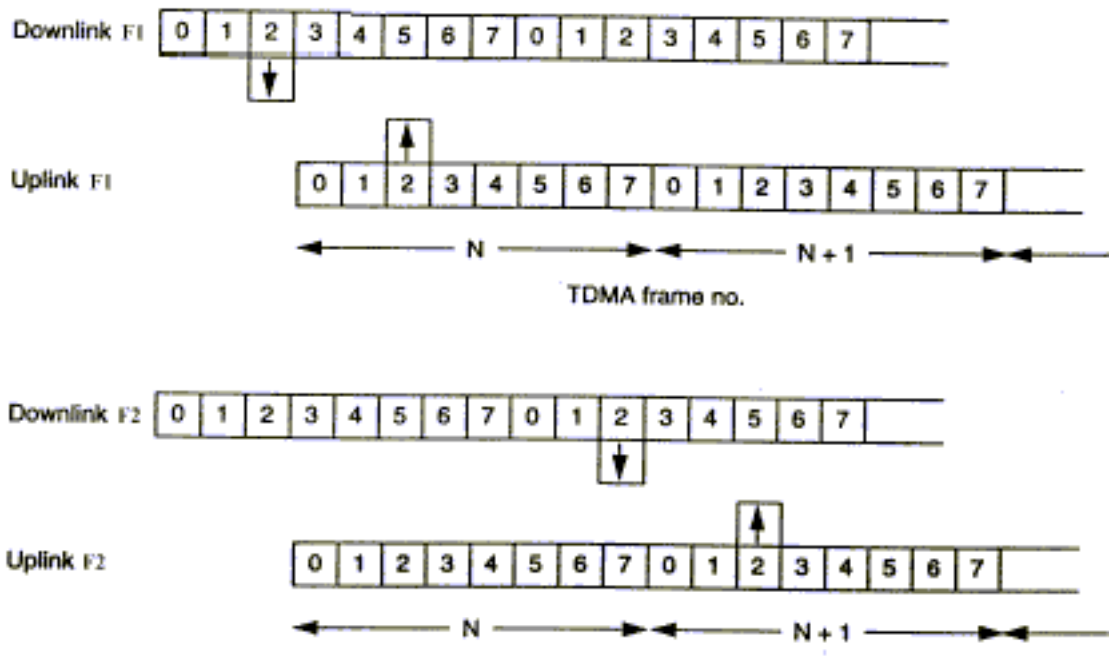

Figura 27: Saltos en frecuencia

En la figura podemos observar que durante cada trama TDMA el time slot se mantiene, pero cambia la frecuencia de transmisión de acuerdo a un patrón preestablecido.

Avance en el tiempo (Timing Advance)

El Timing advance es una técnica desarrollada para solucionar el problema del time alignment. Según este mecanismo, la estación base controla los retardos de cada móvil que esta transmitiendo. Si estos se hacen demasiado grandes, la BTS puede ordenar a los móviles que adelanten su transmisión con respecto a su burst correspondiente, para que la información sea recibida en el momento adecuado.

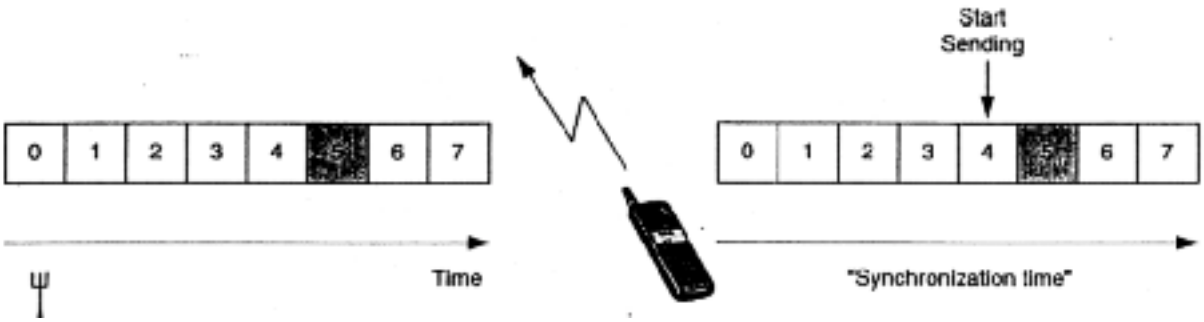

Figura 28: Time advance

Obviamente, este avance en el tiempo no puede crecer de forma indefinida, ya que esta relacionado con el tamaño de la célula. El avance de tiempo está codificado con 6 bits, por lo que puede tomar valores de 0 a 63 (la unidad en este caso es el tiempo de bit que equivale a 3.69μs). Así pues, el avance de tiempo máximo es 63 x 3.69μs = 232.47μs, cosa que se corresponde con una distancia máxima de unos 70Km, suponiendo una velocidad de 3E+8m/s. Esta distancia debe ser entendida como de ida y vuelta, por lo que nos queda un radio máximo de célula de 35Km.

Con esto terminamos el breve repaso al sistema GSM. En la sección siguiente estudiaremos un elemento muy vinculado a dicho sistema, la señalización SS7.

El sistema SS7

Introducción

Durante los primeros 50 años de las comunicaciones telefónicas, la demanda de teléfonos creció de forma paulatina y continuada. Más tarde, durante la depresión económica, la demanda de servicios telefónicos se frenó. No obstante, la tecnología continuó evolucionando, aunque de forma más lenta que en años anteriores. Cuando empezó la segunda guerra mundial, la demanda de servicios telefónicos volvió a incrementarse agudamente. Inicialmente, fueron los motivos puramente militares, los que impulsaron este crecimiento, aunque más tarde, esta demanda fue creciendo debido a las necesidades de una multitud de industrias que formaban parte del engranaje de la guerra.

Los problemas para abastecer esta demanda fueron increíbles, ya que no todas las naciones tomaron acuerdos a nivel de estandarización para facilitar la realización de las llamadas internacionales. Así, las compañías telefónicas tuvieron graves problemas para cubrir las demandas que se produjeron durante este periodo de guerra.

Tras la guerra, la demanda llegó a alcanzar proporciones enormes. Por una parte aparecieron nuevos negocios con nuevas necesidades, y por otra parte, los existentes, casi triplicaban su demanda año tras año. Incluso áreas que nunca habían tenido una fuerte demanda de servicios telefónicos, ahora aumentaban sus líneas, presionadas por el nuevo mundo emergente de las telecomunicaciones modernas.

Para responder a esta demanda las compañías telefónicas no podían hacer más cosas que añadir nuevas líneas. Un millar de nuevos teléfonos podrían suponer 10.000 nuevas llamadas al día, que obviamente necesitaban de nuevas conexiones para llevarlas a cabo. Además, para acrecentar el problema, el tráfico telefónico no era regular, había picos y caídas en el uso del teléfono, es decir, el número de llamadas simultáneas a ser tratadas aumentaba.

Pronto se planteo la cuestión de cómo los cables telefónicos podían ser más eficientes. Obviamente, si cada cable era más eficiente, podría ser capaz de transportar más conversaciones, y así, la cantidad de nuevos cables necesitados disminuiría.

Las causas del problema

Una de las formas de hacer más eficientes los cables era usarlos sólo para transportar conversaciones. Por entonces, el cable que era usado para transportar la conversación, era usado a su vez para transmitir toda la información necesaria para conectar y administrar la llamada, es decir también transportaba información de señalización.

En la época de la posguerra la señalización consistía en representaciones analógicas del sonido. De la misma forma en que la voz se convertía en una señal eléctrica para ser enviada a través del cable, la señalización era enviada sobre el cable en forma de señales analógicas que serían convertidas en sonido en el receptor.

Todos nosotros estamos familiarizados con algunas de esas señales. Si descolgamos el teléfono oímos lo que se llama tono de línea (*dialtone*). Ese sonido indica al llamante que la línea telefónica está conectada a la central local de conmutación y que puede marcar el número destino. En la compañía telefónica, el final de la línea de abonado, el circuito completo que permite enviar la señal de dialtone indica que el teléfono está descolgado. Si alguien llamará en ese momento al aparato descolgado, la llamada no podría ser establecida. Actualmente, con la llamada en espera, un sonido se coloca en la línea indicando que se esta produciendo una llamada entrante, pero anteriormente, si alguien llamaba a un teléfono ocupado o sencillamente descolgado, solo escuchaba la señal de ocupado (*busy*).

Hoy en día, cada dígito marcado coloca dos frecuencias en la línea, que permiten a la central identificar el número pulsado. Esto sistema recibe el nombre de Dual Tone Multifrecuencia (DTMF). Durante los años 40 y 50, la misma información era obtenida mediante la interrupción de la línea de conexión. El número de interrupciones se correspondía con el número marcado. Un dial rotatorio cumplía con esta función.

Una vez que se terminaba de marcar, la compañía telefónica comparaba el número marcado con una tabla de enrutamiento, que proporcionaba la información necesaria para conmutar los canales y enrutar de forma adecuada la llamada. La siguiente central de conmutación también recibía el número marcado y lo consultaba en su propia tabla de enrutamiento, para determinar cual era la siguiente conexión que debía realizarse. Finalmente, la central de conmutación que estaba conectada con el teléfono marcado, intentaba realizar la llamada. Si el llamado estaba hablando, su línea indicaba una condición de descolgado. Antes de que existiera la llamada en espera, esto significaba que se debía retornar una señal de ocupado. Esta señal, no era el único problema asociado a la señalización en el circuito de voz, pero si el más importante, y el que nos puede servir para entender el hecho de querer eliminar la información de señalización de dicho circuito.

El envío de la señal de ocupado suponía que todas las conexiones que se habían realizado para el intento de la llamada, debían permanecer para que esta señal pudiera ser devuelta al llamante, de manera que dicho circuito no podía ser utilizado por otra llamada. El circuito estaba perdido hasta que el llamante colgara el teléfono. Este uso ineficiente del circuito, fue una de las razones que impidieron a las compañías telefónicas sostener la nueva demanda de servicios.

Los conceptos de la solución

Los conceptos digitales estaban ya suficientemente avanzados como para que la compañías telefónicas se plantearan el paso de la información analógica de señalización a paquetes digitales, que serían enviados a través de la red usando cables existentes para el uso digital. Un canal simple o circuito individual analógico podía solo administrar una conversación y la señalización asociada a ésta de una sola vez. Sin embargo, un paquete digital era capaz de transportar información de señalización, y a su vez podía compartir un canal común con cientos o miles de otros paquetes digitales. Así, con sólo una línea digital, se podría transportar la información de señalización de miles de circuitos de voz. Esto se conoce como Canal Común de Señalización.(CCS).

Los resultados de este nuevo concepto fueron claros inmediatamente, ya que la central local era capaz de obtener la información de señalización enviada desde la central remota a través de una línea paralela al circuito de voz. De esta forma podía enviar dicha información al llamante sin que ninguna de las conexiones entre la central origen y destino fueran requeridas para dicha tarea. Tan solo se mantenía en uso la conexión del usuario con la central local.

Este interfaz digital con la red telefónica, y el uso del CCS, iban a ser los precursores de la aparición de los números 900, de las tarjetas de crédito telefónicas y del desarrollo de numerosos servicios, como SMS a móviles, identificación del llamante, y otros servicios inteligentes disponibles a través de esta nueva filosofía.

No obstante, si se pretendía que el nuevo concepto fuera útil, y hablando de comunicaciones un sistema es útil cuando nos permite comunicarnos con cualquier parte del mundo, debía desarrollarse un estándar que estableciera las guías de cómo el nuevo sistema podía actuar en cada situación. El organización que llevó a cabo este trabajo fue el CCITT (Consultative Committee on International Telephone and Telegraph).

La historia de los organismos de estandarización

Los estándares de telecomunicaciones empiezan cuando en Mayo de 1865, la Convención Internacional de Telegrafía fue firmada por 20 países. Una vez el acuerdo fue establecido, la organización conocida como Unión Internacional de Telegrafía, fue la encargada de reglamentar los aspectos discutidos en el acuerdo, para que estos pudieran llevarse a cabo.

Diez años después, la invención y rápido desarrollo de los servicios telefónicos, hizo que la Unión de Telegrafía empezará a recomendar estándares para el uso internacional de la telefonía.

Las comunicaciones radio se unieron solo 20 años después, y la necesidad de hacer uso de normas agilizó la celebración de la Conferencia Internacional de Radio en 1906. El resultado fue la firma de la primera Convención Internacional de Radio-Telegrafía.

Por 1927 ya había un Comité Consultivo Internacional de Radio (CCIR), un Comité Consultivo Internacional de Telefonía (CCIF) y un Comité Consultivo Internacional de Telegrafía (CCIT). En 1932, se decidió combinar las Convenciones de Telegrafía y Radio-Telegrafía, formando así la Convención Internacional de Telecomunicaciones, que en 1934 paso a denominarse ITU (Unión Internacional de las Telecomunicaciones).

Después de la segunda guerra mundial, en 1956, el CCIF y la CCIT se unieron formando el CCITT (Comité Consultivo Internacional de Telefonía y Telegrafía). A este grupo se le encargó la realización de las recomendaciones que serían conocidas posteriormente como Sistema de Señalización SS7. En los años siguientes los subcomités fueron reorganizados y la CCITT fue reemplazada por la actual ITU-TS.

Obviamente, no se nombró al nuevo sistema de señalización como número 7, sin más. Existieron 6 versiones anteriores, pero éstas nunca pasaron del papel a la práctica. El sistema anterior al SS7, por ejemplo, se denominaba CCIOS6 (Common Channel Interoffice Signalling Systems). Por ultimo mencionar que cada cuatro años, empezando desde 1976, las recomendaciones establecidas se recogen en una solo colección que se distingue de las anteriores por el color de sus portadas. Así, actualmente se puede consultar, el libro Naranja (1976), el libro Amarillo (1980) o el libro Blanco (1992), por ejemplo.

Arquitectura del sistema de señalización SS7

Signalling Tranfer Point (STP)

¿Cual es el elemento clave en la red pública telefónica conmutada (PSTN)? Obviamente, existen varios elementos importantes, pero son los centros de conmutación los que hacen que sea verdaderamente una red. Los centros de conmutación son el elemento de unión entre todos los componentes que forman la red.

En el sistema de señalización SS7, dichos elementos de conmutación reciben el nombre de STP (Signaling Transfer Point).

La PSTN requiere conexiones entre líneas de voz, y la forma de organizar dichas líneas y las conexiones entre ellas determinará en gran medida la capacidad final de la red. El sistema SS7 requiere el uso de líneas de transmisión que estén continuamente disponibles. Estas conexiones permanentes reciben el nombre de links y pueden ser individuales o estar agrupados (T1,E1).

El trabajo del STP es examinar el destino de los mensajes que recibe, consultar una tabla de enrutamiento, y enviar los mensajes a través del link establecido en dicha tabla. El enrutamiento es necesario porque, como las centrales de conmutación, los STP pueden tener tanto links a nodos finales dentro de la red como a otros STP, que completarán el enrutamiento de las comunicaciones que no son directas a través del STP que manda el mensaje.

Por otra parte, el buen funcionamiento de las telecomunicaciones exige redundancia. Por esta razón los STP están siempre duplicados. Los links que conectan los STP permiten a los mensajes cruzar de uno a otro y se conocen como Cross Links o simplemente como C links.

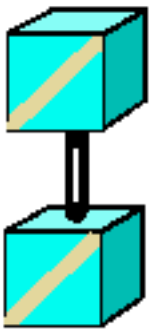

Figura 29: Signalling Transfer Point (STP)

Las denominaciones que reciben los links dentro del sistema SS7 se definen en función de lo que conectan, y a veces, en función de la tarea que desempeñan. Se usan letras del alfabeto (A-F). Conociendo los tipos de links podemos tener un conocimiento inmediato del tipo de nodos de la red, independientemente de las aplicaciones que funcionen en ellos.

Signalling End Point (SEP)

El SEP es el punto terminal dentro del sistema SS7, de la mima forma que el teléfono es el punto terminal dentro de la PSTN. El teléfono tiene una dirección, en forma de número telefónico, que le permite ser reconocido dentro de la PSTN por los centros de conmutación.

El SEP usa una dirección que se conoce como SPC (Signalling Point Code). Dicha dirección esta formada por tres partes, que reciben el nombre de Red, Cluster y Miembro, de la misma forma que un número de teléfono consta de un código de área, de un código de central y de un número de línea.

Dentro de la PSTN, el número de teléfono tiene cierta relación con el área geográfica en la que nos encontremos, cosa que no ocurre con las direcciones del sistema SS7. En este caso, las direcciones están relacionadas con la forma en la que los SEP se conectan a los STP's

Los enlaces mostrados en la figura conectan un SEP a un STP, proporcionando acceso a la red para el SEP. Por esta razón, dichos enlaces reciben el nombre de Access Links, o simplemente A links. De las dos conexiones que existen entre el SEP y los STP, una debe ser escogida como principal. Generalmente, el más cercano o el que menor tráfico está cursando se escoge como principal, aunque en muchos casos el SEP sólo dispone de una conexión a la red a través de un STP local.

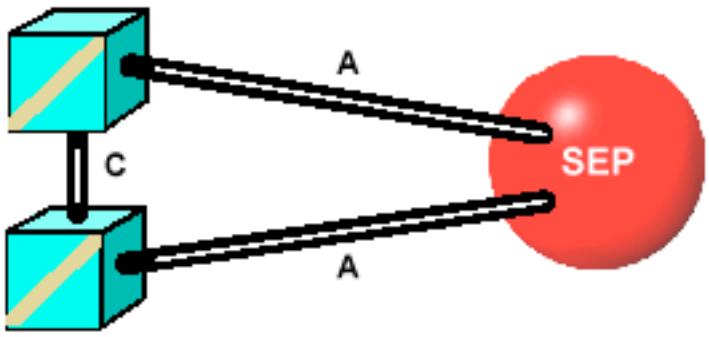

Figura 30: Signalling End Point (SEP)

Enlaces de tipo B y D

Un STP que no tiene links con la red vecina no puede enrutar mensajes, salvo que sean mensajes provenientes y dirigidos a los SEP's que se conectan a él. Así, para que un STP cumpla realmente con sus funciones de enrutamiento debe estar conectado a los STP's vecinos. Por el hecho de la redundancia, cada STP del par se conecta a cada STP del par vecino. El resultado son cuatro enlaces que forman un puente entre dos redes locales. Por esto, los enlaces reciben el nombre de Bridge Links, o simplemente B links.

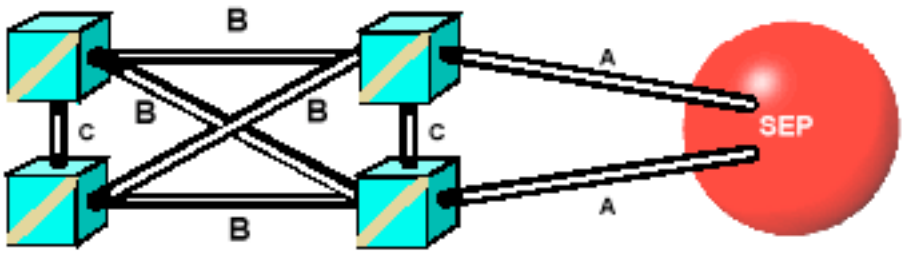

Figura 31: Interconexión entre STP's

Al igual que en la PSTN, en el sistema de señalización SS7 también existe una jerarquía de conmutación. Los pares de STP's locales conectan SEP's a la red. Pero si un STP se conecta solo a los STP's vecinos sus capacidades de enrutamiento se limitan y además las conexiones requeridas aumentan. Por eso también existen STP's que pertenecen a una jerarquía superior, que no conectan SEP's a la red, sino que se dedican a conectar STP's entre si, es decir a conectar subredes pertenecientes a distintos niveles de conmutación entre si. El resultado son los llamados Diagonal links o D links.

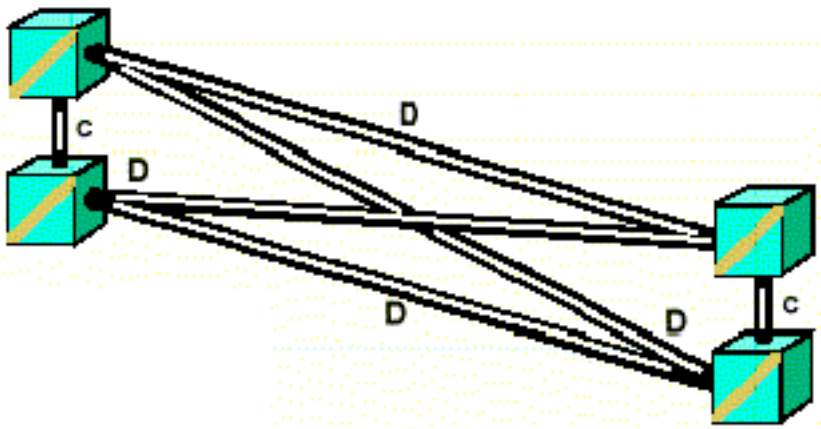

Figura 32: Interconexión entre STP's pertenecientes a distinto nivel de conmutación

Enlaces de tipo E y F

Ya hemos mencionado un tipo de conexión entre los SEP's y los STP's, pero existe otro. Para mejorar el acceso al red que tiene un SEP, este podría tener links de tipo A redundantes con su par de STP locales. No obstante, lo que se hace es escoger otro par de STP's para conectarse a él, ganando así mayor capacidad de acceso a la red en caso de caída del par local de STP's. Este nuevo STP suele estar más alejado. Los nuevos links se denominan extended links o E links.

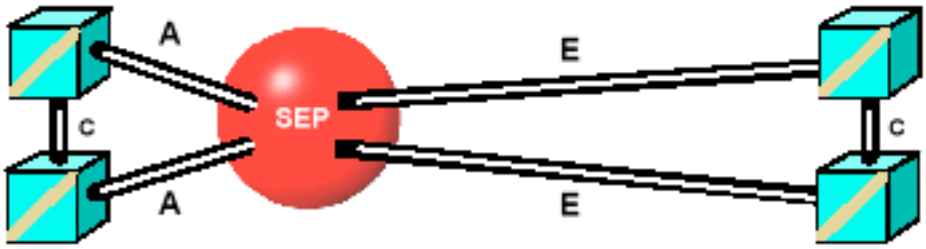

Figura 32: Enlaces de tipo E

En muchas redes, existen nodos SEP que solamente tienen la función de proveer o almacenar datos y de realizar operaciones particulares propias de cada operador. Dichos nodos especiales puede tener o no un acceso a la red. En la figura podemos observar que tanto el SEP como el SEP especial tienen A links, por lo tanto dichos nodos podrían comunicarse a través de sus respectivos STP's. Sin embargo, disponen de una conexión directa, denominada F link (Fully Associated).

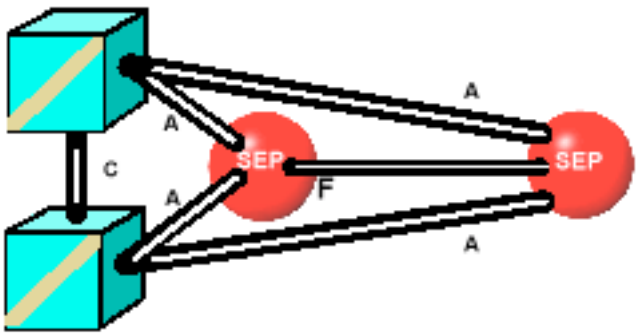

Figura 33: Enlaces de tipo F

Estos links de tipo F solo son usados por los SEP que se conectan a través de ellos. Por lo tanto puede usarse un protocolo propio más simple que en el resto de la red, y que sea suficiente para que ambos nodos entiendan la infomación transmitida y el propósito de ésta.

Tipos de nodos de señalización

En nuestra discusión hemos usado el termino SEP para describir un Punto de Señalización Final genérico. Ahora veremos los tipos específicos de puntos de señalización, y ya que el sistema SS7 surge con la idea de mejorar la eficiencia de la red PSTN, comenzaremos por mencionar los puntos en común.

SSP (Service Switching Point) y CCSSO (Common Chanel Signalling Switching Office)

Estos dos tipos de nodos de señalización están relacionados. El primero recibe el nombre de CCSSO (Common Chanel Signalling Switching Office). Con este termino nos referimos a las centralitas de las oficinas que tienen la capacidad de usar SS7 en lo que se refiere a la señalización de las llamadas interurbanas.

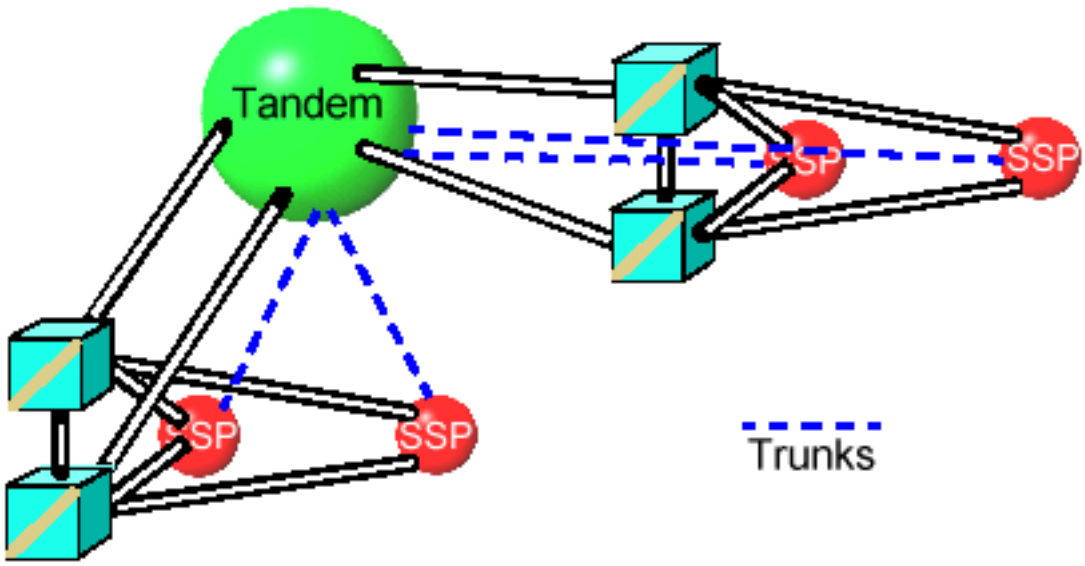

Figura 34: SSP y CCSSO

El segundo se denomina SSP (Service Switching Point). Como el CCSSO, este nodo puede manejar llamadas, y además tiene otras capacidades, como la de hacer peticiones a bases de datos para actuar en función de sus respuestas. La mayor diferencia entre ambos es que el CCSSO no dispone de software, cosa que lo convierte en una versión limitada de un SSP.

SCP (Service Control Point)

Cuando un número tal como 900 o 902 es marcado, no existe posibilidad para el elemento de conmutación de enrutar la llamada, porque verdaderamente no se corresponde con un número de teléfono real. De hecho, un número 900 nos puede conectar con números distintos en función del área geográfica donde nos encontremos. Exactamente, el elemento de conmutación envía una petición a una base de datos, que le contesta con una traducción del número 900 a un número telefónico real. Entonces la llamada se enruta tal y como si se hubiera marcado dicho número desde el primer momento.

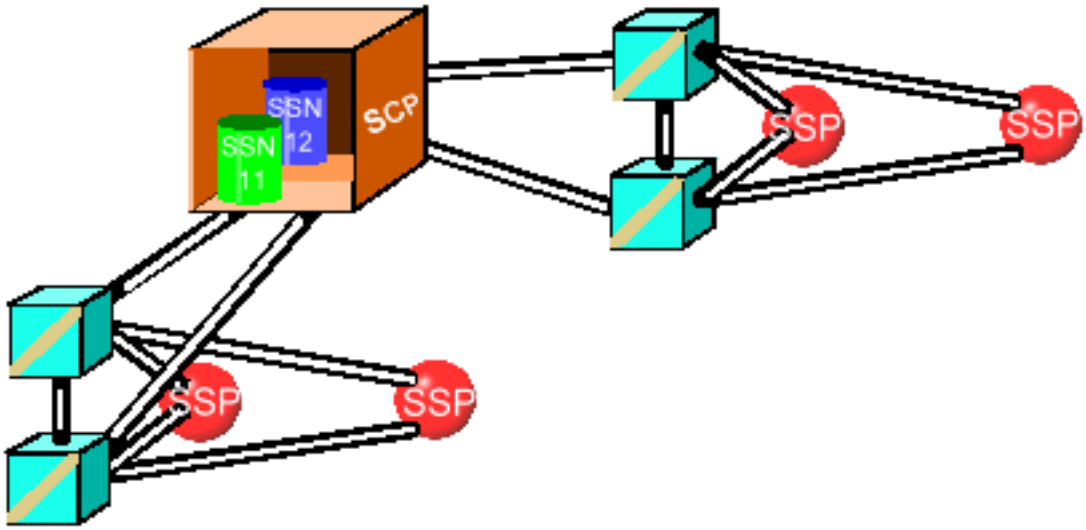

Figura 35: Funcionalidad del SCP

La base de datos que realiza esta función esta localizada en una dirección SS7 (Signalling Point Code). Un nodo de este tipo, que es capaz de proporcionar información de una base de datos o realizar otra serie de tareas digitales, como verificación de tarjetas telefónicas, se denomina SCP (Service Control Point).

El SCP proporciona el punto de acceso requerido para distintos servicios digitales, como hemos mencionado anteriormente. No obstante, estos servicios pueden residir o no en la misma localización que el SCP. En muchas ocasiones el SCP realiza las tareas de Front End para los servicios localizados en otra parte.

Como hemos dicho, los nodos en el sistema SS7 tienen una dirección (SCP). Pero esto no es suficiente para un direccionamiento correcto si pretendemos acceder a un determinado servicio ubicado en un SCP. Otro valor debe ser usado para identificar a la aplicación o servicio que se esta intentando localizar. Para este propósito, el sistema SS7 usa simplemente un valor ,representado en el paquete del mensaje con un byte y por lo tanto con un rango de 0 a 255, que se llama SSN (Subsystem number).

El número de subsistema identifica típicamente a bases de datos, ya que son las aplicaciones más frecuentes que suelen residir en un SCP. Sin embargo, pueden identificar cualquier otro servicio. Resumiendo, como el SPC proporciona acceso a distintos servicios, no basta con transmitir las peticiones al SPC, sino que se tiene que mandar el SSN para especificar la dirección exacta del servicio que se requiere, dentro del SCP.

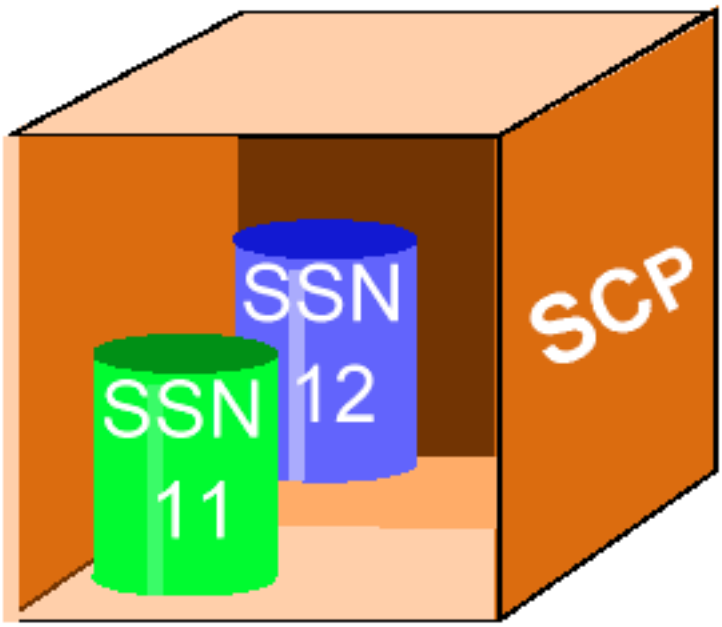

Figura 36: Estructura de un SCP

IP (Intelligent Peripheral)

En muchas ocasiones, determinados servicios precisan funcionalidades para las que el SCP no esta equipado, y ésto acarrea la utilización del Periférico Inteligente. En general, el IP es como un nodo de señalización mucho más potente que el resto, que puede manejar las peticiones hechas desde de la red, proveyendo a los servicios de mayor equipamiento, características y funcionalidades.

En el mundo de las telecomunicaciones, muchas tecnologías quedan obsoletas rápidamente. Obviamente, las nuevas tecnologías requieren nuevo equipamiento, y desplegar este nuevo equipamiento lleva tiempo y conlleva una serie de gastos. Esto implica que en numerosas ocasiones las viejas y nuevas tecnologías tengan que coexistir.

Una respuesta para este problema es instalar ambas tecnologías en un número limitado de localizaciones de la red y permitir al resto de nodos acceder a ellas cuando les sea necesario. Estos nodos son los IP's, que además de cumplir con esta función de concentración, tienen, como hemos dicho anteriormente, otra muy importante, la de implementar servicios de valor añadido que precisan de actuación software y hardware muy potente, que no puede ser soportada por otro tipo de nodo dentro de la red.

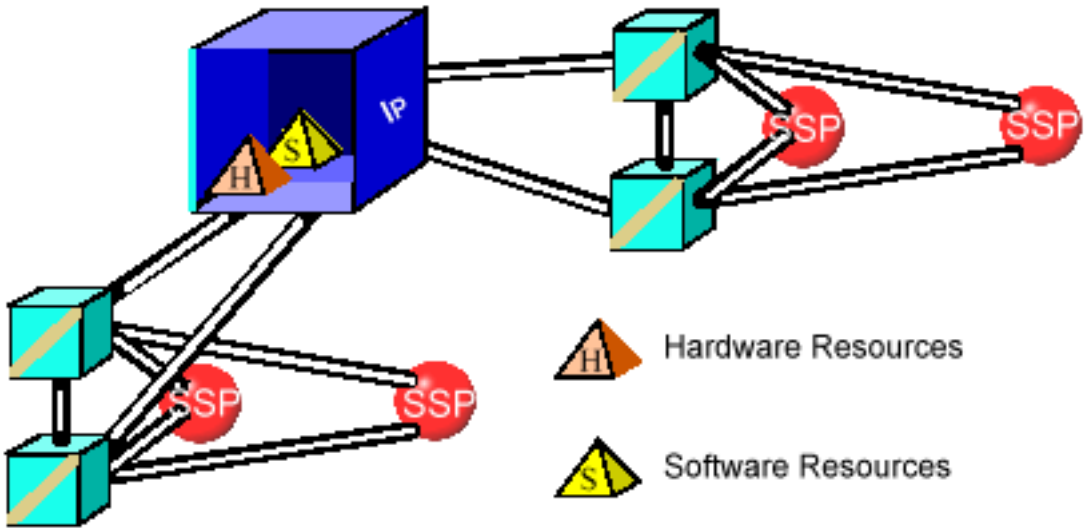

Figura 37: Estructura del IP

MSC (Mobile Switching Center)

Las redes de telefonía móvil disponen de numerosos nodos dentro de la red SS7. Los centros de conmutación móviles controlan y se comunican con los transceptores que están dentro de las células. El transceptor cumple con la parte radio de una red móvil. El siguiente paso es que la MSC establezca una conexión con la PSTN o con otra red móvil en modo entrante o en modo saliente.

No obstante, para realizar la llamada o cualquier otra acción invocada por el usuario, la MSC debe obtener antes cierta información. Esto lo realiza poniéndose en contacto con distintos nodos de señalización:

- HLR: Base de datos donde reside la información propia del usuario.
- AUC: Implementa procesos de seguridad para verificar y validar los teléfonos que se usan.
- SMC: Short Message Center, que coordinar el envío de mensajes cortos.

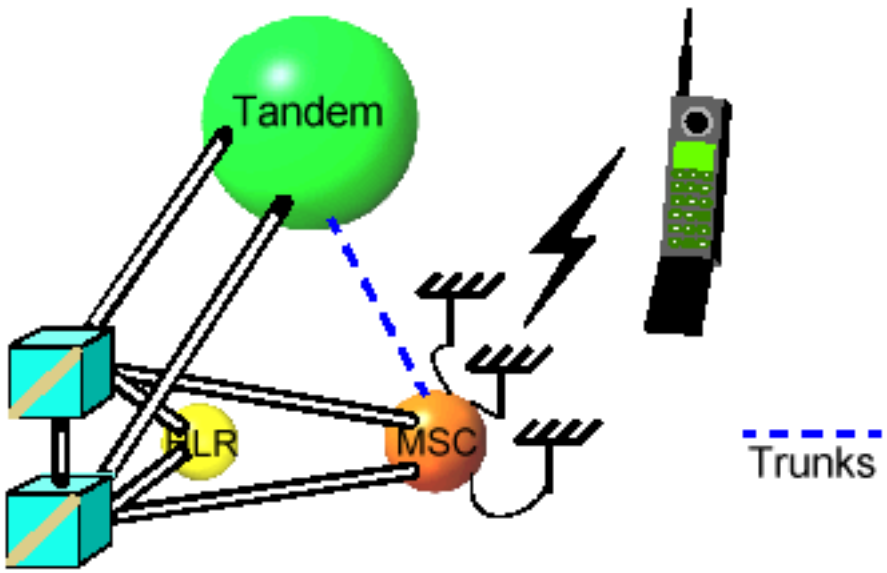

Figura 38: Relación entre la red móvil y el sistema SS7

Por último, hacer hincapié en el hecho de que las tres aplicaciones mencionadas anteriormente, que son tan solo un ejemplo, pueden residir en nodos de señalización por separado, o conjuntamente en uno único. En este último caso se tendría que acceder a ellas a través del SSN.

El modelo de capas

Introducción

Para entender el sistema SS7, es necesario entender el modelo de capas en que se organizan los distintos protocolos. Hacia 1983, algunas de las mayores compañías de telecomunicaciones habían empezado a darse cuenta de los problemas que existían cuando ordenadores de distintos tipos pretendían comunicarse. Así, se decidió crear un interfaz especificó que pudiera ser usado por todos.

No obstante, durante el proceso se percibió que, creando un interfaz específico, se iba a cerrar la posibilidad de implementar y desarrollar futuros estándares y tecnologías de computadores. Así que se decidió no crear un interfaz específico, sino un modelo de arquitectura en capas que permitiera desarrollar futuras tecnologías. El resultado fue el modelo OSI (Open Systems Interconnection), que más tarde sería adoptado por la ISO (International Standars Organization).

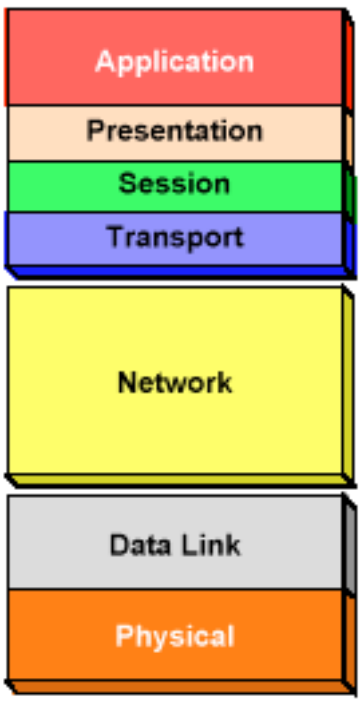

Figura 39: Modelo de capas (OSI)

Un protocolo de capas consiste en una serie de módulos, cada uno diseñado para cumplir un cierto grupo de funcionalidades propias, y para ofrecer dichas funcionalidades al resto de módulos. Un módulo puede estar constituido por uno o varios protocolos organizados

de distintas formas, la única restricción es que cumpla las funcionalidades especificadas y que se atenga al interfaz de comunicación entre el módulo superior e inferior. Es decir, cada módulo es parte de la arquitectura total del modelo y ofrece sus facilidades a otros, que se denominan Partes de Usuario.

Hay numerosas ventajas que provienen de usar el modelo de capas. Por ejemplo, para añadir una nueva funcionalidad a un módulo, sencillamente se tendrían que respetar los interfaces de comunicación, de forma que la nueva funcionalidad sería totalmente transparente para el resto de módulos. Por otra parte, para añadir una nueva parte de usuario a una red vieja, lo único que se tiene que hacer es desarrollar su propia funcionalidad, y después hacer que use las funcionalidades que necesite de las existentes. De esta forma, la conversión de protocolos y la combinación de redes resulta sencilla, simplemente usando los servicios disponibles en cada red.

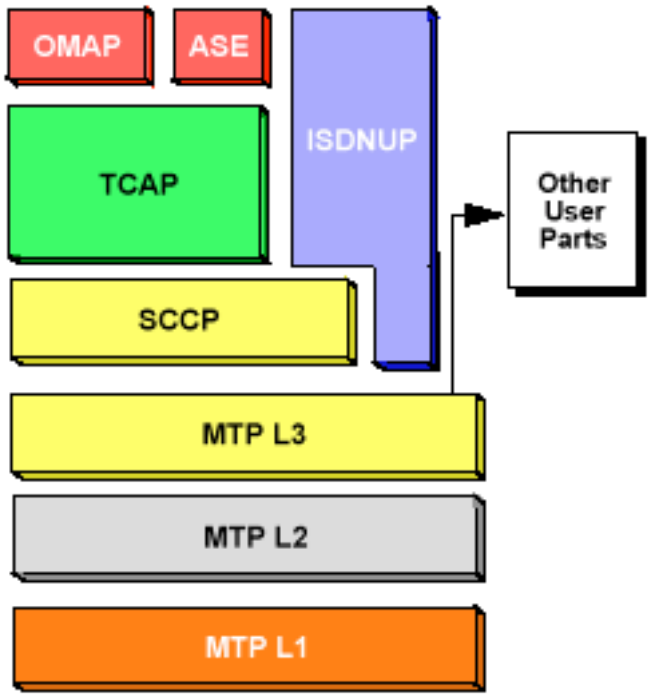

Figura 40: Modelo de capas del sistema de señalización SS7

Paralelismo entre el modelo SS7 y el modelo OSI

Es dificil encontrar un sistema que incorpore todas las funcionalidades de las siete capas de la arquitectura, agrupadas además de la misma forma que en el modelo de capas OSI. El sistema de señalización SS7 no es una excepción. En la siguiente figura se puede observar que, mientras la mayoría de las capas bajas incorporan directamente las funcionalidades correspondientes de OSI, algunas de las funcionalidades de las capas altas se mezclan y no tienen un paralelismo directo, por ejemplo, la ISDNUP (Integrated Services Digital Network Users Part) se extiende a través de la capa de red y la capa de aplicación.

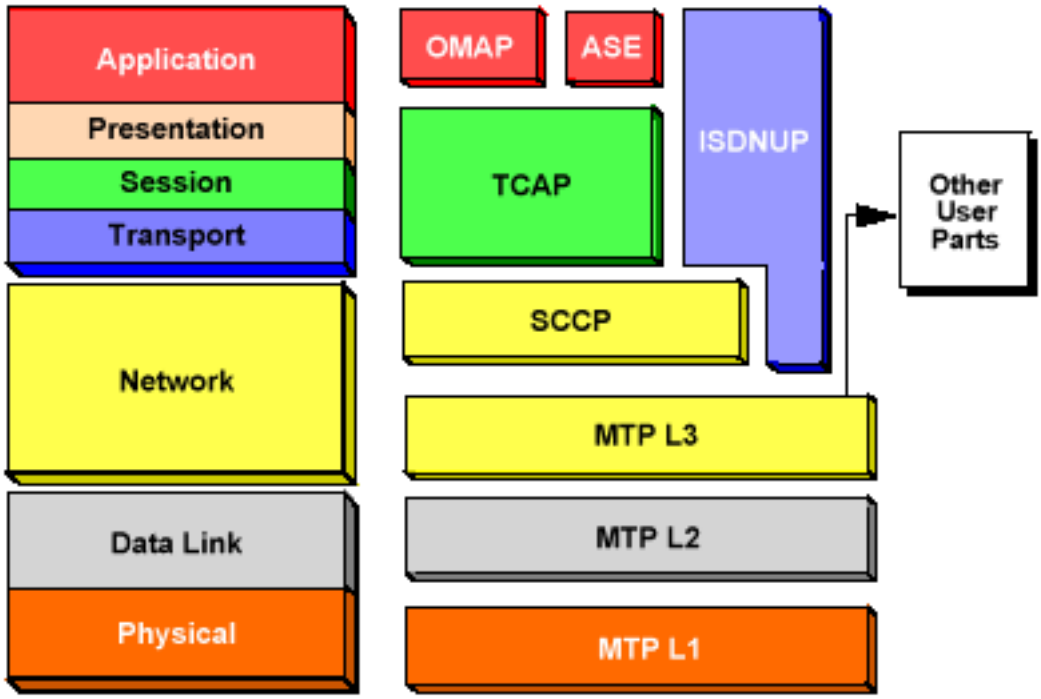

Figura 41: Paralelismo entre las capas del sistema SS7 y el modelo OSI

Se pueden apreciar, además de las capas principales en las que nos centraremos posteriormente, la parte OMAP (Operations, Maintenance and Administration Part) y la parte ASE (Application Service Element), que están ubicadas en el nivel de aplicación. La parte de *Otras Partes de Usuario* que no se muestra aquí, incluye la TUP (Telephone Users Part) y la DUP (Data Users Part).

El modelo OSI recomienda que las comunicaciones entre las capas sean lo mas simple posibles. De esta forma se previenen pérdidas en efectividad en las conexiones entre las capas. El SS7 cumple este requerimiento a través del uso de primitivas, que no son más que códigos que se transmiten entre las distintas capas para identificar los servicios requeridos de la capa receptora. Se suelen clasificar en primitivas de:

- Petición
- Indicación
- Respuesta
- Confirmaciones

A continuación se muestra la figura básica en la que se basara el desarrollo de las principales capas del sistema SS7.

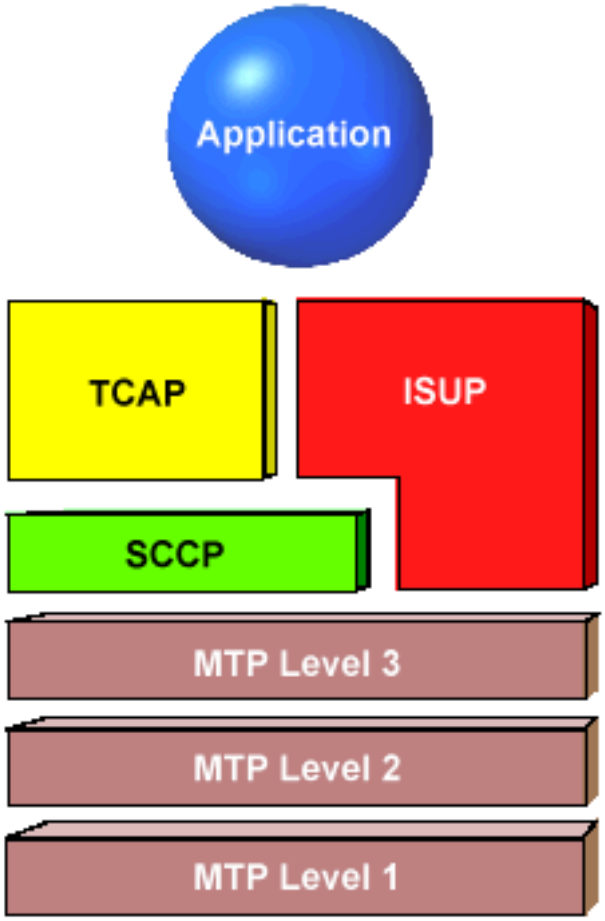

Figura 42: Modelo de capas genérica del sistema SS7

MTP 1

Comenzaremos el examen de las capas por los niveles más bajos. Estos son los niveles que primero manejan los mensajes recibidos y los últimos en manejar los mensajes salientes.

La capa MTP (Message Transfer Part) nivel 1 representa la capa física. Esto significa que es la capa que controla la conexión entre los distintos nodos de la red, donde los diferentes servicios residen y se ejecutan, y a los que es necesario acceder. El MTP de nivel 1 se encarga del control de los enlaces, de los sincronismos y de todas las consideraciones físicas necesarias a la hora de transmitir datos sobre un medio físico.

Esta capa concierne a los ingenieros eléctricos, que son los encargados de considerar que tipos de líneas de transmisión podrían ser validas dentro de la infraestructura de la red. Así pues, esta capa es básicamente de tipo hardware. Para los ingenieros software tiene poco interés, ya que solo son concernidos por la MTP de nivel 1 en el sentido de que ellos se encuentran por encima, y obviamente, es necesario un interfaz y una buena interacción con la capa física.

Figura 43: MTP nivel 1

Las tarjetas de interfaz para el nivel físico SS7 están extendidas dentro de la infraestructura de las telecomunicaciones a lo largo de todo el mundo. El estándar SS7 tiene, además, numerosas variaciones que le permiten trabajar sobre T1, E1 o DS0, entre otras posibilidades.

MTP 2

Introducción

En el siguiente nivel, el sistema SS7 empieza a ser inteligente. Esto implica, desde el punto de vista de las capas, que el MTP de nivel 2 implementa el último paso inteligente de un mensaje antes de ser transmitido a través de los links, de la misma manera que realiza la primera acción inteligente cuando un mensaje es recibido desde la red.

El MTP de nivel 2 esta muy relacionado con los links, y una de las principales tareas que tiene asignada es la monitorización de estos y el control de la congestión. Estrictamente hablando, es imposible que un link se congestione, ya que un link transportara solo tanto tráfico como la línea de transmisión le permita, por ejemplo 64.000 bits/s. La congestión realmente se refiere a las colas de mensajes que esperan a ser transmitidos. Las colas están limitadas en tamaño, y si se envía un mensaje a una cola que está completa (congestionada), éste será perdido.

El sistema SS7 tiene numerosos mecanismos para manejar la congestión, pero el MTP de nivel 2 simplemente la monitoriza y la reporta, es decir, no la controla estrictamente salvo en determinados aspectos que se comentarán seguidamente. Este trabajo lo hará el MTP 3.

Otro tarea del nivel 2 es reorganizar los mensajes salientes en forma de paquetes básicos, que reciben el nombre de unidades de señalización. Hay tres tipos de unidades de señalización, con características comunes. Dichas unidades de señalización pueden ser de hasta 279 octetos.

- El paquete que se utiliza para incluir el mensaje SS7 es llamado **Message Signal Unit**.
- El paquete usado solamente para transmitir información acerca de los links se denomina **Link Status Signal Unit**.
- Finalmente, existe un paquete usado para asegurarse de que no hay cortes en la transmisión y de que hay datos reconocibles sobre el link, llamado **Fill In Signal Unit**.

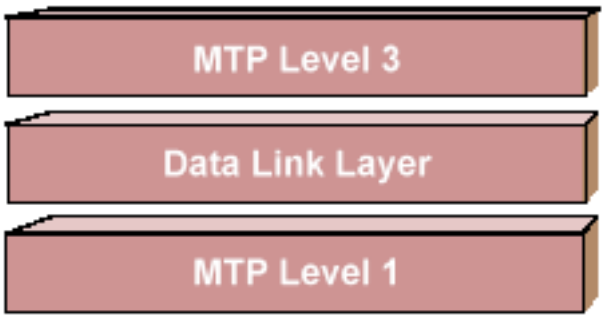

Figura 44: MTP de nivel 2

Mecanismo de la transmisión de datos

En toda trama de datos es importante para la parte de recepción reconocer donde se debe empezar a leer el paquete. Por esto, el MTP de nivel 2 tiene la tarea de aplicar un código de "*empieza a leer aquí*" a cada paquete. En las redes ANSI se usa el código al principio de cada paquete, mientras que en las redes ITU se usa al final y al comienzo de cada paquete. El código o flag se define como un byte con 0 en los extremos y unos en medio (01111110).

No obstante, muchas veces, en la trama de transmisión aparece la misma secuencia de bits, cosa que provocaría la terminación de la lectura del paquete en una red ITU o el comienzo de la lectura del siguiente paquete en una red ANSI, y por lo tanto la lectura incorrecta de la trama. Para evitar esto, la cadena de transmisión es examinada antes de ser transmitida con la intención de localizar secuencias de cinco 1's consecutivos (bit stuffing). Si esto ocurre, se coloca un 0 después del quinto 1. Finalmente, se ponen los flags que delimitan a los paquetes y se transmite el mensaje. En la parte receptora, el MTP de nivel 2 chequea los mensajes entrantes. Después de desechar los flags se lee la trama buscando secuencias de cinco 1's consecutivos, y si los encuentra elimina el 0 siguiente, recuperando de esta forma el mensaje original.

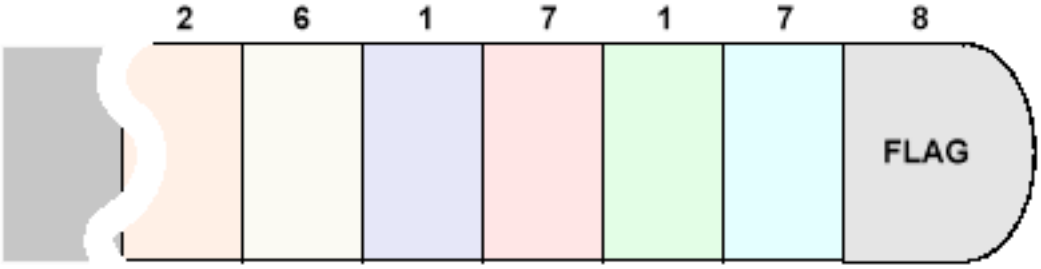

Figura 45: Estructura de la trama en el sistema SS7

El MTP de nivel 2 tiene otras responsabilidades en relación con la transmisión de los mensajes, validar la integridad de los mensajes que recibe y corregir aquellos que no pueden ser leídos. Esto no puede ser realizado por la parte receptora, sin la ayuda de la parte transmisora, y por ello las unidades de señalización incorporan información para facilitar esta tarea.

La figura muestra los campos comunes de las tres unidades de señalización, generalmente estos campos reciben el nombre de "*housekeeping*". Su propósito es proveer a la MTP de la información y los medios necesarios para que esta pueda cumplir con la mayor eficacia posible la misión de salvaguardar la integridad de la información que se transmite y recibe. Así, la MTP es capaz de realizar las siguientes acciones:

- Leer correctamente los paquetes, asegurándose de que los datos no están corruptos.
- Requerir copias de los mensajes cuyos datos son comprometidos o erróneos.
- Permitir la recepción de ack's que indican la buena recepción de los paquetes.

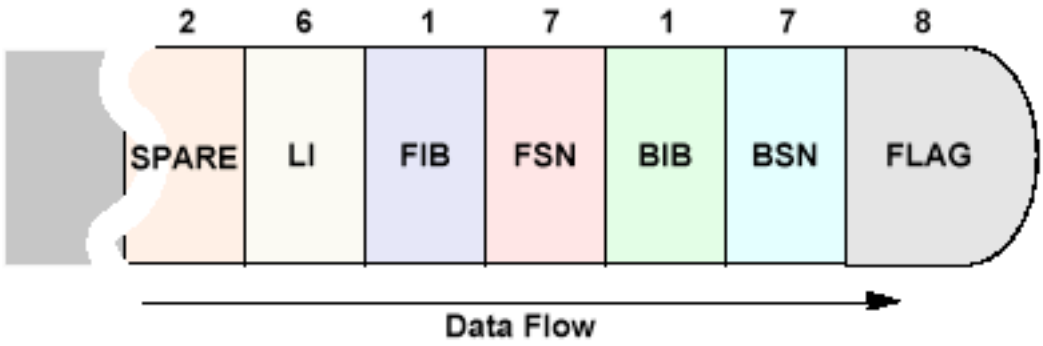

Figura 46: Campos comunes de las unidades de señalización

La flecha indica el sentido de la transmisión. Por lo tanto, los distintos campos más significativos que se van recibiendo son, en este orden:

- Flag de delimitación de los paquetes. (8 bits)
- Campo BSN, Backward Sequence Number. (7 bits)
- Campo BIB, Backward Indicator Bit. (1 bit)
- Campo FSN, Forward Sequence Number, usado por la parte transmisora MTP para colocar valores cíclicos (0-127) que identifican a cada paquete. (7 bits)
- Campo FIB, Forward Indicator Bit. (1 bit)

Los mensajes son transmitidos desde colas que están ubicadas en cada uno de los links. Cada cola está constituida, realmente, por dos buffers. Un buffer desde donde los mensajes son enviados directamente, llamado "*transmit buffer*", y un segundo buffer donde se van copiando los mensajes transmitidos, denominado "*retransmit buffer*". Con el número aplicado para su referencia (FSN), el paquete espera en el buffer de retransmisión hasta que se recibe el acknowledgment que indica que el mensaje se ha recibido correctamente, entonces la copia es destruida.

El proceso que se usa para mantener la integridad de los paquetes que se transmite consta de las siguientes fases:

- Primero la parte transmisora coloca un valor (0-127) en el campo FSN del mensaje a transmitir. El campo BIB se rellena con el valor del último BIB correcto recibido, y el campo FIB se rellena con el mismo valor que el BIB. Así, cuando el mensaje se transmite, contiene un FSN determinado y un BIB y FIB iguales (1 o 0). Una vez que el mensaje ha sido transmitido se copia en el buffer de retransmisión.

- Cada vez que la parte receptora recibe un mensaje correcto, almacena el campo FSN y el campo FIB. Esto lo hace para los mensajes buenos, porque en los malos esta información no podría ser leída asegurando que fuera correcta. De esta forma, la parte receptora conoce en todo momento el valor del FSN y del FIB del último paquete recibido de forma correcta.

- Cuando se recibe un mensaje incorrecto, la parte receptora utiliza la información almacenada del ultimo mensaje correcto (FSN y FIB) para pedir una copia. Esto se realiza utilizando diferentes paquetes. Generalmente, la MTP esta enviando periódicamente información acerca del estado de los links usando un paquete llamado Link Status Signal Unit. El MTP usará el siguiente paquete de este tipo para retornar el ack negativo. En el paquete de vuelta el MTP usa el FSN almacenado del último mensaje correcto como valor para el BSN de ese paquete. También rellena el FIB con el valor almacenado y coloca el BIB al valor contrario. Es decir, si el FIB es 0, el MTP pone el BIB a 1. Cuando la parte transmisora recibe el paquete, lee el valor del último mensaje bien recibido en el BSN y mira si el FIB y el BIB son diferentes o iguales. Si son distintos, se supone que el mensaje ha sido recibido erróneamente y que se requiere una copia, en caso contrario la recepción del paquete ha sido correcta y el mensaje se borra del "*retransmit buffer*".

La figura muestra la forma en que la parte transmisora rellena el FSN y copia los mensajes en el buffer de retransmisión una vez enviado.

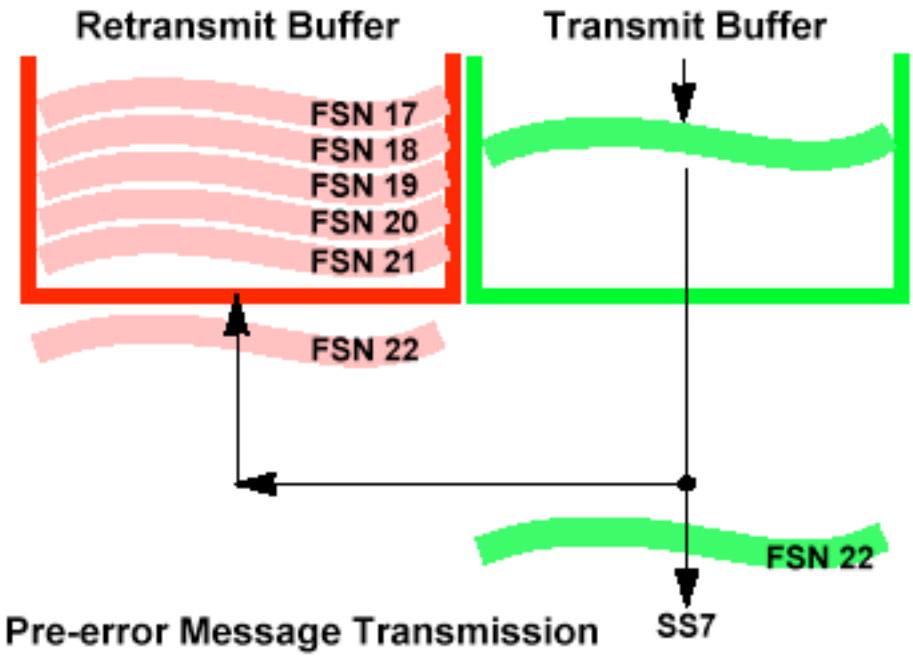

Figura 47: Transmisión de paquetes en el sistema SS7

Vamos a suponer que el mensaje con FSN 19 no fue recibido correctamente. La parte receptora MTP tomará el identificador (FSN) del último mensaje recibido correctamente, en este caso 18, y lo colocará en el BSN del paquete que será devuelto a la parte transmisora. También se asegurara de que el BIB se establezca como opuesto al FIB. Esto hecho sirve para requerir la retransmisión del paquete. Cuando el paquete es recibido en la parte transmisora la diferencia entre el FIB y el BIB provoca una serie de acciones:

- La transmisión se detiene.
- Los mensajes, comenzando por el 19, son retransmitidos en secuencia.
- Los mensajes en el buffer anteriores al 19 son borrados.
- La transmisión comienza de nuevo.

Usando este procedimiento, la parte receptora garantiza la integridad de los mensajes que recibe, y la parte transmisora puede limpiar el buffer de retransmisión, previniendo la congestión.

La parte receptora debe retornar respuestas incluso cuando recibe los mensajes de forma adecuada. Esto se hace de forma similar a cuando se envía una petición de copia. Se transmite un paquete de Link Status información, que contiene el FSN del ultimo mensaje recibido correctamente, pero esta vez el BIB tiene el mismo valor que el FIB. Esto es visto desde la parte transmisora como un ack positivo, permitiendo así la destrucción de todas las copias, incluyendo la del FSN indicado en el paquete.

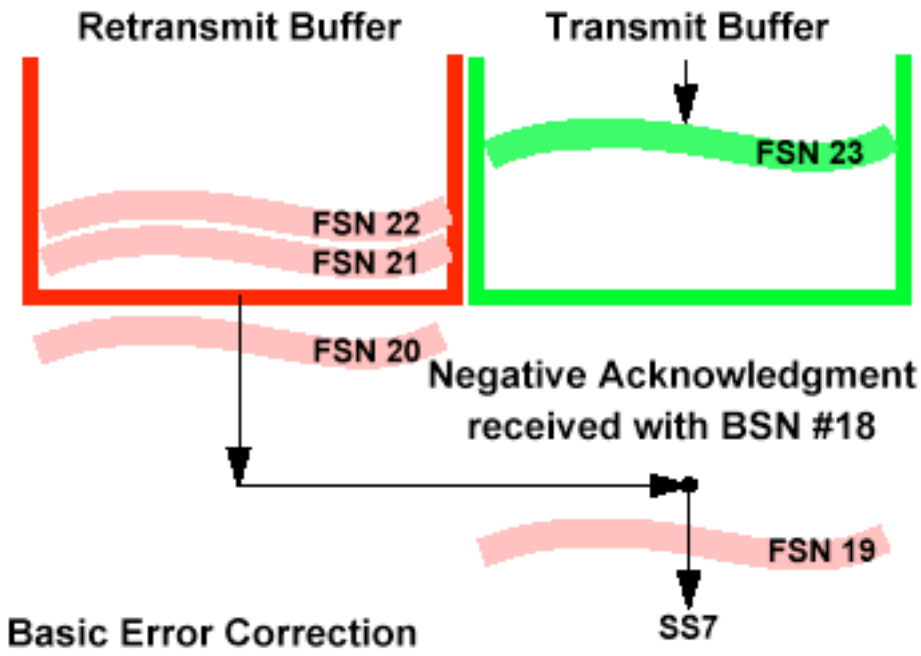

Figura 48: Proceso de retransmisión de copia

Todo este proceso de transmisión se realiza sobre los links. Si un link fallase, o cayera, no se recibirían ni los acks positivos ni los acks negativos, por lo que el proceso descrito anteriormente no tendría ninguna utilidad. En este caso, se necesitarían otros mecanismos para que no se produjera congestión en los buffers. Uno de estos mecanismos consiste en un temporizador, denominado T7, que esta esperando las respuestas, tanto positivas como negativas de cada paquete. Si el temporizador vence sin recibir el ack, la transmisión debería ser detenida en ese link. Otro mecanismo del que dispone la MTP son las unidades de señalización **Fill In Signal Unit**, a través de las cuales se puede detectar directamente que no existen datos sobre el link.

Otros mecanismos de detección de errores

Número de octetos

La longitud total de los campos de una unidad de señalización es siempre un número par de octetos. Esto significa que el numero total de bits del paquete dividido por 8 debe dar como resto 0. Si el resultado es distinto de 0, el paquete se considera erróneo y es descartado.

Campo CRC

Este campo contiene un código (Cyclic Redundancy Code) que es una representación del numero total de bits transmitidos en la unidad de señalización o paquete, y que es colocado por la parte transmisora. En la parte receptora, este código CRC se recalcula a partir de la información contenida en cada uno de los paquetes, y si no coincide con el recibido, el paquete es incorrecto. En caso contrario es correcto.

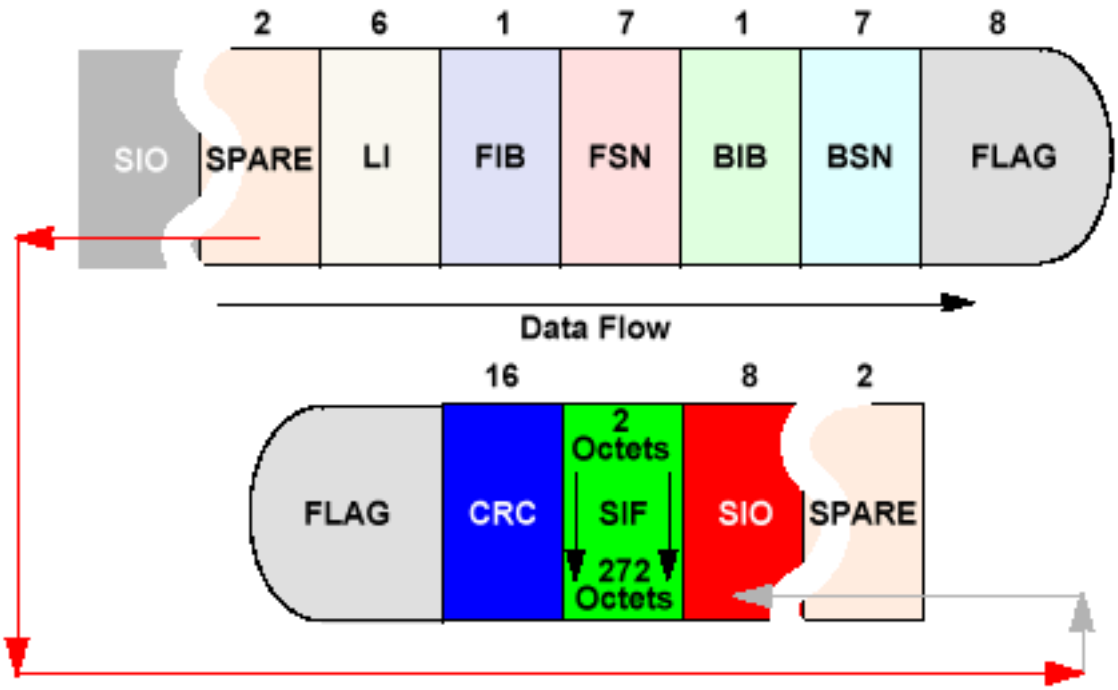

Figura 49: Campos CRC, SIF y SIO de un paquete MSU

En la figura podemos ver los campos CRC, SIF y SIO, que son propios de la unidad de señalización MSU. El SIF, que no ha sido mencionado hasta ahora, es el que contiene la información en si.

AERM

El MTP nivel 2 no solo realiza un seguimiento de la información transmitida, sino también de los links sobre los que ésta es transmitida. Generalmente, se emplean dos procedimientos para determinar el buen funcionamiento de los enlaces.

El primero se conoce como *Alignment*. Se usa cuando el link se da de alta por primera vez, y en cada ocasión en que éste se da de baja y es reactivado. Durante el proceso, la MTP usa un temporizador llamado *Aligment Error Rate Monitor*, que determina el periodo de análisis del link. Este periodo recibe el nombre de aligment normal o aligment de emergencia, en función del valor que se escoja para el. Los valores típicos se muestran en la siguiente figura.

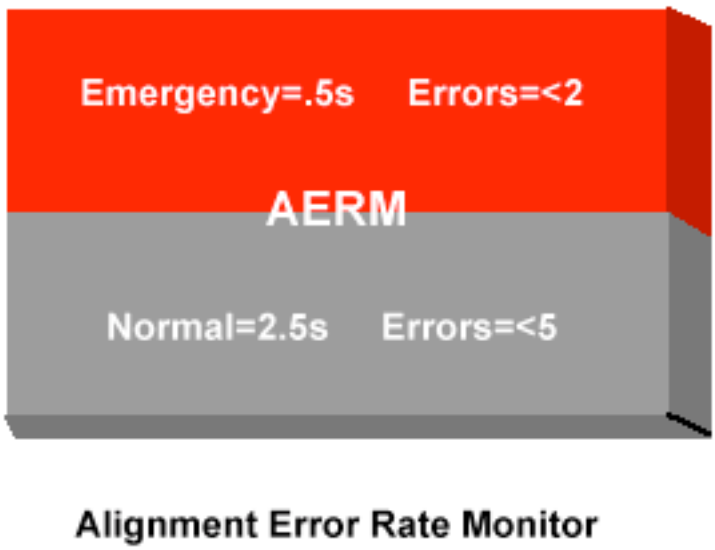

Figura 50: Valores del AERM para 64Kbps

Poco después del establecimiento de la conexión en el link, la MTP establece el AERM, y durante este periodo se envían Fill In Signal Units para monitorizar el estado del enlace.

Si la configuración del AERM fue establecida en modo emergencia, los FISU son enviados durante 0.5 segundos. Los paquetes FISU no contienen datos, es decir, si quitamos el campo SIO y SIF de un MSU tenemos un paquete FISU. Durante este periodo, un error simple será ignorado. Sin embargo, si ocurren dos errores, se considerará que el link no es aceptable y el proceso de aligment empezará de nuevo.

Durante el periodo de aligment, el MTP de nivel 2 esta también reportando sus actuaciones sobre el link. Esto lo realiza a través de los paquetes LSSU (Link Status Signal

Unit). Este paquete dispone de los mismos campos que un MSU, excepto el SIO y el SIF, que son sustituidos por un campo de uno o dos bytes donde se indica la actuación que se está realizando sobre el link y su estado. Así, una vez establecido el AERM, se envían LSSU's que contendrán por una parte "N" (Normal) o "E" (Emergency) en relación al aligment escogido, y por otra parte "O" (Out of Aligment) o "OS" (Out of Service), entre otras posibilidades, en relación al estado del link. Si cualquier nodo de la red recibe un "OS", sabrá que no debe usar ese link en concreto.

Si la configuración se establece a normal aligment, los FISU son transmitidos durante 2.5 segundos. Durante este tiempo, 4 errores serán ignorados. Sin embargo, si se detectan 5 errores, el link se considera no válido y el proceso de alineación empieza de nuevo, hasta que en alguna ocasión finalice de forma positiva.

SUERM

Hasta ahora hemos descrito como el MTP controla el estado del link antes de empezar a transmitir sobre él. Sin embargo, el MTP también debe controlar el link durante la transmisión.

La monitorizacion durante la transmisión se realiza usando lo que se denomina Signal Unit Error Rate Monitor (SUERM). Este monitor es un simple contador, que se incrementa con cada error que se produce. Si llega a 64, el link se deja fuera de servicio y debe ser realineado, es decir, se procede a realizar un proceso de alignment sobre el.

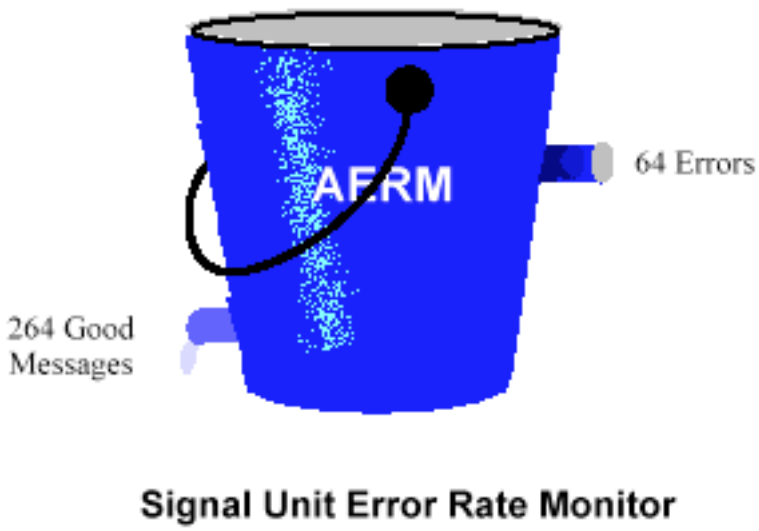

Figura 51: Contador SAERM

No obstante, si queremos realizar un control sobre la tasa de error (errores/s) durante la transmisión, la simple utilización de un contador no es suficiente. Por ello, lo que se hace exactamente, es aumentar el contador cada vez que se recibe un paquete erróneo y decrementarlo cada vez que llegan 256 paquetes no erróneos. De esta forma se introduce el concepto de ratio dentro de la técnica usada.

MTP 3

Unidades de señalización

Antes de pasar a analizar el MTP de nivel 3, vamos a describir algo más los tres tipos de signal units utilizadas en el sistema de señalización SS7.

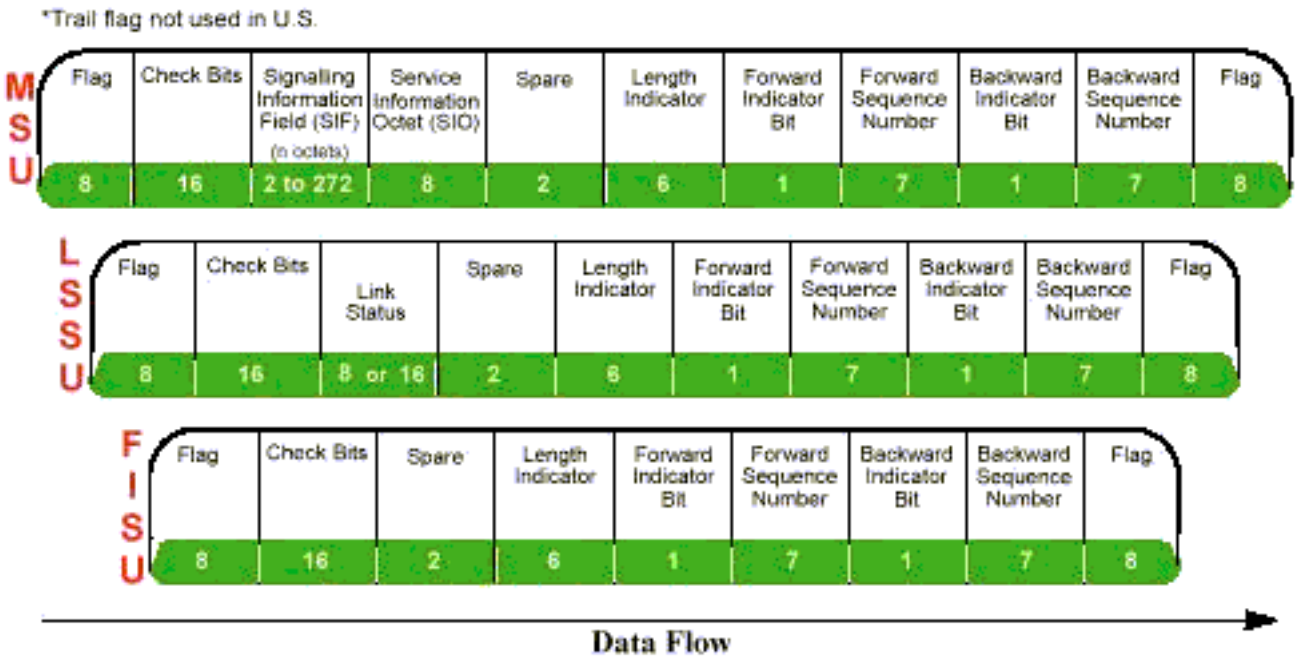

Figura 52: Unidades de señalización básicas

EL **Message Signal Unit** (MSU) contiene un campo llamado Service Information (SIO), que contiene información que identifica el tipo de datos que transporta el paquete, como datos ISUP o TCAP, por ejemplo. Además, este campo, en determinadas ocasiones, transporta tambien información en relación a:

- Monitorización de red.
- Prioridad del paquete.

La información de señalización en si, esta ubicada en el campo Signaling Information Field (SIF), que puede ser considerado como el campo de datos.

El **Link Status Signal Unit** (LSSU) dispone de un campo simple, en lugar del SIF y del SIO, que se denomina Link Status Field. En este campo, de uno o dos bytes, se transmite información sobre la congestión, los estados de los alignments, etc.

El **Fill In Signal Unit** (FISU) no tiene ningún campo en lugar del SIF o SIO. Este paquete se usa como relleno entre la transmisión de los MSU y los LSSU, con la intención de que el MTP receptor vea siempre actividad sobre el link.

La funcionalidad del MTP nivel 3 se divide en dos grupos, **S**ignalling **M**essage **H**andling (SMH) y **S**ignalling **N**etwork **M**anagement (SNM).

- SMH: Se encarga de controlar el direccionamiento de los paquetes que envía y recibe.
- SNM: Se encarga de manejar el tráfico, los links y las rutas disponibles.

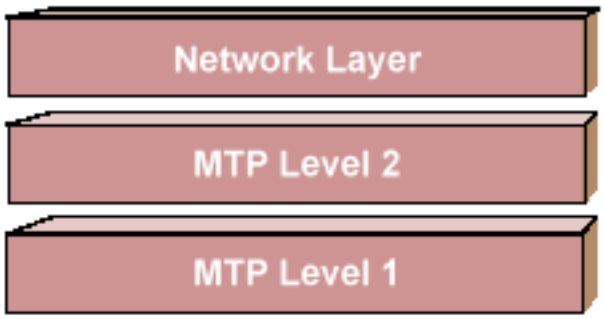

Figura 53: MTP de nivel 3

El MTP nivel 3 recibe continuamente información (desde el MTP de nivel 2 o desde otros nodos remotos de la red) sobre el estado de los links, las rutas y los destinos. La mayor parte del trabajo del nivel 3 consiste en hacer uso de esta información para controlar el tráfico sobre los recursos de los que el dispone. Esto significa, por ejemplo, que cuando un link esta congestionado, el direccionará el trafico de ese link a otro que no lo esté.

Control del tráfico

El MTP de nivel 3 controla si sus recursos están disponibles o no. Hay muchas razones por las que un link puede estar no disponible. Un link que ha fallado, que esta congestionado o bloqueado, o que sencillamente está desactivado, es visto por el nivel 3 como un link no disponible. Como se verá posteriormente, el MTP de nivel 3, en circunstancias normales, esta generando un código (Signalling Link Selection, **SLS**) que se usa para informar al resto de nodos de la red los links operativos de los que dispone el nodo en cuestión.

Cuando recibe una indicación, por parte del MTP de nivel 2, de que un link esta no disponible, cambia el SLS que estaba enviando, y simultáneamente, la salida de los nuevos mensajes hacia otro link disponible (recuérdese que en la red SS7 los links entre nodos están duplicados). Este proceso recibe el nombre de **Changeover**. Cuando la condición que produjo el Changeover desaparece, el MTP debe usar los links disponibles de forma eficiente, por ello redirige cierta cantidad de tráfico al link restaurado. Este proceso recibe el nombre de **Changeback.**

Control de rutas

Además de controlar el tráfico sobre los links, el MTP de nivel 3 debe controlar las rutas de encaminamiento hacia nodos exteriores.

Puede ser que el tráfico dirigido a un destino remoto no pueda llegar a éste porque una ruta propia (2 links redundantes que unen un nodo con otro) esté no disponible. Cuando esto ocurre, la tabla de enrutamiento es consultada para ver si existe una ruta alternativa hacia el mismo destino que esté disponible. Si esto es así, la ruta saliente es cambiada en un proceso denominado **Forced Rerouting**. Cuando la ruta original está disponible de nuevo, el MTP de nivel 3 vuelve a cambiar la ruta de los mensajes en un proceso llamado **Controlled Rerouting**.

Control de destinos

El MTP puede recibir información desde la red indicando que algún destino esta no disponible. Esto fuerza al MTP a consultar la tabla de enrutamiento para ver si existen destinos alternativos, y si este fuera el caso, se redirigiría el tráfico a estos.

Se debe observar que el MTP nivel 3 restablece el trafico sobre el link o ruta original que tenia configurada, siempre que la condición que provoco el cambio desaparezca. Toda esta actividad de redireccionamiento de tráfico en respuesta a las condiciones de los links o de la red se encuentra dentro del grupo de funcionalidades SNM (**S**ignalling **N**etwork **M**anagement).

Otra tarea en relación con el SNM de la que el MTP nivel 3 es responsable, es la denominada MTP Restart. Si un nodo perdiera momentáneamente todo su acceso a la red, se deberían tener en cuenta ciertas consideraciones especiales a la hora de restaurarlo, ya que las condiciones de la red durante su ausencia podrían haber cambiado. Por ejemplo, los nodos remotos que estaban disponibles en el instante de la caída podrían no estarlo ahora. Todo el proceso necesario para reactivar un nodo es lo que se conoce como MTP Restart.

El nodo que se está reactivando necesita un tiempo para restaurar su información de red. Sin embargo, los centros que envían mensajes a dicho nodo lo verán, durante su periodo de reactivación, como disponible, y empezarán a enviar mensajes inmediatamente, cuando dicho nodo todavía no es capaz de aceptar tráfico. El nodo que reentra en la red debe prevenir esta situación, y además, debe asegurarse de que un número adecuado de sus recursos están disponibles antes de invitar al resto de nodos a la transmisión de tráfico.

Para realizar esto, el primer mensaje que enviará a los nodos que transmiten será, precisamente, el de no transmitir mensajes. Esto se hace usando un Traffic Restart Waiting Message seguido por un Traffic Restart Allowed, que se envía cuando el nodo ya ha actualizado toda su información de red y es capaz de aceptar tráfico. Otra consideración a tener en cuenta sería la de transmitir el tráfico que se pudiera tener almacenado antes de la caída, cosa que debería realizarse en primera instancia. En general, la reactivación de un nodo es tan sencilla como lo descrito anteriormente, pero dependiendo del tipo de nodo, este proceso puede implicar un conjunto considerable de operaciones.

Funcionalidades SMH

EL otro conjunto de funcionalidades de la que se ocupa el MTP de nivel 3 es el Signalling Message Handling (SMH), que a su vez se divide en Message Discrimination y Message Distribution.

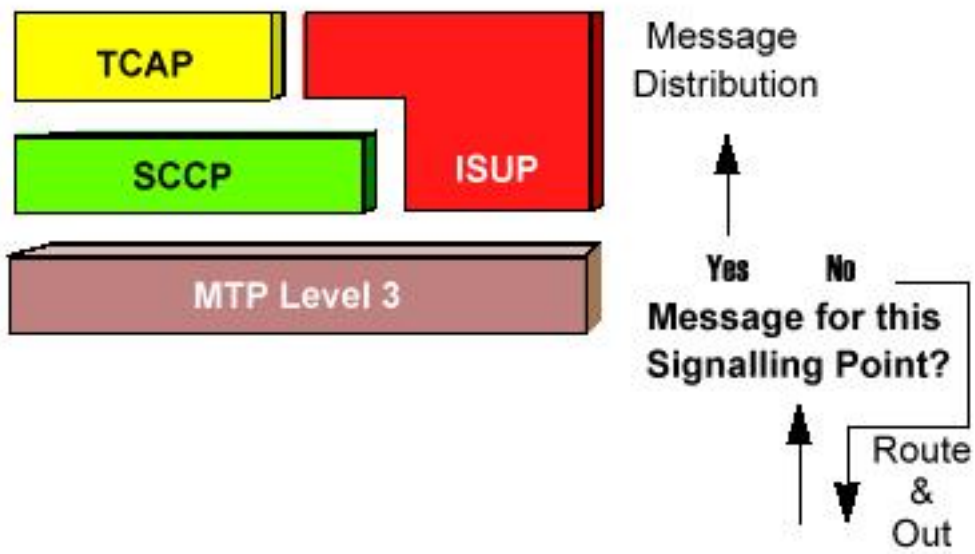

Figura 54: Message Discrimination

La figura muestra el proceso de Message Discrimination. El mensaje es examinado en primera instancia, para determinar si esta dirigido a este nodo (Destination Point Code). Si no es así, la regla es “enrutar fuera”. Esta es una funcionalidad muy invocada en un STP, ya que este tipo de nodo soporta la mayor responsabilidad del enrutamiento dentro de la red. Para otros nodos, dicha función esta limitada o incluso es inexsistente. Ciertos nodos podrían ser requeridos para hacer algún tipo de enrutamiento limitado, particularmente enrutamiento intra-red usando F links, pero en la mayoría de los casos el nodo no tiene especificaciones de enrutamiento, y sencillamente se deshace del mensaje que no esta direccionado a él.

Si el mensaje llega al nodo correcto, entonces se produce el Message Distribution. La mayoría de las capas no tienen más función que pasar el mensaje a la capa superior (User Part). En el MTP 3 sin embargo, se debe realizar una selección de los mensajes. Esto es así porque el

nivel 4 puede consistir en distintas User Parts. La SCCP y la ISUP son las frecuentes, pero puede existir una TUP (**Telephone Users Part**) o incluso una DUP (**Data Users Part**). Los datos encontrados en el octeto SIO (Service Information Octet) del MSU (message Signal Unit) ayudan al nivel 3 a tomar esta decisión.

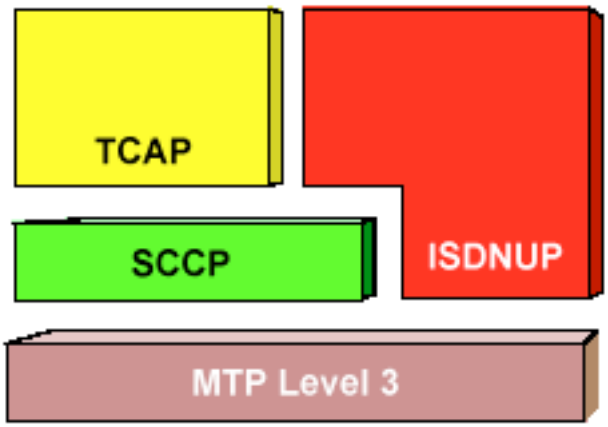

Figura 55: Partes de Usuario

Antes de movernos a los otros niveles, debemos aclarar el termino Users Parts. Cada capa, a través de su conjunto de funcionalidades, ofrece servicios a las otras capas. La capa 3, por ejemplo, usa los servicios de la capa 2 para estar informada del estado de los links, linksets y rutas, y a la vez, ofrece sus servicios a la capa 4.

Un primer ejemplo, de este hecho se basa en el uso del Signalling Link Selection Code, que proporciona la capa 3. Este código es usado por el nivel 3 para indicar a las capas inferiores el link sobre el cual cada paquete debe ser enviado. Así, el nivel 3 inserta dicho código en cada paquete para que cada uno sea mandado sobre un link diferente y el trafico se distribuya sobre todos los links disponibles. En el estándar ANSI, por ejemplo, el bit más significativo del código Signalling Link Selection Code se rota para cambiar la selección del link.

Parte de Usuario SCCP-Signalling Connection Control Part Layer

Mencionaremos en este punto el SCCP, aunque posteriormente se profundizará en sus funcionalidades. El SCCP provee servicios de distinto tipo, y dos de estos requieren que los datos sean transmitidos en secuencia. Si los datos son distribuidos sobre diferentes links, la aplicación en el nodo remoto puede no ver los mensajes en el mismo orden en el que fueron transmitidos. La razón de esto radica en que cada link tiene su propia cola de mensajes.

En este caso, la única forma de garantizar que los paquetes se reciban en orden es haciendo uso del SLS de la capa MTP. Así, cuando se requiere, la capa MTP 3 congela el SLS durante el periodo de la transmisión, para poder mandar todos los mensajes sobre el mismo

link repetidamente. De esta forma, el nivel 3 asegura que todos los mensajes llegaran en secuencia al nodo destino y no fuera de orden.

Parte de Usuario ISUP-Integrated Services User Part

Introducción

La ISUP ofrece dos grupos de servicios, conocidos como Básico y Suplementario. Los servicios básicos son los encargados del establecimiento, mantenimiento y finalización de una llamada normal, mientras que los servicios suplementarios se encargan de agregar funcionalidades "suplementarias" al proceso de la llamada, como podrían ser los desvíos, la llamada en espera o la llamada a tres.

Por otra parte la funcionalidad ISUP puede ser dividida en tres categorías, **Signalling Procedure Control** (SPRC), **Circuit Supervision Control** (CSC), **Call Processing Control** (CPC).

El SPRC se comunica directamente con la MTP, y además ofrece soporte para el CSC y el CPC. La parte de la ISUP que trata la conexión de los circuitos de voz dentro de la parte de conmutación se conoce como Call Control Aplication.

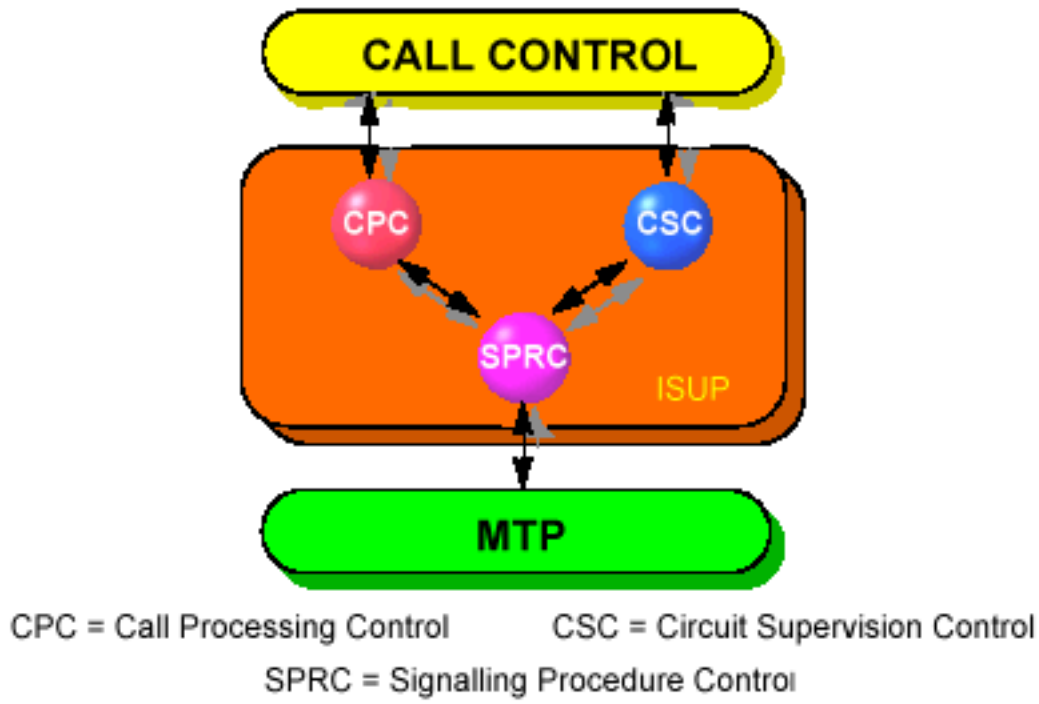

Figura 56: User part ISUP

Aunque el termino estandarizado para esta parte de usuario es realmente ISDNUP (Integrated Services User Part), normalmente se utiliza la denominación ISUP. Esto es así porque el estándar hace referencia a todas las porciones de la PSTN, mientras que el termino ISUP se usa para hacer referencia solamente a la información de señalización que se precisa para establecer las conexiones de voz.

Como hemos dicho, la ISUP maneja toda la información de señalización necesaria para establecer y mantener las conexiones de una llamada. Cada conmutador obtiene la información del conmutador previo hasta que la conexión entre los usuarios llega a establecerse. Así, los mensajes ISUP se mueven a través de la red SS7 de unos nodos de conmutación a otros, de forma paralela a las conexiones de voz que están siendo establecidas.

Realización de la llamada

El proceso empieza con el análisis de los dígitos marcados en el conmutador origen. Posteriormente, se consulta la tabla de enrutamineto para determinar cual es el conmutador apropiado al que se dirigirá la llamada. Una vez determinado el siguiente conmutador, se selecciona una conexión a dicho conmutador, a la cual se conectará la línea del llamante. Esto ocurre a nivel de conexiones de voz.

El paso paralelo, a nivel de SS7, es enviar un mensaje de señalización al siguiente conmutador, indicándole cual de sus conexiones va a ser usada, y además, transmitiéndole toda la información necesaria para que sea capaz de seleccionar la siguiente conexión. Para este objetivo, se usa un mensaje ISUP denominado **IAM** (Initial Address Message). Este mensaje, como hemos dicho, contiene toda la información necesaria para que el conmutador sea capaz de consultar sus tablas y seleccionar la siguiente conexión que resulte más adecuada para la conexión del origen y el destino. El nodo que ha enviado el IAM recibirá un mensaje confirmando que el conmutador que lo recibió esta ahora en posesión de toda la información de direccionamiento necesaria. Este mensaje se llama **ACM** (Address Complete Message).

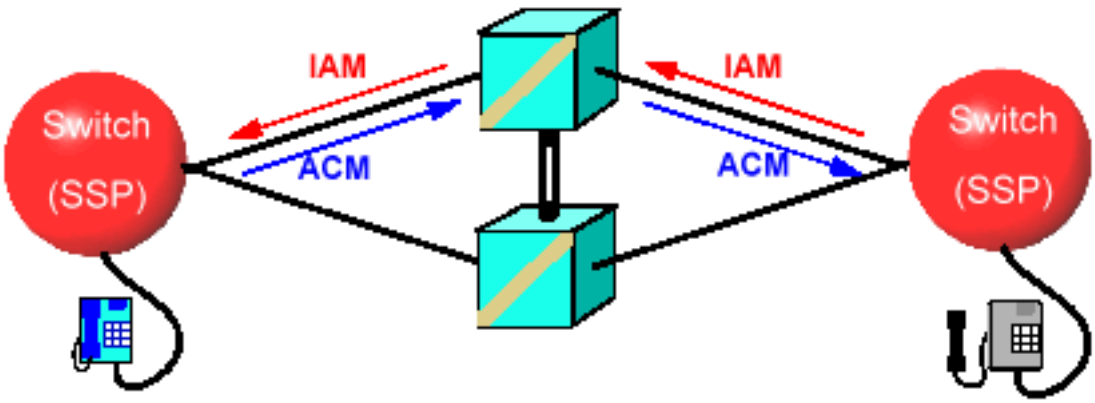

Figura 57: Proceso de establecimiento del circuito de voz

Cuando el nodo que esta conectado al destino reciba el IAM y determine que el esta conectado directamente al destino, comprobará si el interfaz de línea del usuario esta “on hook”. En tal caso, enviará una señal para que el teléfono destino empiece a sonar. Al mismo tiempo se usará el sistema SS7 para enviar un ACM hacia atrás, que en este caso provocará el “ringback” en el teléfono llamante. Si el llamado tiene su línea ocupada, se procede de forma similar, pero devolviendo la señal de ocupado.

Anteriormente al sistema SS7, esta señales de ocupado o de marcado no se transmitían en forma de paquetes digitales, sino que se usaba el circuito de voz establecido para enviar dichas señales en forma analógica, cosa que provocaba un desperdicio en el uso de los conmutadores. Con la aparición del sistema de señalización SS7, este tipo de señales desaparecieron del circuito de voz, aunque no totalmente, porque en la conexión final entre la central local y el teléfono destino la línea sigue siendo usada para transmitir señalización y voz, ya que pocos hogares disponen hoy en día de terminales digitales.

Hoy en día, los conmutadores pueden hacer conexiones muy rápidamente, y, aunque es mucho menor que hace algunos años, el tiempo para realizarla no es cero. Cuando los circuitos de voz transmitían también la información de señalización, existía un tiempo de conexión de cada conmutador con el siguiente, cosa que ralentizaba el establecimiento de la llamada.

Actualmente, como la señalización no ocupa el circuito de voz, no se precisan establecer conexiones para transmitirla, sino que sencillamente se reservan como ocupadas. Si la respuesta desde el conmutador final indica que el teléfono esta ocupado, este circuito reservado queda instantáneamente liberado, sin perdidas de tiempo en conexiones y desconexiones. Si el teléfono llamante es descolgado, las conexiones reservadas se hacen efectivas casi simultáneamente, con lo que no existen tiempos aditivos de conexión.

Una vez que el teléfono esta sonando, no existe, durante un tiempo, información de señalización siendo intercambiada. Cuando el teléfono es descolgado, el conmutador final envía un **ANM** (Answer Message) hacia la red SS7. De esta forma se notifica a cada conmutador que el circuito completo debe existir ahora. Así, todo conmutador que no haya realizado todavía efectiva la conexión, deberá hacerla ahora.

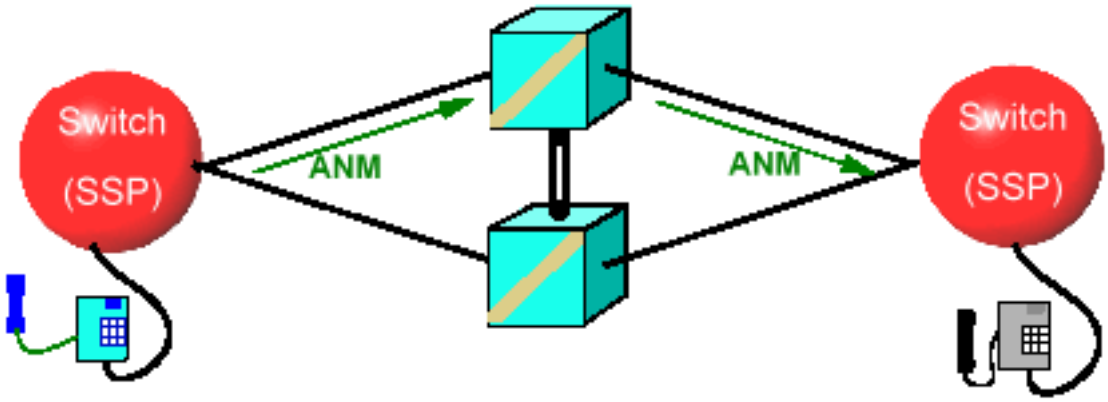

Figura 58: Establecimiento de la llamada

Si suponemos que se realiza una llamada normal, y no tipos especiales de llamada como conferencias, etc.., la conversación tendrá lugar y los conmutadores sencillamente mantendrán las conexiones, hasta que uno de los dos usuarios cuelgue.

Una vez que el nodo final percibe el cuelgue, envía un **REL** (Release Message) al conmutador previo dentro del circuito establecido. A medida que cada conmutador va recibiendo el REL, libera la conexión del circuito que tenia establecida. A su vez, el nodo que recibe el REL, devuelve un **RLC** (Release Complete) hacia el conmutador del que recibió el REL, confirmando que ha recibido el mensaje de desconexión y que esta se ha producido de forma satisfactoria.

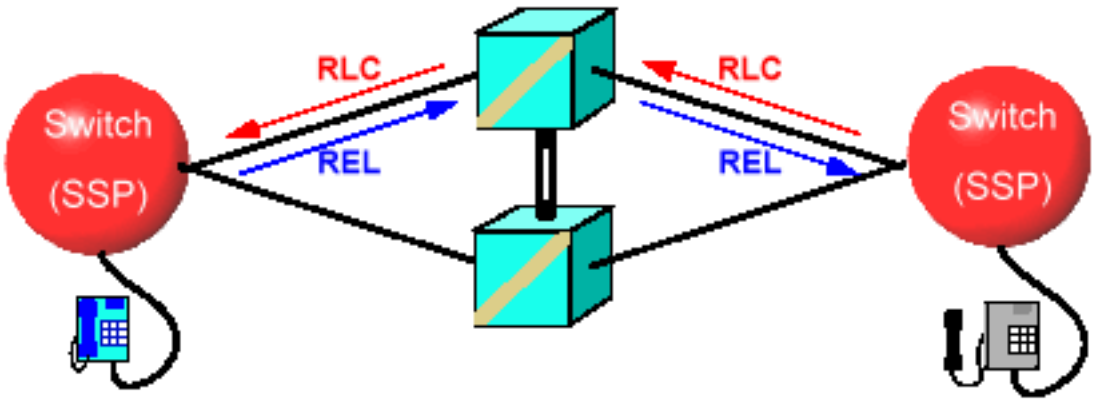

Figura 59: Proceso de liberación de una llamada

Cada conmutador que envía un REL, establece un temporizador de espera, que se desactiva cuando recibe el RLC. Si el temporizador vence sin que se haya recibido un RLC, cabe la posibilidad de que el conmutador a quien fue enviado el mensaje no lo haya recibido y mantenga todavía su conexión. Si esto ocurre, se alertará a la aplicación de control de la existencia de un problema potencial para que esta tome las medidas necesarias.

Otro temporizador importante es el que establece el primer nodo del circuito de voz. El temporizador se establece cuando este nodo envía el mensaje ANM, y vence con la recepción del REL. De esta forma se calcula la duración de la llamada y en función de ésto su coste.

Servicios SCCP - Signalling Connection Control Part Layer

Introducción

Como su propio nombre indica, la SCCP se hace cargo de las conexiones dentro de la red SS7. Estas conexiones no son similares a las del circuito de voz, ya que en este caso se trata de una red de conmutación de paquetes digitales. En general, la SCCP se encarga del control de las reglas que rigen la transmisión de datos en una red de este tipo, intentando proporcionar mayores funcionalidades a la transmisión de datos de las que dispone la MTP de nivel 3, especialmente en el aspecto del direccionamiento.

El MTP de cualquier nodo solo considera a que nodo adyacente debe enviar el mensaje, independientemente de que éste sea el destino final o no. Por ello, solo trabaja con los Signalling Point Codes de sus nodos adyacentes.

Por su parte, el SCCP considera la transmisión del mensaje en el sentido global, desde el origen hasta el destino final. Así pues, el SCCP trabaja con los SPC de todos los nodos de la red, y no solo con los de sus adyacentes.

Además, el SCCP también se encarga de tratar el problema del subdireccionamiento. Por ejemplo, en una localización dada, con un SPC determinado, pueden coexistir varias aplicaciones o servicios. Si solo usamos el SPC como información de direccionamiento, no existiría la posibilidad de saber que servicio estamos requiriendo. El SCCP resuelve este problema usando identificadores de servicios, conocidos como SSN.

El SSN esta representado en el paquete de tipo Message Signal Unit usando solamente un byte de datos. Por esta razón, el rango será un valor de 0 a 255. Algunos de los valores bajos suelen están reservados, para servicios estándares propios de la red.

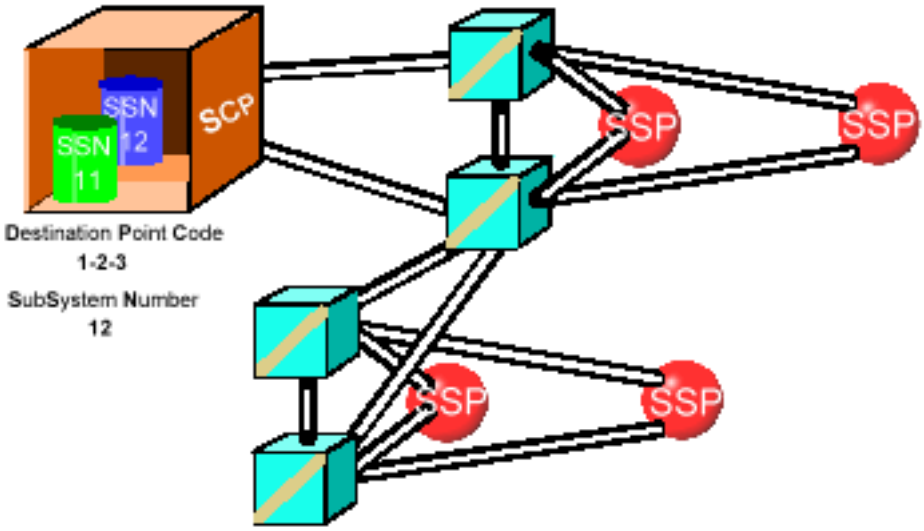

Figura 60: Direccionamiento y subdireccionamiento

Uso del Global Title

Además del Signallng Point Code, a veces también llamado Destination Point Code y del SSN, el SCCP provee otros medios de direccionamiento como el Global Title (GT).

El GT es, esencialmente, un alias de direccionamiento. Por ejemplo, para hacer una petición a una base de datos que proporciona la traducción de los numeros 900, el conmutador que usa el GT no necesita conocer donde esta la base de datos ni que SSN puede tener. En vez de esto, precisa simplemente conocer una localización (generalmente se trata de un STP), que sabe donde puede ser encontrada la información.
El proceso es el siguiente:

- El conmutador prepara un mensaje codificado como GT. Esencialmente, la codificación identifica el tipo de información que se requiere y además incluye los datos necesarios para que esta información pueda ser obtenida. Por ejemplo, cuando alguien llama a un numero 900, el conmutador codifica un mensaje como global title, indicando que se necesita una traducción del numero a un numero normal, e incluyendo los dígitos marcados. El conmutador envía este mensaje a un STP, que aparecerá en su tabla de enrutamiento como la localización a la que se deben enviar las peticiones de traducción codificadas como GT.

- Cuando el STP recibe el mensaje, decodifica el GT, y a partir de sus tablas es capaz de encontrar el SPC y el SSN del destino adecuado. Una vez obtenida esta información el STP envía la petición de traducción al SPC determinado.

- El SPC realiza la traducción y devuelve la respuesta al STP, que a su vez reenvía el mensaje al conmutador origen

EL uso del GT ofrece numerosas ventajas. Por una parte, sin el GT, cada conmutador en el mundo debería tener actualizada su información de enrutamiento para tener acceso a cualquier nuevo servicio y a cualquier nuevo nodo. Usando el GT, solo las localizaciones STP encargadas de recibir este tipo de peticiones necesitan tener actualizadas sus entradas en las tablas. Y así, cada conmutador que use GT's tiene inmediatamente acceso transparente a todos los nuevos servicios.

Además, si en un momento dado el SCP destino para una determinada petición cae o es imposible acceder a el, el STP cambiará su entrada por la de otro SCP que realice las funciones de backup del anterior. Así, el SCP origen recibirá la respuesta correcta, sin tener que haberse preocupado de todo el proceso intermedio. Esto permite una sencilla adaptación dinámica (solo los STP's que reciben GT se ven afectados) a las condiciones de la red.

Otra ventaja es que usando GT's, una subred podría mantener ocultos determinados servicios para el resto de la red, teniendo la oportunidad de trabajar con servicios propietarios o de pago.

Bases de datos redundantes

La figura ilustra la utilización de bases de datos redundantes dentro de la red. Aquí, las bases de datos están en diferentes localizaciones físicas y el subsistema dado para cada una de ellas es el mismo. Otro forma de obtener redundancia seria colocar la BD y su backup en la misma localización y usar diferentes SSN para acceder a ellas. Esto muestra una de las misiones más importantes de la SCCP, el agrupamiento de funcionalidades en determinados nodos, liberando al resto de carga añadida.

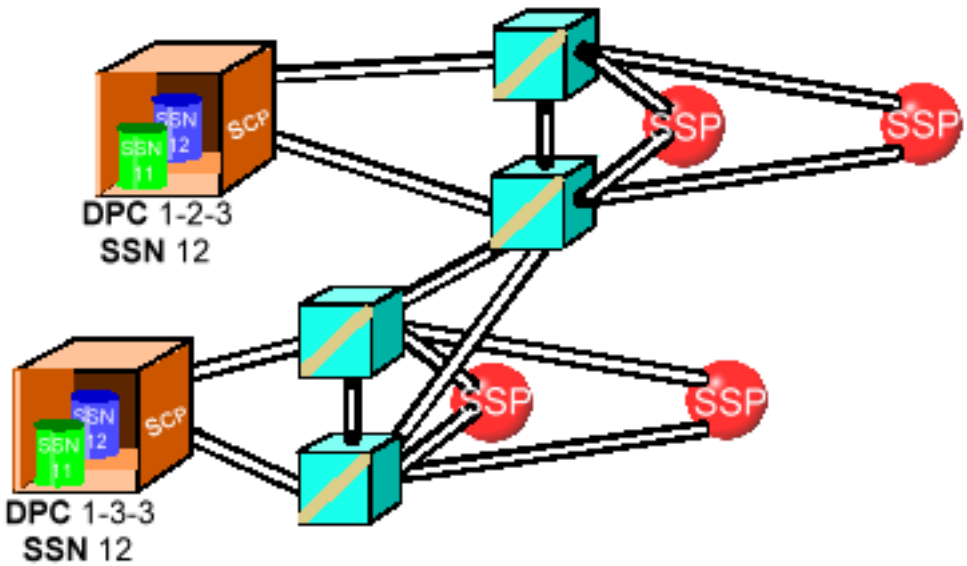

Figura 61: Bases de datos redundantes

El manejo de las bases de datos redundantes es otra tarea implementada por el SCCP. El proceso empieza cuando un servicio programa reiniciar una de sus bases de datos por cualquier razón de mantenimiento. Dicha base de datos usará los mensajes SCCP para informar a su backup de este proceso. Si la base de datos de backup, esta preparada para abastecer las peticiones que ahora le serán dirigidas, devuelve un ack positivo, y el proceso de reinicio de la primera base de datos comienza.

Obviamente, ciertas localizaciones de la red necesitan estar informadas del proceso de reinicio, ya que dicha información es imprescindible para reenrutar las peticiones mientras la base de datos principal esta no disponible. Dichos nodos se conocen como **C**oncerned **P**oint **C**odes (**CPC**). El SCCP es el encargado de informarlas, mediante un mensaje **SSP** (**S**ub**S**ystem **P**rohibited).

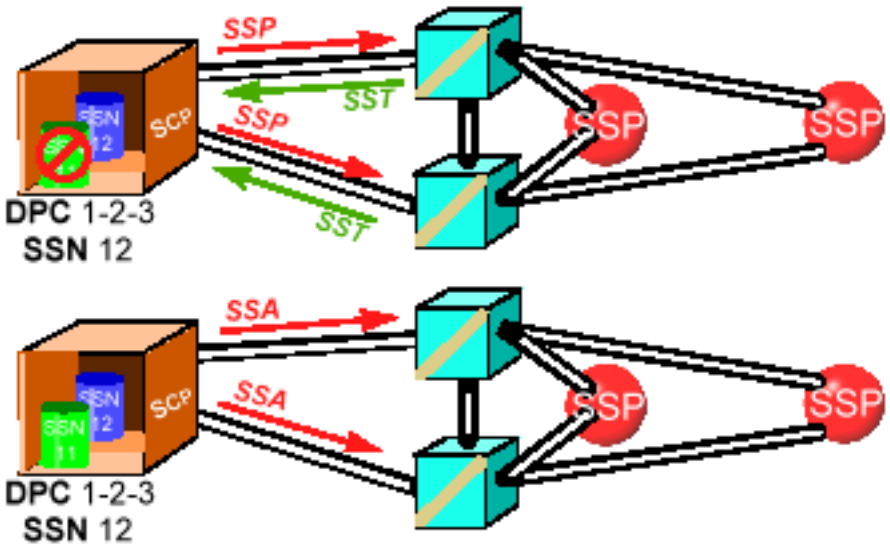

Figura 62: Mantenimiento de bases de datos

El SCCP recibe como respuesta a este mensaje un **SST** (**S**ubsystem **S**tatus **T**est). Una vez recibido el SST, se tiene la certeza de que los CPC conocen la situación actual, y se completa el proceso de shutdown. Durante el tiempo que dure éste, las peticiones serán enviadas a la base de datos de backup, y además no se dejará de enviar SST's a la base de datos original para chequear su estado.

Esta transmisión continua de SST's finaliza cuando se recibe un **SSA** (**S**ub**S**ystem **A**llowed) por parte de la SCCP que controla la base de datos, cosa que se produce cuando el proceso de reinicio ha terminado. Si el SCCP recibe como respuesta al SSA un SST esto significa que el SSA no fue recibido, así que se envían SSA hasta que no se recibe un SST. Una vez completado el proceso las peticiones volverán a ser redirigidas a la base de datos principal.

TCAP - Transaction Capabilities Aplcation Part

Pasamos ahora a estudiar una Parte de Aplicación y no una Parte de Usuario, es decir, nos encontramos en la parte más alta del modelo de capas, donde no existe obligación de ofrecer funcionalidad a un nivel superior.

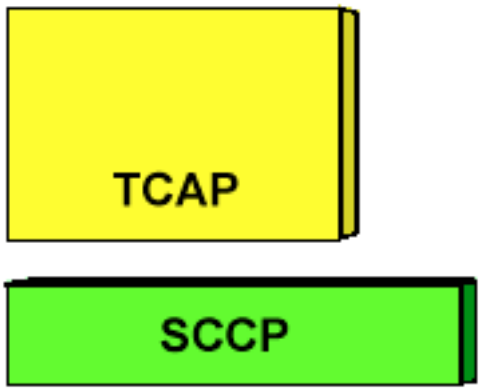

Figura 63: Parte de Aplicación TCAP

La funcionalidad de TCAP es adecuar y presentar los datos en distintos formatos estadarizados para que estos puedan ser usados y entendidos por los distintos servicios en un entorno multivendedor.

TCAP y SCCP van juntos. El SCCP provee el SSN necesario, controla los direccionamientos, realiza tareas de segmentación cuando el mensaje es demasiado largo, y maneja todas las consideraciones sobre el uso de los GT's; además de ofrecer un transporte para los mensajes TCAP, que dentro de la MSU se encuentran en el campo SIF. Por su parte, TCAP es capaz de invocar numerosas acciones, tanto a nivel de bases de datos como de conmutación.

A su vez, existe otra parte de aplicación, el Mobile Application Part (GSM, IS41-C), que va encasulada en los mensajes TCAP, y que se considera como una extensión de éstos.

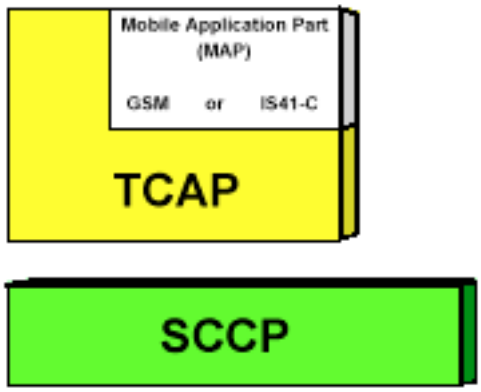

Figura 64: Parte de Aplicación MAP

Cuando una petición TCAP es enviada, se le añade un identificador de transacción. Esto se realiza porque el conmutador puede estar recibiendo y enviando peticiones sin un orden determinado. El identificador de la transacción también se copia en las respuestas, permitiendo así correlar cada petición con su respuesta.

El mensaje TCAP, a su vez, se divide en porciones mas simples, como la parte de transacción, la parte de componente y la porción de diálogo, pero toda su estructura se verá con más detalle en la siguiente sección.

Protocolos TCAP y MAP

Introducción

En esta parte del proyecto vamos a describir el desarrollo de una sencilla librería que utilice la capa de protocolos del sistema de señalización SS7. Concretamente, nos centraremos en los protocolos TCAP y MAP, y en la integración de dichos protocolos con las capas inferiores.

La librería en si, tendrá la capacidad de realizar operaciones con una base de datos básica dentro del sistema GSM, el HLR. La comunicación con dicha base de datos es muy importante para la mayoría de los servicios de valor añadido que se desarrollan en la red inteligente. Cualquier servicio que precise localizar a un usuario, enviar una notificación USSD o un mensaje corto, por ejemplo, necesita de un diálogo con el HLR. Generalmente, todo este tipo de operaciones se implementan de forma software en librerías independientes que son usadas por el servicio que las precise.

En nuestro caso, la librería sera capaz de realizar las operaciones necesarias para enviar una notificación USSD y para localizar a un usuario.

Protocolos TCAP y MAP

Antes de empezar, debemos conocer los protocolos que se van a usar. El protocolo TCAP (PACT-Parte de Aplicación de las Capacidades de Transacción), se usa de forma genérica, tanto para transmitir información como para invocar operaciones remotas. La unidad básica del protocolo TCAP se denomina mensaje o diálogo TCAP.

Por su parte, el protocolo MAP (Mobile Application Part), está encapsulado dentro del protocolo TCAP, y añade las funcionalidades necesarias para realizar operaciones que interactúan con la red móvil.

Antes de describir la estructura de estos protocolos, hablaremos del modo de funcionamiento elemental. Supongamos, que un servicio móvil precisa conocer la red del operador extranjero que esta usando un usuario en roaming.

El proceso a seguir sería, básicamente, el siguiente:

- El servicio mandaría un mensaje TCAP al nodo donde se encontrase la base de datos HLR. Este mensaje contendría toda la información de direccionamiento necesaria para que la petición llegase al nodo correspondiente, y además, incluiría los datos relativos a la operación que debiera realizarse, en este caso la localización de un usuario. Por su parte, el protocolo MAP encapsulado en el mensaje contendría la información de dicho usuario.

- Una vez que el mensaje llega al HLR, y se ha obtenido la operación a realizar, el protocolo MAP pasa a primer plano, ya que es éste quien contiene la información necesaria para que dicha operación pueda realizarse.

- Así, con todos los datos, se obtiene la respuesta requerida, que es enviada a través de un mensaje TCAP, de respuesta. En este mensaje, también existe parte MAP, pero ahora ya no cumple una función tan importante como la anterior, ya que la respuesta está en la parte TCAP.

Cada mensaje TCAP, se denomina generalmente diálogo TCAP. Todos los diálogos que forman parte de una misma operación llevan un identificador de diálogo similar. Así, en este caso, tanto la petición como la respuesta llevarían el mismo identificador. Si la operación hubiese requerido más de dos diálogos, todos ellos contendrían el mismo valor en dicho campo.

Esto resulta útil, cuando un servicio realiza varias operaciones simultáneamente. De esta forma es capaz de correlar peticiones y respuestas de cada operación, sin riego a error.

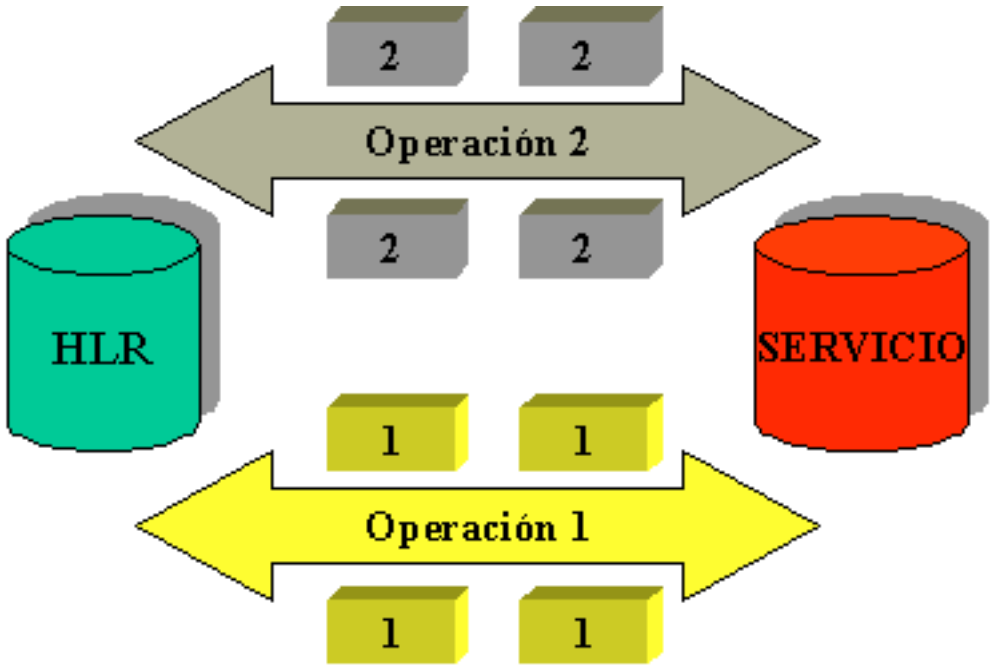

Figura 65: Transmisión de diálogos TCAP

Mensajes TCAP

Introducción

Un mensaje TCAP esta formado por tres partes:

- Porción de Transacción.
- Porción de Componente.
- Porción de Diálogo.

Figura 66: Partes del protocolo TCAP

La porción de transacción contiene información de control para el propio protocolo e información de direccionamiento necesaria para que el mensaje llegue a su destino.

La parte de componente lleva toda la información relacionada con las operaciones a realizarse.

La porción de diálogo lleva encapsulada la información MAP, que será desencapsulada en el destino, para realizar la operación definida en la parte de componente, pero en base a dicha información MAP.

En este sentido el protocolo TCAP realiza las funciones de conductor del protocolo MAP. Pasamos a describir de forma más detallada las distintas partes del mensaje TCAP.

Parte de Transacción

La parte de transacción contiene los siguientes campos:

- Subsistema origen y destino.
- Global Title origen y destino.
- Primitiva de transacción.

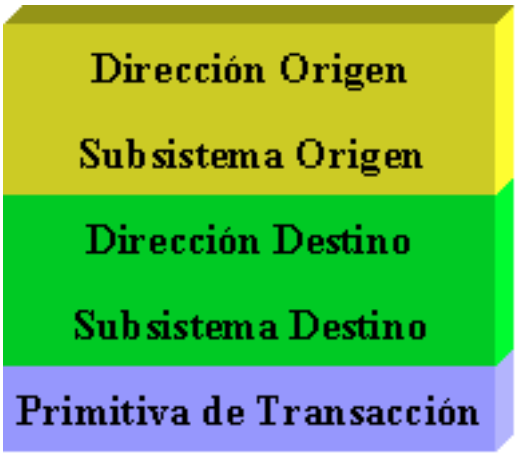

Figura 67: Parte de transacción

Global Title

El global title origen y destino contienen la información relativa a la dirección origen y destino. Su estructura es la de un número de teléfono normal, 34609490005, por ejemplo, pero no contiene explícitamente la información necesaria para encaminar el mensaje dentro de la red de señalización. Así, un global title requiere de una traducción previa por parte de la PCCS para extraer la información de encaminamiento. Dicho proceso recibe el nombre de GTT (Global Title Traduction).

El resultado del GTT puede ser un SPC + un SSN o un SPC + otro GT, por lo que un mensaje puede requerir varias traducciones antes de llegar a su destino. Las tablas de encaminamiento en base a GT's son bastante complejas, y sólo algunos puntos de la red poseen capacidades de GTT (recuerdese en este punto lo dicho en el capítulo anterior acerca del GT).

La estructura general de un global title es la siguiente:

34 + IR + X0X1X2 +X3X4X5 + X6X7X8

donde:

- 34: Indicativo del país, en este caso España.
- IR: Identificativo de red, (GSM, RI, ...).
- X0X1X2: Provincia de señalización.
- X3X4X5: Punto de señalización dentro de la provincia.
- X6X7X8: Número de subsitema.

Codificación TDBC

Cabe destacar que el GT, previamente a ser enviado es codificado en TDBC. Esta codificación consiste en coger los números que componen el GT de dos en dos y transponerlos. Posteriormente se define una rutina que realiza esta función.

Primitiva de Transacción

En dicho campo se establece el código de acción a efectuar al nivel más bajo de la comunicación mediante diálogos TCAP. Las distintas primitivas nos permiten:

- TR-UNI: Inicio de intercambio de diálogos sin esperar respuesta.
- TR-BEGIN: Inicio de intercambio de diálogos esperando respuesta.
- TR-CONTINUE: Mantenimiento del intercambio de diálogos esperando respuesta.
- TR-END: Finalización del intercambio de diálogos de forma correcta.
- TR-ABORT: Finalización del intercambio de diálogos de forma incorrecta.

Implementación software de la parte de transacción

A continuación se detalla una posible implementación software de la parte de transacción:

```
//************* DECLARACION DE TIPOS, VARIABLES Y FUNCIONES *************

//Definición del tipo DirSpcSsn

struct DirSpcSsn
{
   int spc;
   int ssn;
}

//Definición del tipo TituloGlobal

struct TituloGlobal
{
   int tipo_traduccion;
   int tipo_codificacion;
   int naturaleza_direccion;
   int global_title[6];
}
```

```
//Definición del tipo Direccion

struct Direccion
{
   octet             indicadores_direccion;
   DirSpcSsn      direccion;
   TituloGlobal    titulo_global;
}

Direccion dir_origen;
Direccion dir_destino;

DirSpcSsn direccion1;
DirSpcSsn direccion2;

TituloGobal  gt_origen;
TituloGlobal gt_destino;

int[] codificar_TDBC (char * cadena)
{
  int gt_codificado[6];
  char aux;
  int digito, digito_siguiente;

  aux=cadena[1];
  digito=atoi(&aux);
  aux=cadena[0];
  digito_siguiente=atoi(&aux);
  gt_codificado[0]=16*digito+digito_siguiente;

  aux=cadena[3];
  digito=atoi(&aux);
  aux=cadena[2];
  digito_siguiente=atoi(&aux);
  gt_codificado[1] = 16*digito+digito_siguiente;

  aux=cadena[5];
  digito=atoi(&aux);
  aux=cadena[4];
  digito_siguiente=atoi(&aux);
  gt_codificado[2] = 16*digito+digito_siguiente;

  aux=cadena[7];
  digito=atoi(&aux);
  aux=cadena[6];
  digito_siguiente=atoi(&aux);
  gt_codificado[3]= 16*digito+digito_siguiente;
```

```
  aux=cadena[9];
  digito=atoi(&aux);
  aux=cadena[8];
  digito_siguiente=atoi(&aux);
  gt_codificado[4] =16*digito+digito_siguiente;

  aux='0';
  digito=atoi(&aux);
  aux=cadena[10];
  digito_siguiente=atoi(&aux);
  gt_codificado[5] = 16*digito+digito_siguiente;

  return gt_codificado;
}

//*****************************************************************************

direccion1.ssn = 16;   //Subsistema origen
direccion2.ssn = 19;   //Subsistema destino
direccion1.spc = 0;    //Sin SPC, enrutado por titulo global
dirección2.spc = 0;    //Sin SPC, enrutado por titulo global

gt_origen.tipo_traduccion=0x00;         //sin traduccion
gt_origen.tipo_codificacion=0x11;       //plan de nume 1 y GT impar
gt_origen.naturaleza_direccion=0x04;  //Impar
gt_origen.global_title=codificar_TDBC("34609490005");

gt_destino.tipo_traduccion=0x00;         //sin traduccion
gt_destino.tipo_codificacion=0x11;       //plan de nume 1 y GT impar
gt_destino.naturaleza_direccion=0x04;  //Impar
gt_destino.global_title=codificar_TDBC("34609490006");

dir_origen.indicadores_direccion =  TCAP_IND_DIR_RUTA_GT+
                                    TCAP_IND_DIR_GT_4+
                                    TCAP_IND_DIR_SSN_PRESENTE;

dir_destino.indicadores_direccion =  TCAP_IND_DIR_RUTA_GT+
                                     TCAP_IND_DIR_GT_4+
                                     TCAP_IND_DIR_SSN_PRESENTE;

dir_origen.direccion=direccion1;
dir_destino.direccion=direccion2;

dir_origen.titulo_global=gt_origen;
dir_destino.titulo_global=gt_destino;
```

```
if(primitiva_transaccion = = TR_END)
{
      //El tipo de primitiva es finalización correcta
      dialogo.tipo_transaccion =TR_END;
      dialogo.origen=direccion_origen;
      dialogo.destino=direcion_destino;
};

if(primitiva_transaccion = = TR_BEGIN)
{
     //El tipo de primitiva es inicio de diálogos
     dialogo.tipo_transaccion=TCAP_TRANSACCION_BEGIN;
     dialogo.origen=direccion_origen;
     dialogo.destino=direcion_destino;
};
```

Porción de diálogo

La porción de dialogo contiene las siguientes partes:

- Versión de protocolo MAP.
- Protocolo MAP encapsulado
- Contexto de aplicación.

Figura 68: Porción de diálogo

Versión MAP

Actualmente existen dos versiones del protocolo MAP, MAP1 y MAP2. En la versión MAP2, que es la que se ha venido describiendo, la información MAP se encapsula en la porción de diálogo, mientras que en la versión 1 dicha información se transmite en la parte de componente. Así pues, la forma más usual de indicar en que versión trabajamos, es rellenar o no la porción de diálogo. Si no se rellena, se entenderá que estamos en versión MAP1, y que la información de dicho protocolo estará en la parte de componente.

No obstante, cabe destacar que en ocasiones la información de la operación a realizar y la información MAP son reiterativas. Cuando esto ocurre, si trabajamos en versión MAP1 no se añade un nuevo componente con la información del protocolo MAP. No obstante, en la versión MAP2 si se debe rellenar la porción de diálogo con la información MAP aunque sea reiterativa. Esto ocurre, por ejemplo, en el caso de la operación SendRoutingInformation, como se verá posteriormente.

Contexto de aplicación

El contexto de aplicación identifica a un conjunto de operaciones, y depende de la versión MAP con la que estemos trabajando. Es decir, cada identificador es válido para un conjunto de operaciones en versión MAP1 o MAP2. Cuando el destino decodifique la información, comprobará que el identificador de operación de la parte de componente es uno de los abarcados por el contexto de aplicación.

Según las estandarizaciones, una porción de diálogo vacia indica que trabajamos en versión MAP1, como hemos dicho anteriormente. Otra forma de determinar esto es utilizar el contexto de aplicación adecuado, aunque este método resulta, obviamente, más costoso.

Protocolo MAP

Las primitivas fundamentales que se usan en el protocolo MAP son:

- MAP-OPEN
- MAP-ACCEPT

aunque existen otras como:

- MAP-CLOSE
- MAP-REFUSE
- MAP-USER-ABORT

Una primitiva MAP-OPEN siempre va asociada a una primitiva de transacción TR-BEGIN, es decir, al inicio del intercambio de diálogos; mientras que un MAP-ACCEPT va asociado a una primitiva TR-CONTINUE o TR-END, en la parte de transacción.

Además, el protocolo MAP se codifica en ASN1, antes de ser encapsulado. Este sistema de codificación se usa para transmitir de forma más eficiente la información, y permite detectar de forma más fácil los posibles errores.

Para realizar la codificación ASN1 se puede usar un compilador ASN1, denominado *snacc* (libre distribución), que facilita enormemente esta labor. Dicho compilador lee cierta información de un fichero y genera unas clases capaces de codificar los datos en ASN1 de forma inmediata. En el fichero deben aparecer los datos a codificar y sus respectivos tipos. Esta información debe estar estandarizada, ya que tanto el receptor como el emisor deben codificar y decodificar de igual manera.

Basándonos en las correspondientes especificaciones el archivo a realizar para ser compilado por el *snacc* será el siguiente:

```
-- Definición de estructuras simples

maxAddressLength        INTEGER::=20;

TBCD-STRING ::= OCTET STRING( SIZE(1) );

IMSI ::= TBCD-STRING(SIZE(3..8));

AddressString ::= OCTET STRING( SIZE(1..maxAddressLength) );

-- Definición de estructuras complejas

MAP-DialoguePDU ::=[0] CHOICE
{
      map-open             [0]  IMPLICIT MAP-OpenInfo,
      map-accept           [1]  IMPLICIT MAP-AcceptInfo,
      map-close            [2]  IMPLICIT MAP-CloseInfo,
      map-refuse           [3]  IMPLICIT MAP-RefuseInfo,
      map-userAbort        [4]  IMPLICIT MAP-UserAbortInfo,
}
MAP-OpenInfo ::=SEQUENCE
{
      imsi                    [0]  IMPLICIT IMSI OPTIONAL,
      originationReference  [1]  IMPLICIT AddressString OPTIONAL,
      msisdn                  [2]  IMPLICIT AddressString,
      vlrNo                   [3]  IMPLICIT AddressString OPTIONAL
}

MAP-AcceptInfo ::= SEQUENCE
{
}
```

Una vez compilado dicho archivo, tenemos preparadas las clases que nos permitirán codificar la estructura del protocolo MAP en ASN1. No obstante, generalmente estas clases no se usan directamente, sino que se recubren con otras derivadas de ellas, para facilitar su manejo dentro del servicio. A continuación se muestra un extracto de la nueva clase que se debe generar, incluyendo uno de los métodos más importantes, *codifica_open*:

```
SBBoolean SRV_MAP_DialoguePDU::codifica_open(char* msisdn_,int a, SBSeqChar&
mensaje, char* imsi_, int c, char* originationReference_, int b, char* vlrNo_, int d)
{
//Entramos en codifica openInfo
choiceId = MAP_DialoguePDU::map_openCid;
SBBoolean retorno = FALSE;
if(map_open !=NULL)
{
    delete map_open;
```

```
    map_open =NULL;
}
map_open = new MAP_OpenInfo();
map_open->msisdn.Set(&msisdn_[0],a);

if(imsi_ != NULL)
{
     map_open->imsi = new AddressString();
     map_open->imsi->Set(&imsi_[0],c);
}

if(originationReference_ != NULL)
{
     map_open->originationReference = new AddressString();
     map_open->originationReference->Set(&originationReference_[0],b);
}

if(vlrNo_ != NULL)
{
     map_open->vlrNo = new AddressString();
     map_open->vlrNo->Set(&vlrNo_[0],d);
}

AsnBuf outputBuf;
size_t encodedLen=0;
int dataSize = 1024;
char data[1024];

//Inicializa un buffer para escribir en el
outputBuf.Init(data, dataSize);
outputBuf.ResetInWriteRvsMode();

//Codifica los valores para ponerlos en el buffer
if (!BEncPdu(outputBuf, encodedLen))
{
    //ERROR: Al codificar openInfo
}
else
{
    //Ok. codificado openInfo
    outputBuf.ResetInReadMode();
    outputBuf.CopyOut(&mensaje[pos_ini_datos],outputBuf.DataLen());
}
if(map_open !=NULL)
{
    delete map_open;
    map_open =NULL;
}
return retorno;
}
```

Llamando a este método ya tendríamos codificada la información MAP correspondiente en ASN1, y estaría lista para ser incluida en el mensaje TCAP, cosa que se muestra a continuación.

Implementación software

Una posible implementación software de la porción de diálogo, que usa la clase anterior, sería, obviando la definición de los tipos:

```
if(map = = 1)
{
    //La version de MAP es 1
    //No rellenamos la porcion de dialogo
    porcion_dialogo.valor_defecto(0);
}
else
{
    //Estamos en version MAP 2

    SeqOctet ap_ctx;

  //Rellenamos el contexto de aplicacion, en este caso con el identificador de operaciones USSD
   //Contexto de aplicacion para MAP2
    ap_ctx.length(7);
    ap_ctx[0] = 0x04;
    ap_ctx[1] = 0x00;
    ap_ctx[2] = 0x00;
    ap_ctx[3] = 0x01;
    ap_ctx[4] = 0x00;
    ap_ctx[5] = 0x13;
    ap_ctx[6] = 0x02;

    if(primitiva_transaccion = = TR_END)
    {
         porcion_dialogo.resp_ap_context.length(7);
         for(int i=0;i<=6;i++)
        {
          porcion_dialogo.resp_ap_context[i]=ap_ctx[i];
         };
    }

    if(primitiva_transaccion = = TR_BEGIN)
   {
        porcion_dialogo.req_ap_context(ap_ctx);
   };

   //En este campo va la informacion MAP
   SeqOctet info_user;
```

```
    if(primitiva_transaccion = = TR_END)
    {
     //Rellenamos la informacion de usuario con MAP_ACCEPT

     SeqChar prueba;
     SRV_MAP_DialoguePDU* p_aux=new SRV_MAP_DialoguePDU();
     p_aux->codifica_accept(prueba);
     info_user.length(prueba.length());
     memcpy(&info_user[0],&prueba[0],prueba.length());
     delete p_aux;
     p_aux=NULL;
    };

   if(primitiva_transaccion = = TR_BEGIN)
    {
     //Rellenamos la informacion de usuario con MAP_OPEN

     SeqChar prueba;
     char* var1;
     int top[16];

     //Pasamos a TDBC el numero de movil
     top=codificar_TDBC(movil);

     var1=&top[0];
     SRV_MAP_DialoguePDU* pp_aux =new SRV_MAP_DialoguePDU();
     pp_aux->codifica_open(var1,a,prueba,NULL,0,NULL,0,NULL,0);
     info_user.length(prueba.length());
     memcpy(&info_user[0],&prueba[0],prueba.length());

     delete pp_aux;
     pp_aux=NULL;
    };

    porcio_dialogo.info_usuario = info_user;

};
```

Parte de componente

La parte de componente contiene las siguientes partes:

- Primitiva de componente.
- Componentes codificados en ASN1.
- Identificativo de invocación.

Figura 69: Parte de componente

Primitiva de componente

La primitiva de componente tiene una equivalencia directa con la primitiva de transacción, y en cierta manera su información es reiterativa, pero a otro nivel. Las principales primitivas son:

- CT-UNI: Inicio de intercambio de componentes sin esperar respuesta.
- CT-BEGIN: Inicio de intercambio de componentes esperando respuesta.
- CT-CONTINUE: Manteniminto del intercambio de componentes esperando respuesta.
- CT-END: Finalización del intercambio de componentes de forma correcta.
- CT-ABORT: Finalización del intercambio de componentes de forma incorrecta.

Identificativo de invocación

El identificativo de invocación sirve para identificar al componente, ya que en algunas ocasiones se pueden o se deben mandar varios en la parte de componente. Se usa generalmente, en la versión 1 de MAP.

Componentes codificados en ASN1

Como hemos dicho los componentes están codificados en ASN1. A continuación se muestra el fichero .asn1 que se debe generar para ser compilado con el snacc. Se puede observar que cada componente incluye la información necesaria para realizar la operación que se está invocando.

Process Unstructured SS Request

Esta operación se usa para enviar una notificación USSD a un móvil. Siempre es mandada desde el servicio al HLR.

Código de operación: 59

```
ProcessUnstructuredSS-Request ::= SEQUENCE
{
      ussd-DataCodingScheme   USSD-DataCodingScheme,
      ussd-String                    USSD-String
}
```

El campo *ussd-String* contiene el mensaje a mandar comprimido a 7 bits, según el código de alfabeto que se define en el campo *ussd-DataCodingScheme.*

El alfabeto por defecto que se utiliza aparece en la siguiente tabla:

Tabla 3: Carácteres del alfabeto por defecto

				b7	0	0	0	0	1	1	1	1
				b6	0	0	1	1	0	0	1	1
				b5	0	1	0	1	0	1	0	1
b4	b3	b2	b1		0	1	2	3	4	5	6	7
0	0	0	0	0	@		SP	0	¡	P	¿	p
0	0	0	1	1	£	_	!	1	A	Q	a	q
0	0	1	0	2	$		“	2	B	R	b	r
0	0	1	1	3	¥		#	3	C	S	c	s
0	1	0	0	4	è		¤	4	D	T	d	t
0	1	0	1	5	é		%	5	E	U	e	u
0	1	1	0	6	ù		&	6	F	V	f	v
0	1	1	1	7	ì		‘	7	G	W	g	w
1	0	0	0	8	ò		(	8	H	X	h	x
1	0	0	1	9	ç		)	9	I	Y	i	y
1	0	1	0	10	LF		*	:	J	Z	j	z
1	0	1	1	11	Ø	1)	+	;	K	Ä	k	ä
1	1	0	0	12	ø	Æ	´	<	L	Ö	l	ö
1	1	0	1	13	CR	æ	-	=	M	Ñ	m	ñ
1	1	1	0	14	Å	ß	.	>	N	Ü	n	ü
1	1	1	1	15	º	É	/	?	O	§	o	à

Las celdas que aparecen en se corresponden con los símbolos matemáticos más usuales, que generalmente no se suelen usar.

Send Routing Information

Esta operación se usa para pedir al HLR, la red extranjera en la que se encuentra el móvil.

Codigo de operación: 22

```
SendRoutingInfoMAP2 ::= SEQUENCE
{
      msisdn                    [0]   IMPLICIT OCTET STRING(SIZE(1..9)),
      cug-CheckInfo             [1]   IMPLICIT CUG-CheckInfo  OPTIONAL,
      numberOfForwarding    [2]   IMPLICIT NumberOfForwarding   OPTIONAL,
      networkSignalInfo         [10]  IMPLICIT ExternalSignalInfo  OPTIONAL
}

SendRoutingInfoResultadosMAP2 ::= SEQUENCE
{
      imsi                IMSI,
      routingInfo         RoutingInfo,
      cug-CheckInfo   CUG-CheckInfo   OPTIONAL
}
```

Tras la petición, el HLR responderá según la estructura SendRoutingInfoResultados MAP2, que deberemos de decodificar.

Implementación software

A continuación se muestra una posible implementación software, presuponiendo que previamente se han generado las clases de recubrimiento para la estructura ASN1.

```
//Codificacion de la parte de componente para la operación Send Routing Info

void prepara_SRI(unsigned short tipo_tc, SeqULong& ids_invocaciones, PorcionDialogo&
porcion_dialogo, DialogoEnvio& dialogo, SeqComponentes& componentes,RWCString
texto, RWCString movil, int map, RWCString orig, RWCString dest)
{

//Entramos en prepara_SRISM
TCAPComponente com;
if(primitiva_transaccion = = TR_END)
{
   //El tipo de transaccion es TR_END");
   com.operacion.op_local(22);
   //El codigo de operacion es 22 -> SendRoutingInfo
   com.tipo_componente=CT_END;
    //Tipo de componente FINALIZACION
};
```

```
if(primitiva_transaccion = = TR_BEGIN)
{
    //El tipo_tc es TR_BEGIN

    com.operacion.op_local(22);
    //El codigo de operacion es 22 -> SendRoutingInfo
    com.tipo_componente=CT_BEGIN;
};

  SBSeqChar text;

  int c;
  int numero[16];
  char* telefono;

//Pasamos a TDBC el numero del movil
numero=configurar_TDBC(movil);
telefono=&numero[0];

SendRouting* p=new SendRouting();

//Codificamos la estructura del Send Routing Info en ASN1
p->codifica(telefono,c,telefono1,c1,true,text);

com.parametros.length(text.length());
memcpy(&com.parametros[0],&text[0],text.length());

return;
}
```

Envío de un mensaje MAP

Por último, y a modo de resumen, se detalla el proceso de envio de una petición TCAP (Send Routing Information) desde un servicio.

La **parte de transacción** se rellenaría de la siguiente manera:

- **Dirección origen**: La propia.
- **Dirección destino**: La dirección del HLR dentro de la red SS7.
- **Primitiva de transacción**: TR_BEGIN.

La **porción de diálogo** quedaría:

- **Versión MAP**: 2.
- **Contexto de aplicación**: 04 00 00 01 00 13 05 (según las especificaciones).
- Información de usuario: **MAP_OPEN** conteniendo en el campo *msisdn* el número del móvil a consultar.

Finalmente, la **parte de componente** sería:

- **Primitiva de componente**: CT_BEGIN.
- **Código de operación**: 22.
- **Identificador de invocación**: 0 (sólo existe un componente).
- **Componente** codificado en ASN1: Send Routing Information conteniendo en el campo msisdn el número del móvil.

Por su parte, el mensaje TCAP devuelto por el HLR tendría la siguiente estructura.

Parte de transacción:

- **Dirección origen**: La dirección del HLR.
- **Dirección destino**: La dirección del servicio.
- **Primitiva de transacción**: TR_END.

Porción de diálogo:

- **Versión MAP**: 2.
- **Contexto de aplicación**: 04 00 00 01 00 13 05 (según las especificaciones).
- Información de usuario: **MAP_ACCEPT**.

Parte de componente:

- **Primitiva de componente**: CT_END.
- **Código de operación**: 22.
- **Identificador de invocación**: 0 (sólo existe un componente).
- **Componente** codificado en ASN1: Send Routing Information Result conteniendo en el campo imsi la respuesta requerida.

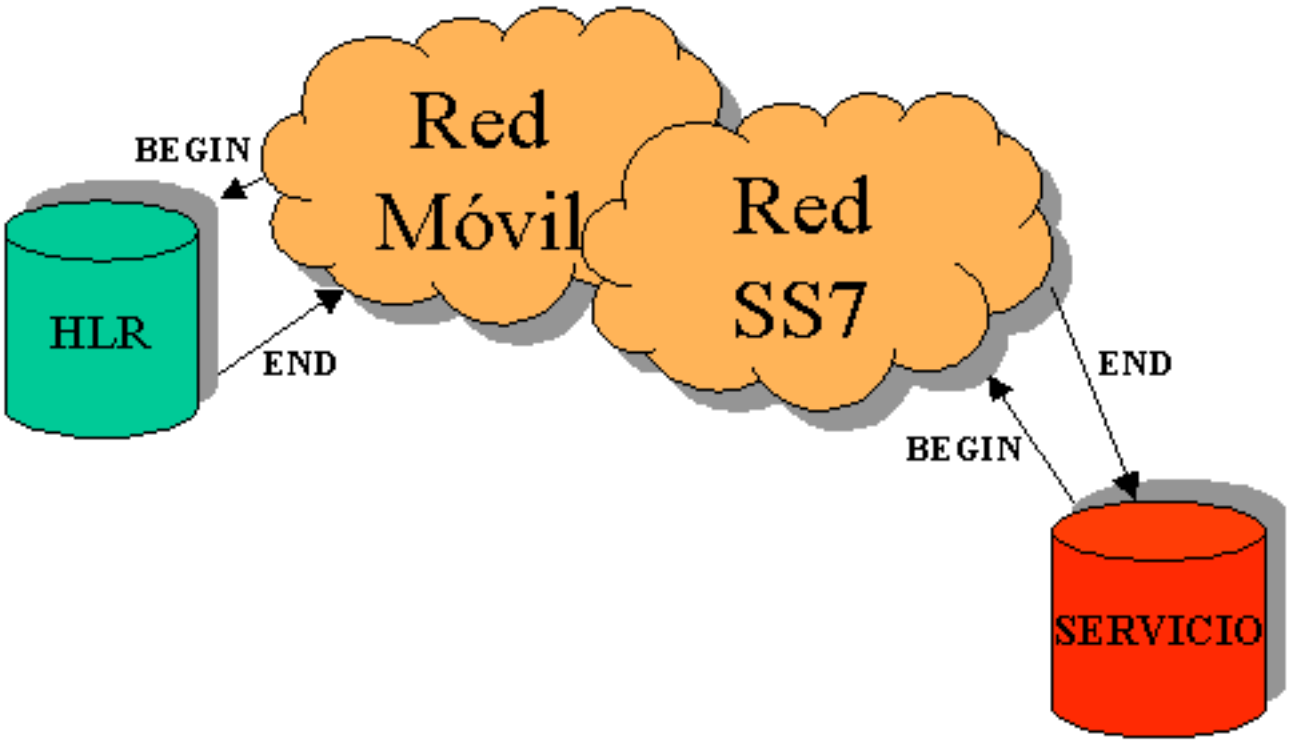

Figura 70: Transmisión de un operación TCAP

Acrónimos

ABS	Alternate Billing Service
ACD	Automatic Call Distributor
ACG	Automatic Code Gapping
ACK	Acknowledgment
ACM	Address Complete Message
AFR	Automatic Flexible Routing
AHT	Average Handle Time
AIN	Advanced Intelligent Network
AIOD	Automatic Identified Outward Calling
AMA	Automatic Message Accounting
AMATPS	AMA Teleprocessing System
AMP	AIN Maintenance Parameter
AMPS	Advanced Mobile Phone System
ANI	Automatic Number Identification
ANM	Answer Message
ANSI	American National Standards Institute
API	Application Programming Interface
APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
ASA	Average Speed of Answer
ASCII	American Standard Code for Information Interexchange (ANSI)
ASE	Application Service Element
ASN.1	Abstract Syntax Notation 1
ATB	All Trunks Busy

ATP	Acceptance Test Procedure
AUI	Attachment Unit Interface
BCD	Binary Coded Decimal
BCI	Backward Call Indicators
BCLID	Bulk Calling Line Identification
BCM	Basic Call Model
BER	Basic Encoding Rules
BG	Business Group
BGID	Business Group Identification
BGP	Border Gateway Protocol
BRI	Basic Rate Interface (ISDN)
BSN	Backward Sequence Number
CAC	Carrier Access Code
CAP	Competitive Access Provider
CC	Call Control
CCA	Call Control Adjunct
CCC	Clear Channel Capability
CCITT	Consultative Committee on International Telephone & Telegraph
CCS	Common Channel Signaling
CDAR	Customer Dialed Account Recording
CDMA	Code Division Multiple Access
CDP	Customized Dialing Plan
CDPD	Cellular Digit al Packet Data
CDSL	Customer Digital Subscriber Line

CED	Call Entered Digits
CGB	Circuit Group Blocking Message
CGSA	Cellular Geographic Service Area
CGU	Circuit Group Unblocking Message
CIC	Carrier Identification Code
CIDS	Calling Identity Delivery & Suppression
CL	Connectionless
CLID	Calling Line ID
CLLI	Common Language Location Identification
CMC	Cellular Mobile Carrier
CMS	(AT&T's) Call Management System
CNAB	Call Name Delivery Blocking
CO	Central Office or Connection Oriented
COT	Continuity Test Message
CPC	Call Processing Control
CPE	Customer Premises Equipment
CPG	Call Progress Message
CR	Conditional Requirement
CRA	Circuit Reservation Acknowledgment Message
CRC	Cyclic Redundancy Check
CRM	Circuit Reservation Message
CRP	Customer Routing Point
CS-1	Capability Set 1
CSC	Circuit Supervision Control

CSU	Channel Service Unit
CT	Call Type
CVR	Circuit Validation Response Message
CVT	Circuit Validation Test Message
DACS	Digital Access Cross-Connect System
DCE	Data Circuit (terminating) Equipment
DLC	Digital Loop Carrier
DMP	Device Management Protocol
DMS	Digital Multiplex Switch
DMT	Discrete Multitone Technology
DN	Directory Number (SS7)
DN	Dialed Number
DNIS	Dialed Number Identification Service
DP	Dial Pulse
DPC	Destination Point Code
DSL	Digital Subscriber Line
DSU	Data Service Unit
DTE	Data Terminal Equipment
DTMF	Dial Tone Multifrequency
DUP	Data User Part
DXI	Data Exchange Interface
EA	Equal Access
EADAS	Engineering & Administration Data Acquisition System
EADASNM	EADAS Network Administration

EAEO	Equal Access End Office
EAMF	Equal Access Multifrequency
EBCDIC	Extended Binary Coded Decimal Interchange Code
EDI	Electronic Data Interchange
EDP	Event Detection Point
EGP	Exterior Gateway Protocol (IETF)
EIA	Electronics Industry Association
EIR	Equipment Identification Register
EKTS	Electronic Key Telephone Service
EMS	Event Management Service
EO	End Office
ESME	External Short Message Entity
ESN	Electronic Serial Number
ETSI	European Telecommunications Standards Institute
EXM	Exit Message
FCS	Frame Check Sequence
FISU	Fill-in Signal Unit
FR	Frame Relay
FRAD	Frame Relay Access Device
FRL	Facility Restriction Level
FSD	Feature Specific Document
FSK	Frequency Key Shifting
FSN	Forward Sequence Number
FSS	Facility Selective Service

FTE	Full Time Equivalent
FTP	Fast Transfer Protocol (IETF)
FUNI	Frame User Network Interface
FX	Foreign Exchange
GN	Generic Name
GRS	Group Reset Message
GSC	Gateway Switching Center
GSM	Global System for Mobile Communication
GTT	Global Title Translations
GTV	Global Title Value
GUI	Graphical User Interface
HDLC	High Level Data Link Control
HFC	Hybrid Fiber Coaxial Cable
HLR	Home Location Register
IAM	Initial Address Message
IC	Interexchange Carrier
ICP	Intelligent Call Processing
ICR	Intelligent Call Router
IDLC	Integrated Digital Loop Carrier
IDT	Integrated Digital Terminal
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
INR	Information Request Message

IP	Intelligent Peripheral or Internet Protocol (IETF)
IPC	Interprocess Communication
IPI	Intelligent Peripheral Interface
ISDN	Integrated Services Digital Network
ISDNUP	ISDN User Part
ISO	International Standards Organization
ISP	Intermediate Service Part
ISPC	International Signaling Point Code
ISUP	ISDN User Part (circuit related)
ITU	International Telecommunication Union
ITU-T	Telecommunication Standardization Sector (of ITU)
ITU-TS	Telecommunication Standardization Sector (of ITU)
IWX	Interworking Function
IXC	Interexchange Carrier
LAA	Longest Available Agent
LAN	Local Area Network
LATA	Local Access & Transport Area
LCN	Logical Channel Number (x.25)
LEC	Local Exchange Carrier
LI	Length Indicator
LNP	Local Number portability
LOCREQ	Location Request
LSSGR	LATA Switching & Signalling Generic Requirements
LSSU	Link Status Signaling Unit

MAP	Mobility Application Part
MBG	Multi-switch Business Group
MCC	Mobile Country Code
MGW	Mini-Gateway Prototype
MIB	Management Information Base
MIN	Mobile Identification Number
MLHG	Multi-line Hunt Group
MMI	Man-Machine Interface
MSC	Mobile Switching Center
MSISDN	Mobile Station ISDN Number
MSO	Mobile Switching Office
MSU	Message Signaling Unit
MTP	Message Transfer Part
MTSO	Mobile Telephone Switching Office (Cellular)
MUX	Multiplexor
NA-TDMA	North American Time Division Multiple Access
NAA	Next Available Agent
NANP	North American Numbering Plan
NCA	Non-Call Associated
NCP	Network Control Point
NDC	National Destination Code
NETID	Network Identifier
NIC	Network Interface Controller
NMS	Network Management System

NNI	Network-to-Network Interface or Network Node Interface
NT	New Technology (Windows)
OAM&P	Operations, Administration, Maintenance and Provisioning
ODBC	Open Database Connectivity
OE	Office Equipment
OMAP	Operations & Maintenance Application Part
OPC	Origination Point Code
OPI	Open Peripheral Interface
OS	Operations System
OSI	Open Systems Interconnection
OTA	Over The Air
OTGR	Operations Technology Generic Requirement
PAM	Pulse Amplitude Modulation
PANS	Pretty Amazing New Services (B-ISDN)
PBX	Private Branch Exchange
PCS	Personal Communications Services
PG	Peripheral Gateway
PIC	Point In Call
PIM	Peripheral Interface Manager
PPP	Point-to-Point Protocol
PRI	Primary Rate Interface
PROFREQ	Profile Request
PSN	Alternative to PSTN (Public Switched Telephone Network)
PSTN	Public Switched Telephone Network

RADIUS	Remote Authentication Dial-In User Service
RARP	Reverse Address Resolution Protocol
REGNOT	Registration Notification
RISC	Reduced Instruction Set Computing
ROUTREQ	Routing Request
SANC	Signaling Area Network Code
SAP	Service Access Point
SCCP	Signaling Connection Control Part
SCP	Service Control Point (SS7)
SCPC	Single Channel Per Carrier
SDLC	Synchronous Data Link Control
SDSL	Symmetric Digital Subscriber Line
SEP	Signaling Endpoint
SF	Status Field
SI	Service Indicator
SIB	Status Indicator Busy
SIF	Signaling Information Field
SIO	Signaling Information Octet
SLC	Signaling Link Code
SLIP	Serial Line Internet Protocol
SLP	Service Logic Program
SLS	Signaling Link Selection
SMDS	Switched Multimegabit Digital Service
SMPP	Short Message Peer to Peer

SMS	Service Management System
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol (IETF)
SS7	Signaling System #7
SSP	Service Switching Point
STP	Signaling Transfer Point
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TDMA	Time Division Multiple Access
TUP	Telephone Users Part
UDP	User Datagram Protocol
UDT	Unitdata
UDTS	Unitdata Service
VAD	Voice Activated Dialing
VANC	Voice Activated Network Control
VLR	Visitor Location Register
VPN	Virtual Private Network
VRU	Voice Response Unit
WAN	Wide Area Network
WATS	Wide Area Telephone Service

Documentación

Como complemento a todo lo desarrollado en este proyecto fin de carrera, se adjunta la siguiente documentación:

- Traceo real de la operación **Send Routing Info** en la red SS7.
- Fichero de ejemplo acerca de la utilización de la codificación **ASN1**.
- Fichero resultante tras ser compilado el anterior con el **snacc**.
- Especificación **GSM 09.02** acerca del protocolo MAP.