ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERIA ELÉCTRICA

STANDARD IS-41

POLITECNICA DEL LITORAL
Guayaquil-Ecuador

TOPICO DE GRADUACIÓN I

Profesor: Ing. Vicente Saltos

Integrantes: Katty Iñiguez V.
Jimmy Rodriguez G.
Rosa Zeas M.

INDICE

INTRODUCCION

Hasta principios de los años 90, los usuarios estadounidenses cuando se transferían entre diferentes sistemas celulares durante viajes a larga distancia, tenían que registrarse manualmente en un nuevo mercado, para esto, el usuario requería llamar a una operadora para solicitar el registro.

Al comienzo de la misma década, las operadoras estadounidenses por medio del comité TR45.2 de la TIA (Telecommunications Industry Association) desarrolló el estándar IS-41 para permitir que diferentes sistemas celulares acomoden automáticamente subscriptores que pasen dentro de su área de cobertura, a esto se llama *Interoperator Roaming* (Transferencia de Interoperador). Este estándar ha pasado por muchas revisiones, incluyendo en cada una más funciones.

El IS-41 esta diseñado para usar información del AMPS (Servicio Telefónico Móvil Avanzado) para administrar la llamada celular en la red de. IS-41 es relativamente simple. Confía en los principios fundamentados de protocolos por capas como el X.25 y ss7 y los utiliza confiadamente como medio de transporte, operando en sus capas de nivel más bajo.

En el presente estudio analizaremos revisiones B, C y D del IS-41, sus aplicaciones y la operación de la red fuera de la MSC (Control de Switcheo Móvil) así como las operaciones entre MSC, VLR (Registro de Localización de Visitante) y HLR (Registro de localización de Recepción)

En el presente estudio para mejor comprensión del estándar IS-41 se definirán conceptos básicos de Sistema de Comunicación Celular.

1.- SISTEMA DE COMUNICACIÓN CELULAR

1.1 ELEMENTOS DE UNA RED CELULAR

1.1.1.- Celda.- La zona que recibe servicio de un transmisor en un sistema celular. Zona de cobertura de cada estación base.

1.1.2.- Estación base: La estación base es el elemento que lleva la señal desde el MSC hasta el abonado celular y viceversa. Tiene como elementos básicos las antenas de transmisión/recepción, los radios, etc. La estación base sirve de enlace entre el abonado celular y la MSC para poder establecer una óptima comunicación.

1.1.3.- Estación móvil (MS): Es una estación dentro de los sistemas celulares que es usada mientras el usuario se encuentra en movimiento en cualquier lugar. Las estaciones móviles pueden ser unidades portátiles o instaladas en un vehículo.

1.1.4.- Centro de Conmutación Móvil (MSC): El Centro de Conmutación Móvil es el cerebro de todo el sistema celular, controla el enrutamiento de las llamadas entre abonados celulares o entre estos y los abonados fijos, determina la celda que provee un mejor servicio para un abonado determinado, identifica la ubicación de cada abonado dentro del sistema, detecta y registra los abonados visitantes (pertenecientes a otra red) y tasa las llamadas realizadas, entre muchas funciones inalámbricas a la red con hilos u otras redes celulares. Dependiendo de la función que realice, puede ser:

- **Home MSC.-** El MSC-H es usualmente localizado en la ciudad donde habita el subscriptor.

- **Gateway MSC.-** Todas las llamadas originadas en la PSTN entran a la red celular a través del MSC-G. Esto es posible gracias a que la red celular tiene unos switches con son conectados a la PSTN y solamente a través de los MSC-G puede existir interconexión.

- **Visiting MSC (MSC-V).-** MSC que incluye servicio en el área en la cual un MS esta en roamung. El MSC-V puede ser algún switch en la red, incluyendo un MSC-H o un MSC-G.

- **Serving MSC (MSC-S).-** Switch que actual y activamente esta dando servicio de radio a un SM. MSC-S es similar a MSC-V, exceptuando que esto se aplica solo al MSC que dando servicio activo a un MS.

- **Originating MSC (MSC-O).-** MSC u otro switch gateway, el cual recibe una llamada que va a ser enviada a un MS. El MSC –O es usualmente el MSC-H, pero puede ser un MSC-G.

- **Anchor MSC (MSC-A),.-** MSC que controla el primer radio asignado a un MS durante una llamada. Para la creación de una llamada celular, el MSC-A no cambia.

1.1.5.-Registro de ubicación local (HLR): Unidad que mantiene toda la información de abonados, incluyendo perfiles de usuario como el número de indentificación del móvil (MIN), número de serie del móvil (MSN) ,información de actividad y ubicación actual, es una base de datos para el almacenaje y gestión de subscriptores. A esta base de datos se llaman Tabla Celular. Cuando un individuo compra un servicio desde un operador, este registra al usuario en el HLR.

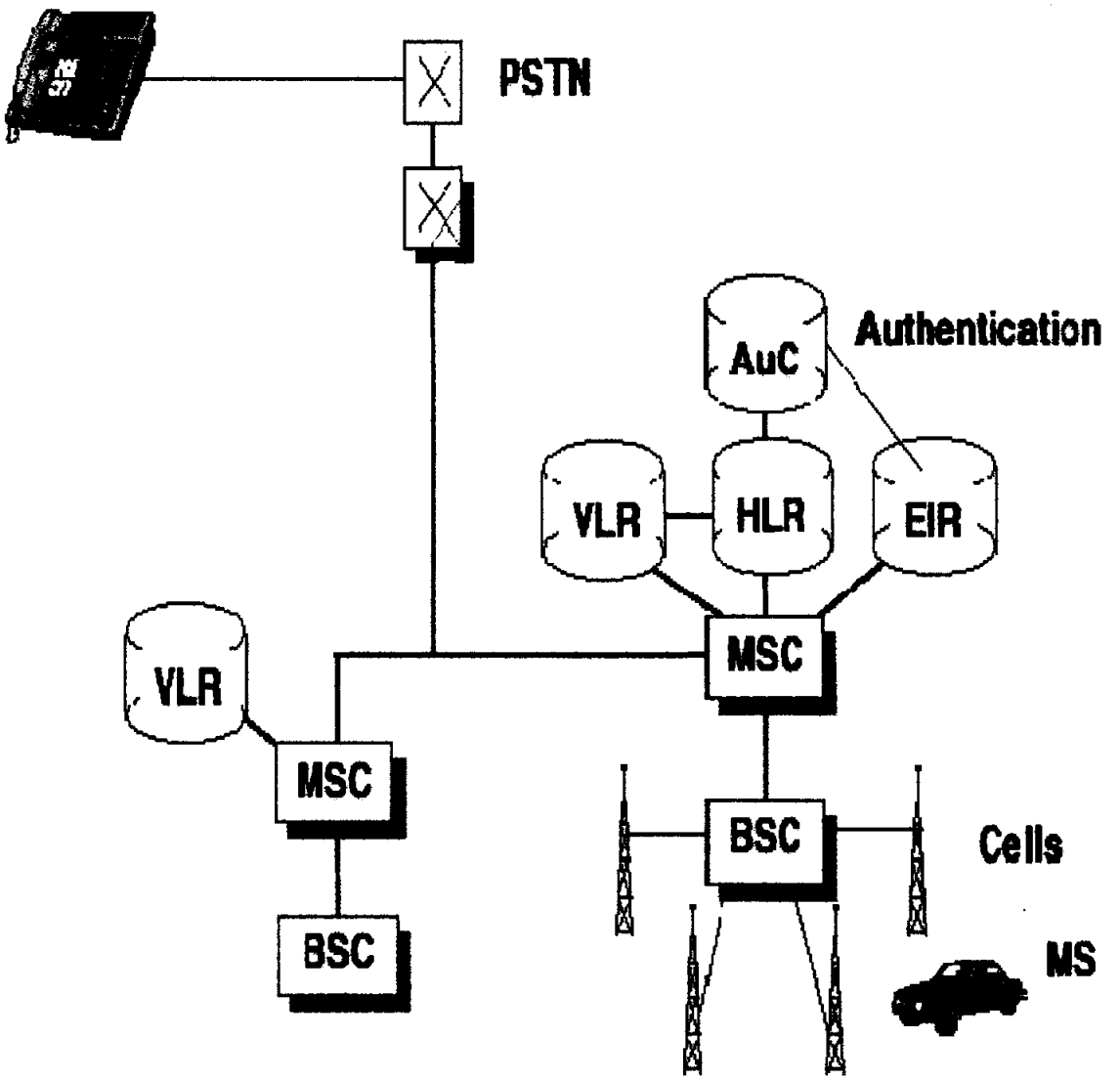
1.1.6.- Registro de ubicación visitada (VLR): Unidad funcional que almacena en forma dinámica la información del abonado que esta siendo roaming en otra area de servicio, esta base se la llama Tabla Servchng .

1.1.7. - Registro de identidad de Equipo (EIR): Es una base de datos usada para mantener una lista de estaciones móviles legitimas, fraudulentas o defectuosas. Cuando un celular se activa, el número de serie es transmitido y verificado en la base datos de teléfonos listados. Hay dos tipos de clasificaciones EIR: Los teléfonos de la lista Gris (ellos pueden registrarse todavía sobre la red, pero se investigaran), los

teléfonos de la lista Negra (incluyen teléfonos hurtados, excluye los teléfonos de la Lista Negra (incluyen teléfonos hurtados, excluye el teléfono de ser usado).

1.1.8.- Centro de Autentificación (AuC).- El AuC es usado por el HLR para garantizar el servicio al Ms.

1.1.9.- Conmutación de la red Telefonía Publica (PTSN).- Es la empresa local de telefonía y las llamadas desde celulares en la que intervienen teléfonos convencionales pasan por su centro de conmutación.

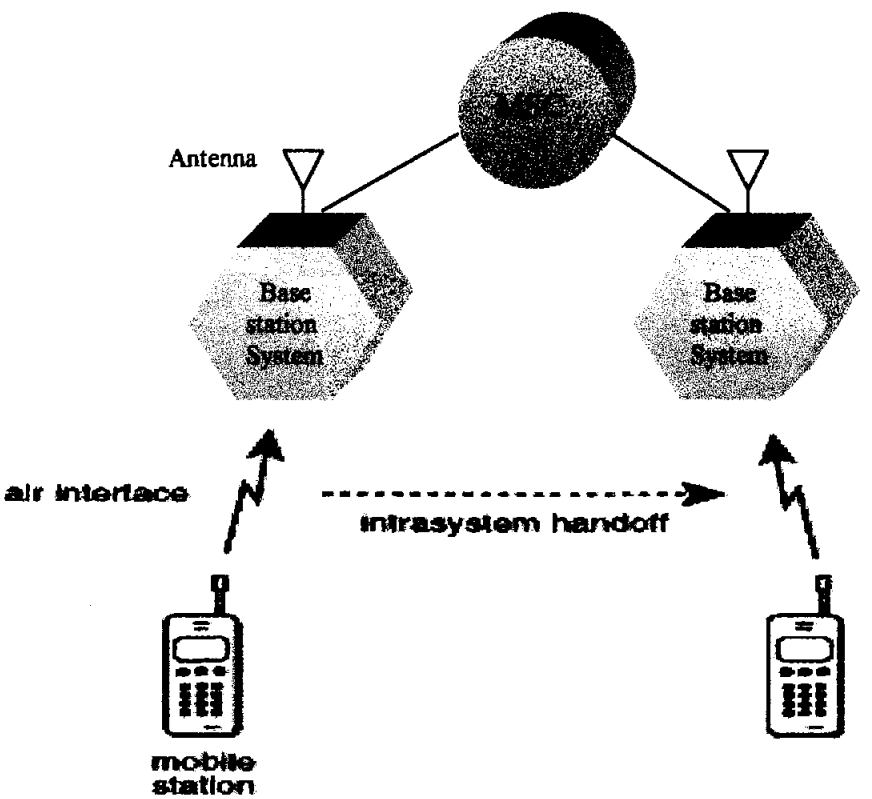


1.2.- Conceptos Básicos

1.2.1.- Handoff.- encierra un grupo de funciones soportadas entre una estación móvil y una red de trabajo que permite el MS moverse de una celda a otra (o de un canal de radio a otro, o entre celdas) cuando una llamada esta en progreso. La función del handoff requiere sofisticada coordinación entre la red y el MS para una transferencia al MS sin errores de un canal de radio a otro durante una llamada. Hay dos tipos de Handoff:

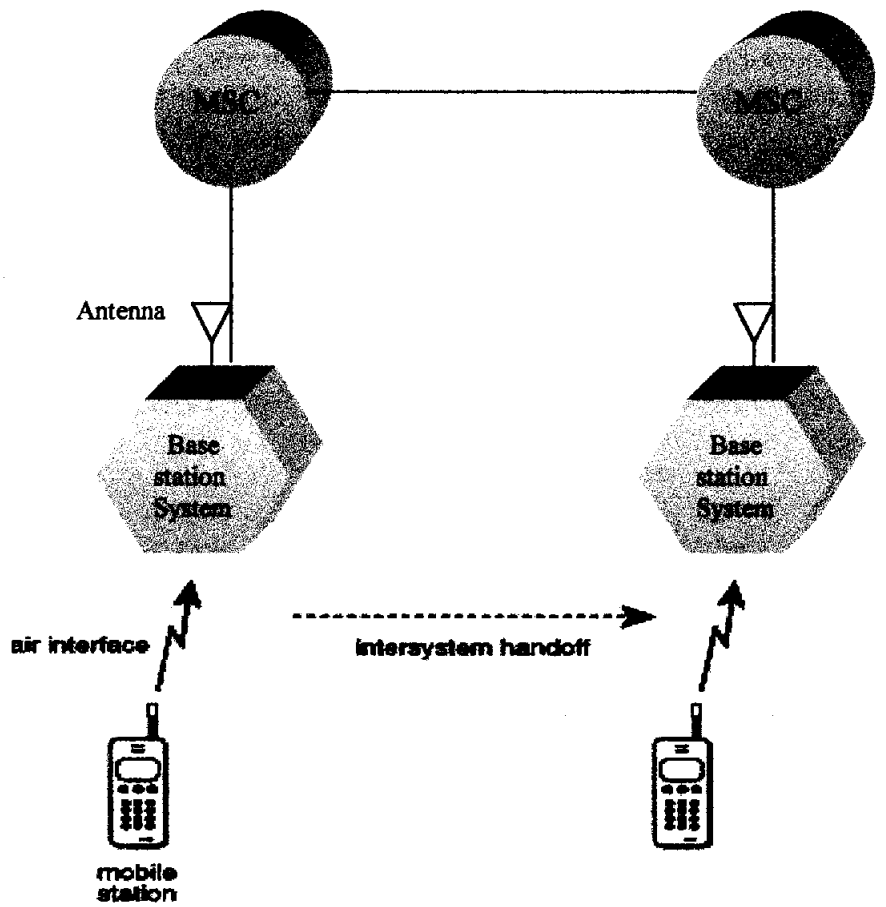
1. Intrasystem Handoff (Handoff dentro de sistemas)
2. Intersystem Handoff (Handoff entre sistemas)

1.2.1.1.- Intrasystem Handoff.- Es un handoff entre dos celdas o canales de radio que "tienden" al mismo MSC (Mobile Switching Center). En este caso, no se requiere la coordinación entre los MSC para soportar el movimiento de un MS entre celdas.



1.2.1.2-Intersystem Handoff (ROAMER).- Es un handoff entre dos celdas que "tienden" a dos diferentes MCS. Este tipo de handoff requiere señalización especializada entre los dos MCS para coordinar el movimiento del MS entre las celdas. Puesto que el protocolo Is-41 tiene que ver con operaciones entre sistemas, este provee las operaciones necesarias para soportar el *Intersysttem Handoff.* El *Intrasystem Handoff* no esta dentro del alcance del IS-41 y la vía con que se maneja son métodos de los propietarios de los MSC.

CELLS INVOLVED IN INTERSYSTEM HANDOFF



1.2.1.2.1.-ROAMER TYPES

- **Transient Roamer.-** Es un MS que es servido por un Sistema de Servicio el cual tiene un acuerdo de intercambio de servicio con el Sistema Local del MS, pero no tiene conectividad con esa red. El MSC/VLR servidor no puede enviar o recibir ningún mensaje desde el HLR del MS. tiene una entrada en la Tabla SERVCHNG con el campo ROAMDATA seteado como TRANS_ROAM.

- **Network Roamer.-** Es un MS en un sistema servidor que tiene un acuerdo de intercambio de servicio con el Sistema Local del MS y tiene conectividad con esa red. El MSC/VLR servidor puede enviar y recibir mensajes desde el HLR del MS, tiene una entrada en la Tabla SERVCHNG con el campo ROAMDATA seteado como NSK_ROAM.

- **Permanent Roamer.-** Es un MS en un Sistema Servidor que define al MS como un abonado local pero define un DN alterno para el MS que seria diferente al DN propio del MIN. El MSC no tiene conectividad de red con el HLR del abonado.
  Un escenario común para un permanent roamer es cuando un MS esta visitando un area por un periodo de tiempo extendido y el MSC no tiene conectividad de red con el HLR del MS, pero el abonado quiere recibir llamadas locales. El MS tiene un campo en la Tabla CELULAR del MSC V que contiene el DN alterno para el MIN (el campo ROAMER esta seteado como Y)

- **Permanent Network Roamer.-** Es igual al Permanent Roamer excepto que el sistema servidor tiene conectividad con el HLR del MS.
  Un escenario común para Network roamers es cuando un abonado conmuta regularmente entre dos áreas de servicio, con un solo teléfono móvil, y tienen un local number en cada area. El MS tiene una entrada en la Tabla CELULAR que contienen un DN alterno para el MIN (el campo ROAMER es seteado como Y).

1.2.2.- AMPS.- Servicio Telefónico Móvil Avanzado que trabaja con FDMA, e incluye dos rango de frecuencia en la región de 800 Mhz. El rango inferior de canales se utiliza para transmisión de los usuarios (móviles, portátiles) y va desde 824MHz hasta 849MHz, se lo denomina Uplink. El rango superior de frecuencia se utiliza para transmisión de la estación bases y va desde 870MHz hasta 894MHz, se lo denomina Dowlink. AMPS es utilizado en EEUU y Canadá, pero AMPS es también un estándar de facto en algunos países de América Latina, es muy común en la cuenca del pacífico y también se encuentra en Africa y en la antigua URSS. Es decir que AMPS se encuentra en todos los continentes excepto Europa y la Antártica. AMPS está definido no solo por

un estándar, sino por muchos estándares. Todos los estándares son desarrollados por el comité TR-45 de la TIA (Telecommunications Industry Association - Asociación de Industriales de las Telecomunicaciones). Hoy día, mas de la mitad de los teléfonos celulares en el mundo operan de acuerdo a los estándares AMPS, los cuales, desde 1988, han sido mantenidos y desarrollados por la TIA. Desde sus humildes comienzos, AMPS ha crecido para acomodarse a la tecnología celular digital de TDMA y CDMA, operación análoga de banda angosta (NAMPS) y modificaciones residenciales.
Más recientemente, las operaciones en las bandas PCS de 1800-2000 MHz han sido agregadas a los estándares para CDMA, TDMA, análogo de banda angosta y prontamente hasta el antiguo análogo sencillo.

1.2.3.-FDMA.- El ancho de banda de frecuencias total asignado se divide en varias subbandas de frecuencia o canales, una vez asignado un canal de frecuencia específico se le utiliza durante todo el período de transmisión de una trama, lo normal es que los canales de frecuencia se asignen por demanda de acuerdo a un canal de señalización aparte. El ancho de banda requiere cada depende de la tasa de datos deseada y el método de modulación.

1.2.4.-PAGE: Mensaje pequeño el que es "broadcast" sobre toda el área de servicio, usualmente en forma simultánea por las estaciones base.

1.2.5.-CDMA: Acceso Múltiple por División de Código, se aplica específicamente a Los sistemas de radio de espectro disperso, maneja portadoras transmitidas con ancho de banda amplio que contienen una gran forma de onda digital y compleja, con una velocidad de bits cien veces más rápida que la velocidad de bits de un usuario individual. Se basa en una secuencia pseudoaleatoria única, en virtud de esto es posible asignar secuencias distintas a cada usuario que sería un "código" único, cada usuario utiliza la misma frecuencia todo el tiempo, pero se mezcla con diferentes patrones de código que lo distinguen. El canal es un patrón de código único.

2.- IS-41

2.1.- DEFINICION DEL IS-41

El Estándar Interino - 41 (IS-41) es el protocolo de mensajería estándar a nivel industrial usado para la transmisión de datos entre los switches celulares de diversos proveedores de servicio, para pasar información acerca de sus subscriptores a de un MSC a otro MSC que lo demande.

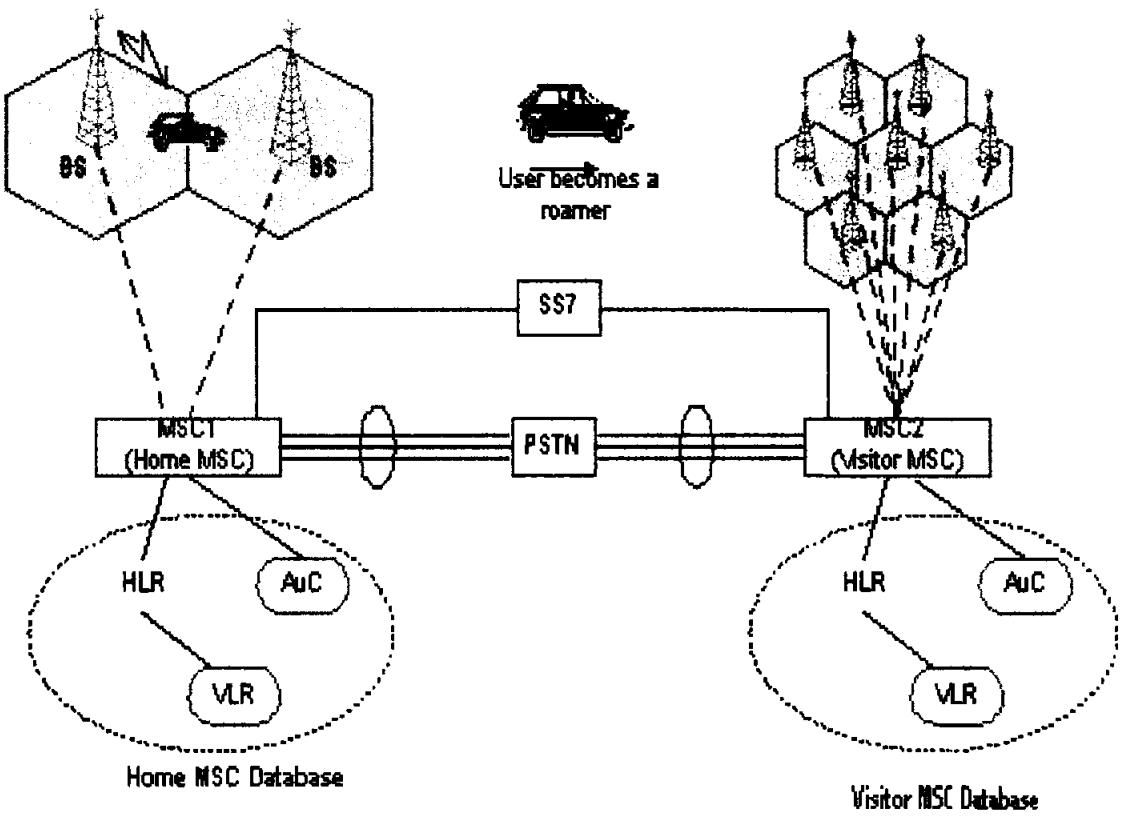
IS-41 es el estándar que facilita la movilidad para los roamers en una red celular. Para establecer una red entre diversos proveedores, el protocolo IS-41 debe ser utilizado.

Desarrollado por Electronic Industry Assosiation y Telecomunications Industry Assosiation.

El IS-41 transmite sobre una característica de AMPS (American Mobile Phone System) llamada Registro Autónomo. Este es un proceso en el cual un usuario móvil notifica a un MSC de servicio, de su presencia y su ubicación. El usuario móvil lleva a cabo esto codificando periódicamente y transmitiendo su información de identidad, lo que permite al MSC actualizar constantemente su lista de subscriptores. El comando de registro es enviado en la cabecera del mensaje de cada canal de control en intervalos de 5 o 10 minutos e incluye un valor de temporización el cual cada móvil usa para determinar el momento preciso en el cual respondería al llamado de servicio de la estación base con una transmisión de registro. En las primeras versiones esta característica se basaba en AMPS, a medida que han desarrollado la tecnología encontramos esta característica aplicada en otros estándares como CDMA.

Cada móvil reporta su MIN y ESN durante la breve transmisión de registro que el MSC puede validar y actualizar la lista de cliente dentro del mercado El MSC es capaz de distinguir usuarios propios de usuarios "transferidos o visitantes" basados en

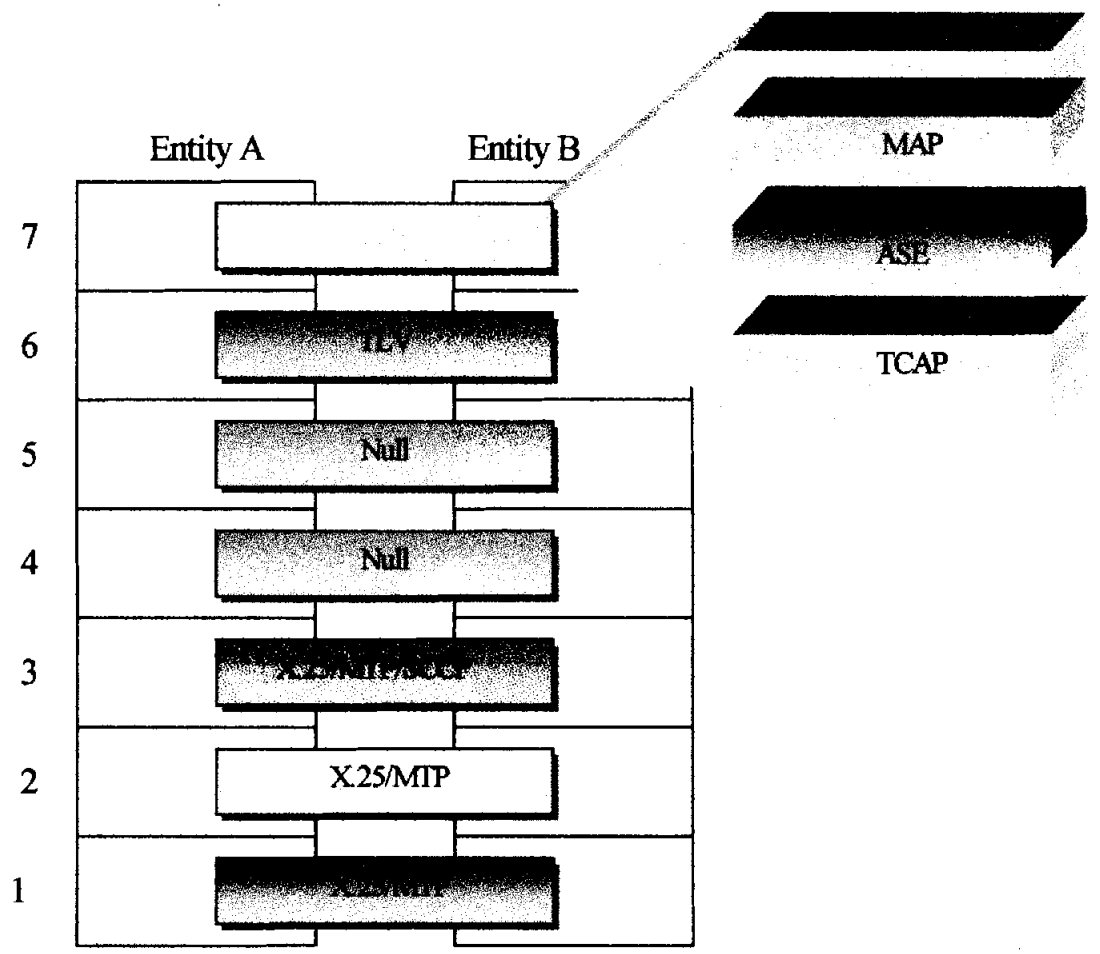
el MIN de cada usuario activo y mantiene una lista de usuarios en tiempo real en el registro de ubicación local (HLR) y registro de ubicación visitada (VLR) como se muestra en la figura.



El IS-41 permite a los MSC de sistemas vecinos manejar automáticamente el registro y validación de ubicación de *roamers* para que los usuarios no se registren manualmente como en un largo viaje. El sistema visitado crea un registro VLR para cada nuevo usuario *roamer* y notifica en el sistema propio vía IS-41 y así puede actualizar su propio HLR.

2.2.- IS41 y OSI

IS-41 es organizado a base del modelo OSI (Open System Interconnection), pero no usa todas las capas de este modelo, tal como se demuestra en la figura.



IS41 Y OSI

Desde la publicación de IS-41 (1991) el modelo OSI ha hecho cambios a las capas de aplicación y presentación. Las ultimas 3 capas de IS-41 coinciden con las ultimas tres capas de X.25, y con las de SS7 conocido como la parte de transferencia de mensajes (MTPs) en SS7. La parte de control de conexión de señalización de SS7 (SCCP) es también parte de la capa 3.La capa 6 usa la sintaxis de transferencia ISO/ITU-T, especialmente el TLV. La capa 7 se muestra claramente en la figura. La parte de aplicación móvil (MAP) del IS-41 hace uso de dos protocolos de la capa 7

del OSI, el elemento del Servicio de Control de Asociación (ACSE) y el Elemento del Servicio de Operaciones Remotas (ROSE) a estos dos protocolos se agrupan como Elemento de Aplicaciones de Servicio.

El ACSE es utilizado para unir dos aplicaciones juntas, por ejemplo la asociación entre la entidad A y la entidad B, pero no es invocado durante la transferencia de mensajes del IS-41. ROSE se invoca para este propósito.

El IS–41 utiliza del SS7 la TCAP (Parte de Aplicación de Capacidad de Transacción).

2.3.- Implementación de la Red IS-41

El IS – 41 puede trabajar a diferentes velocidades dependiendo de red de implementación que use:

- Enlace de datos X.25

Soporte para enlace de datos usando el protocolo CCITT X.25

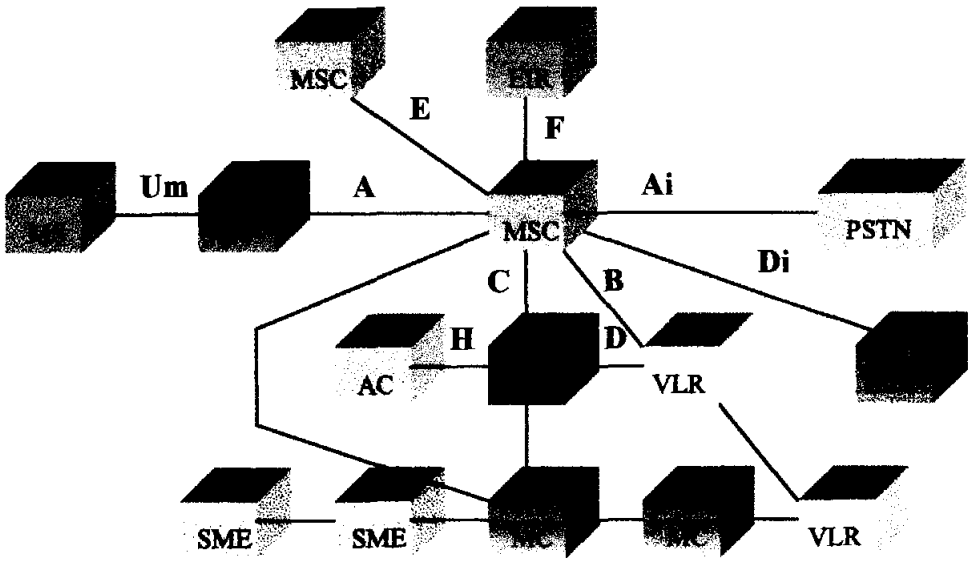
- 19.2 KBps (RS-232) ó
- 56 KBps (V.35)

- Enlaces de datos CCS7

Soporte de enlace de datos usando el standard de Señalización #7 de canal común de EIA/TIA

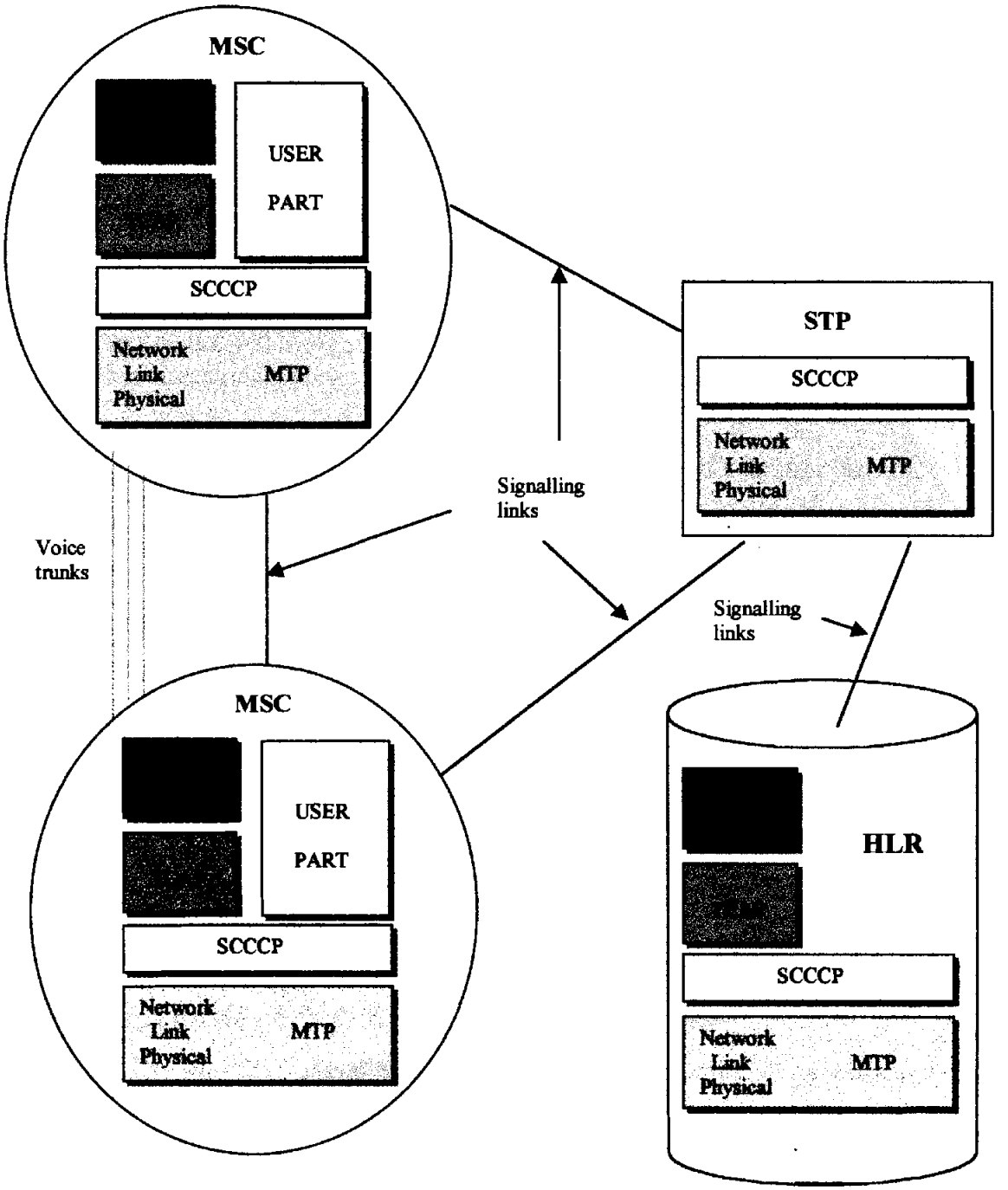
- 56 KBps (V.35 ó DS0)

IS 41 REVISION C NETWORK MODEL



Interface	Applicable Standards		
	ITU/ISO	ANSI	TIA/EIA
A	n/a	n/a	IS-634
Ai	X.25	SS7	IS-93-A
B	X.25	SS7	IS-41.2, IS-41.3
C	X.25	SS7	IS-41.2, IS-41.3
D	X.25	SS7	IS-41.2, IS-41.3
Di	?	T1.611	IS-93-A
E	X.25	SS7	IS-41.2, IS-41.3, IS-41.4
F	not defined	not defined	not defined
H	X.25	SS7	IS-41.2, IS-41.3
Q	X.25	SS7	IS-41.2, IS-41.3
Um	n/a	n/a	IS-54-B (TDMA and AMPS), IS-88 (NAMPS), IS-95-A (CDMA)

2.3.1.- IS-41 sobre CCS7



2.3.1.1.- La Parte de transferencia de mensajes (MTP)

Las 3 capas del MTP comprenden el nivel físico, el nivel de enlace de datos, y el nivel de funciones de red, las mismas que tienen dos responsabilidades básicas:

- Administración de la señalización de red
- Manejo de los mensajes de señalización

2.3.1.2. - La Parte de Control de Conexión de la Señalización de SCCP

1. La capa de SCCP transfiere mensajes desde un subsistema originador (ej. un VLR) hacia un subsistema de señalización de destino (ej. HLR) una vez que el punto de destino es alcanzado.
   - La capa MTP rutea el mensaje al nodo apropiado y el SCCP rutea el mensaje al apropiado subsistema.
2. El direccionamiento SCCP permite el ruteo a otra aplicación residente en el mismo o en un nodo diferente en una red CCS7.
   - El direccionamiento SCCP también permite el ruteo a un subsistema que reside fuera de una red IS-41 particular.
   - Este direccionamiento se lo llama Global Title Traslations

2.3.1.3.- La Parte de Aplicación de Capacidad de Transacción TCAP

1) Una vez que el subsistema que necesita comunicarse con otro es identificado por el SCCP y la conexión se establece, la capa TCAP es la responsable de mantener la conexión.
2) El TCAP esta dividido en los siguientes dos subsistemas
   - Porción Componente:
     - Correlaciona las repuestas a requerimientos
     - provee detección básica de errores
     - asegura que los componentes del mensaje son bien intercambiados
   - Porción de transacción
     - Inicia, mantiene y desconecta señalizaciones.

2.3.1.4.- La Parte de Aplicación Móvil (MAP)

La capa MAP usa el TCAP y el SCCP para transferir información de señalización entre entidades funcionales de la red IS-41.

EL MAP es la responsable de lo siguiente:

- definir funcionalmente nodos de señalización
- definir las interfaces entre nodos de señalización
- definir funciones de señalización requeridas para usar CCS7 para proveer los servicios necesarios para aplicaciones de voz y no-voz en la red de IS41 CCS7

2.3.1.5.- La capa de Parte de usuario (UP)

La capa UP construye los servicios del MTP para proveer señalización orientada a conexión para establecer, monitorear y resetear las troncales de llamadas IS41 CCS7.

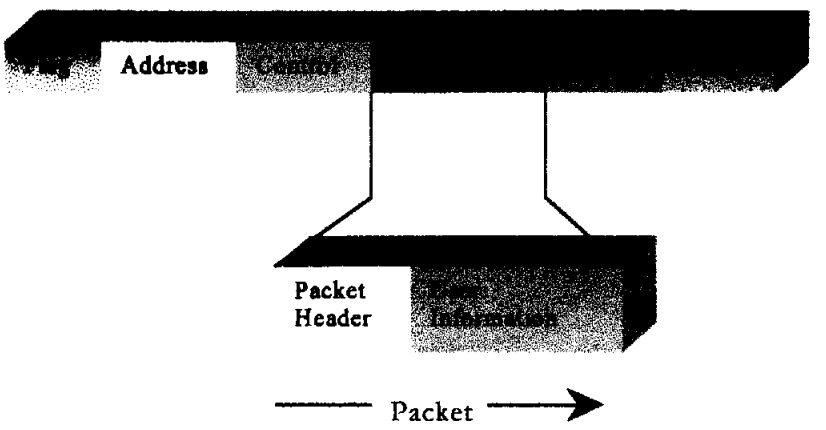
La parte de usuario provee lo siguiente:

- rapido establecimiento de llamadas
- tiempos de espera pequeños para mensajes de llamadas no establecidas
- la capacidad de manejar voz y datos simultáneamente

2.3.2.- IS-41 sobre X.25

X.25 es un protocolo, o más bien, un conjunto de protocolos que han sido estandarizados para poder accesar a una red de conmutación de paquetes. Hace referencia a las tres primeras capas del modelo OSI. Las mismas que son soporte de la red IS-41 donde cada elemento de la red se considera como un nodo por lo cual los mensajes simplemente son encapsulados en paquetes, los mismos que contienen la información del usuario, la validación, el envío de llamadas, el hand off y otras informaciones para mensajes IS-41. El IS-41 lo distribuye de la siguiente manera: el header el cual contiene la validación , el call delivery, el handoff ,etc. Y la parte de datos que contiene información del usuario

TRAMA Y PAQUETE DE X.25



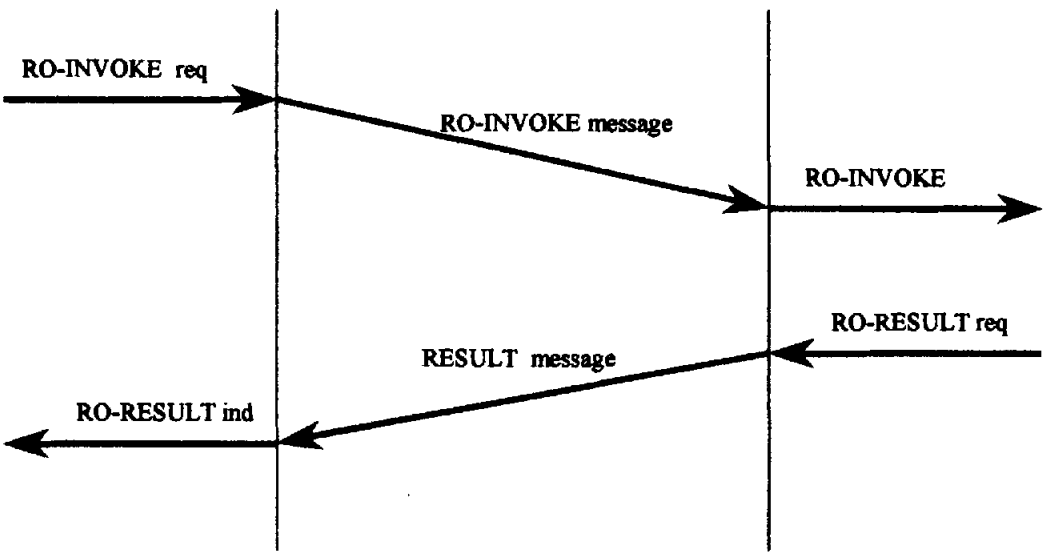
2.4.-Uso Del Elemento de Servicio de Operación Remota (ROSE)

En esta sección proporcionamos un guía del ROSE y como lo utiliza él IS-41. El modelo utiliza un proceso para las operaciones y procedimientos remotos llamados (RPC). Este es basado en el modelo Cliente - Servidor el cual es tipo de comunicación asimétrica, en este medio el cliente envía un mensaje de requerimiento y espera un mensaje de aprobación, el cliente no se entera de la localización del servidor que podría estar en cualquier lugar de la red, esto contrasta con la mayoría de protocolos e identidades del OSI en las cuales la transferencia es simétrica en la cual circula en ambas direcciones en el mismo tiempo. El modelo ROSE es el ideal para IS-41 desde las operaciones entre MSCs, VLRs, y HLRs son asimétricas.

La puesta en practica del RPC del OSI es ROSE, que esta basado en dos principales conceptos: envía pedido de operación a un servidor y transportar los resultados de la operación al cliente.

Los resultados de la operación pueden reportar sobre varias combinaciones de éxito o fracaso de las operaciones, para los procesos de las comunicaciones sincrónicas y asincrónicas

USO DE LOS MENSAJES INVOKE Y RESULT

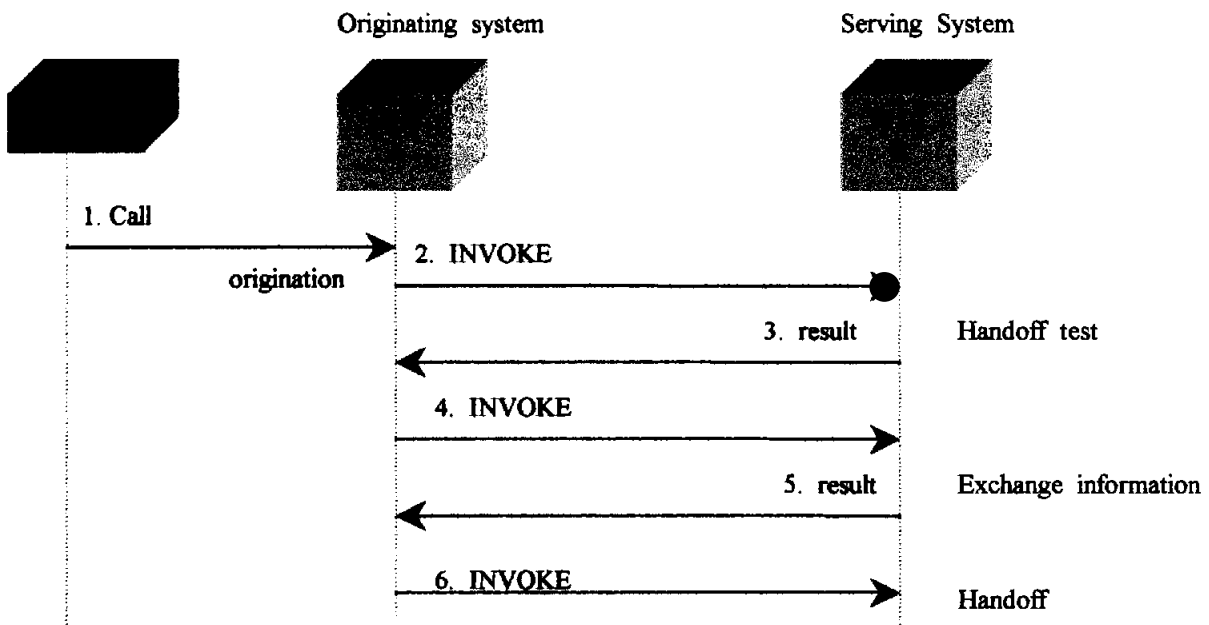


El termino req significa solicitar y el termino ind significa indicación. Las operaciones del ROSE están consideradas sin conexión en el temporizador, no mantiene los diagramas de estados para seguir las operaciones en curso. Después que se haya realizado la operación, el servidor retorna al RO-RESULT req, que es presentado al cliente como el RO-RESULT IND. Los valores en los mensajes de la invocación y de resultados deben de proporcionar la identificación. Las clases de operaciones definidas como sincrónicas y asincrónicas, la operación asincrónica es la mas usada en el IS-41.

2.4.1.-Uso de ROSE en un MS desde un MSC a otro MSC.

La figura muestra los mensajes del ROSE que están intercambiando cuando la estación móvil se mueve desde un MSC otro , en este caso el MSCA a MSC B. Al inicio ROSE invoca un mensaje y los resultados son utilizados para realizar el HANDOFF y realizan las pruebas (eventos 2 y 3) . El conjunto siguiente se invoca y el mensaje resultado en los eventos 4 y 5 son utilizados para los procedimientos administrativos que establece el circuito y verifica la conexión este hecha.

Finalmente la ultima invocación en el evento 6 se envía desde del MSC A para observar que la operación de handoff era acertada.



Example de ROSE and IS-41 operation

3.-OPERACIONES

Ahora tenemos la información suficiente para examinar las operaciones del IS-41. En esta sección muestra algunos ejemplos de las operaciones del IS-41. Para ello primero vamos a explicar dos de los mensajes que se utiliza para tener un mejor entendimiento de las operaciones que se puedan realizar.

1) Registration Notification

Los mensajes involucrados para el registro de móviles son los siguientes : Registration Notification (REGNOT), Registration Cancellantion (REGCANC), Qualification Request (QUALREQ), y el Profile Request (PROFREQ).

Estos mensajes varían de acuerdo a cuantos parámetros manejen. Los parámetros de mensajes para operaciones de registro son:

- Mobile identification number (MIN) :La representación de 10 dígitos del MS
- Mobile serial number : El electronic serial number de 32 bits de la estación móvil.
- Qualification information code: Indica el tipo de calificación necesaria durante el registro, como es la validación y perfil o solo la validación.
- System my type code of VLR: ID del VLR del proveedor de sistemas móviles
- MSC id of serving MSC: Indica el ID de un sistema especificado. Este es un campo de 3 bytes de los cuales 2 bytes son del SID y el otro es el SWNO.
- System my type code of HLR : ID del HLR del proveedor de sistemas móviles.
- Originations indicators: Identifica que tipo de llamadas pueden ser originadas por las estaciones móviles (solo locales o internacionales)

2) LOCATION REQUEST

El mensaje Location Request (LOCREQ) debe contener cuatro parámetros. Estos parámetros Estos parámetros son descritos abajo, parámetros opcionales no se describen en este resumen

- Dialed digits : El numero de la estación a la que se llama
- MSC identifier: Indica el ID del sistema especificado.

- System my type code: es un identificador registrado para cada equipo móvil del proveedor.
- Billing ID field : Contiene el ID del MSC-H . Es inicialmente asignado en el sistema MSC-H . Usado principalmente para registros de facturación pero pueden ser usados también como identificadores. Además del valor SID, este campo puede también contener el número del switch que el id number. Este id number no es requerido, pero el SID y en numero de switch están registrados y se usan en combinación con el SWID.

3.1.-REGISTRO EN UN MSC NUEVO

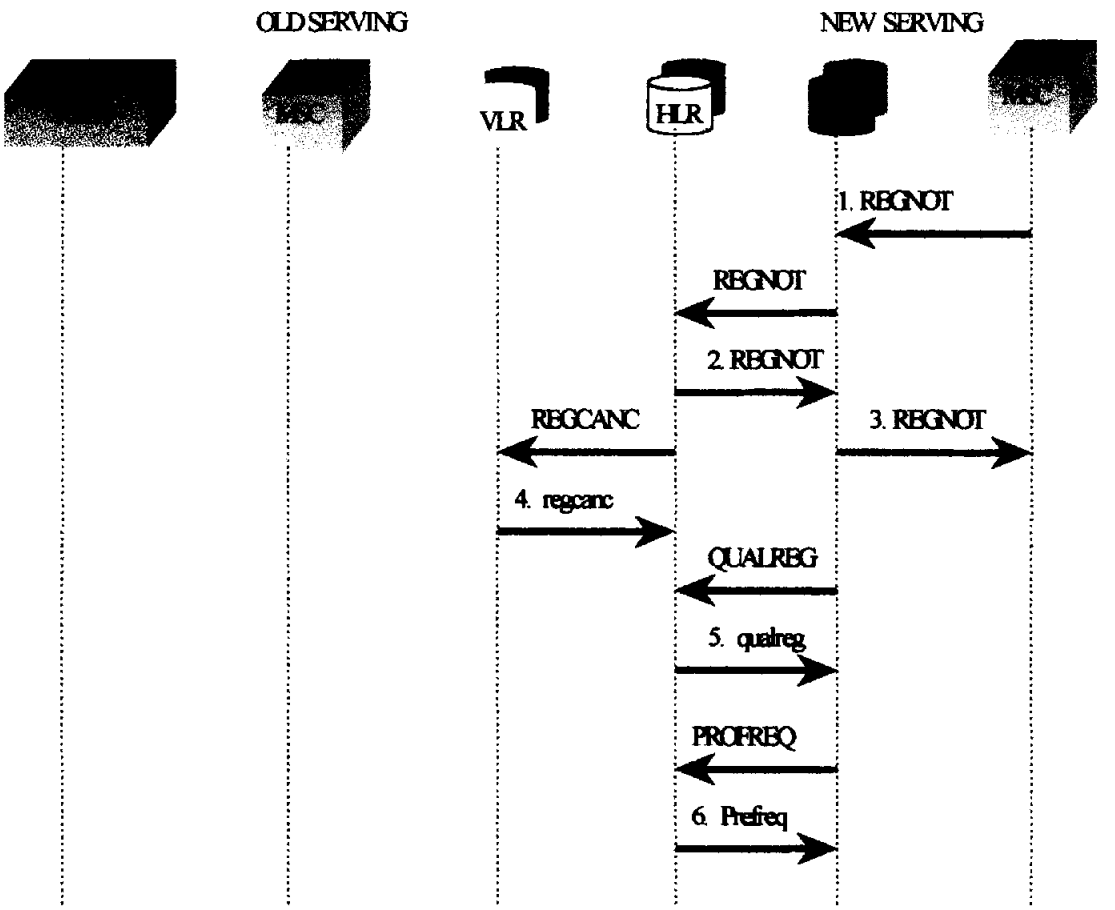
Cuando el MS se mueve a una nueva localidad, IS-41 se invoca para coordinar las especificaciones entre los viejos MSC y VLR. Los nuevos MSC y VLR y su subscriptor HLR, La figura muestra las operaciones para un registro MS en nuevo MSC. Después de que la MSC haya determinado que el MS esta en su area envía un mensaje de la notificación del registro a su VLR (evento 1). Este mensaje continúe:

a. 10 dígitos del numero de identificación del móvil (MIN)
b. 32 bits del numero de serie del móvil (MSN)
c. El código de calificación de la información.
d. Un código del tipo del sistema (un código que identifica al vendedor del sistema AT&T, Motorola, etc.)
e. 3 bits que identifica el sistema especifico que incluye el registro SID.

Si la estación se había colocado previamente con un MSC que esta dentro del dominio del VLR , el VLR no toma ninguna otra acción excepto para asegurarse que la MSC que a la estación móvil este registrado correctamente, en este ejemplo el (evento 2), el VLR envía un mensaje de notificación de registro a su suscriptor HLR este mensaje contiene el MIN y el MSC , sobre la recepción de una respuesta del HLR, el nuevo VLR de nuevo una respuesta a la nueva MSC (evento 3).El evento 4, el HLR envía un mensaje de la cancelación del registro al viejo VLR si la estación a sido colocada a otra parte, este mensaje contiene el mismo tipo de información que el

mensaje de notificación de registro, este mensaje puede ser enviado por el HLR en algún tiempo después, este es recibido por el nuevo VLR. El evento 5 y 6 puede o no puede ocurrir, dependiendo de la implementaron actual. En cualquier evento el nuevo VLR registra el nuevo MS, en el evento 5 es invocado por el VLR envía un mensaje con la calificación de la petición. El propósito de este mensaje es autentificar la estación y determinar los requerimientos de validación, en el evento 6 el VLR puede también enviar una respuesta del perfil del servicio a HLR, para dar mas información al MS. La respuesta esta petición contendrá la información que pertenece a las llamadas creadas, y parámetros referentes a las llamadas perdidas y las llamadas en espera.

REGISTRANDOSE CON UN NUEVO MSC



LOCREQ	Location request message
PROFREQ	Service profile request message
QUALREQ	Qualification request message
ROUTEREQ	Rounting request message

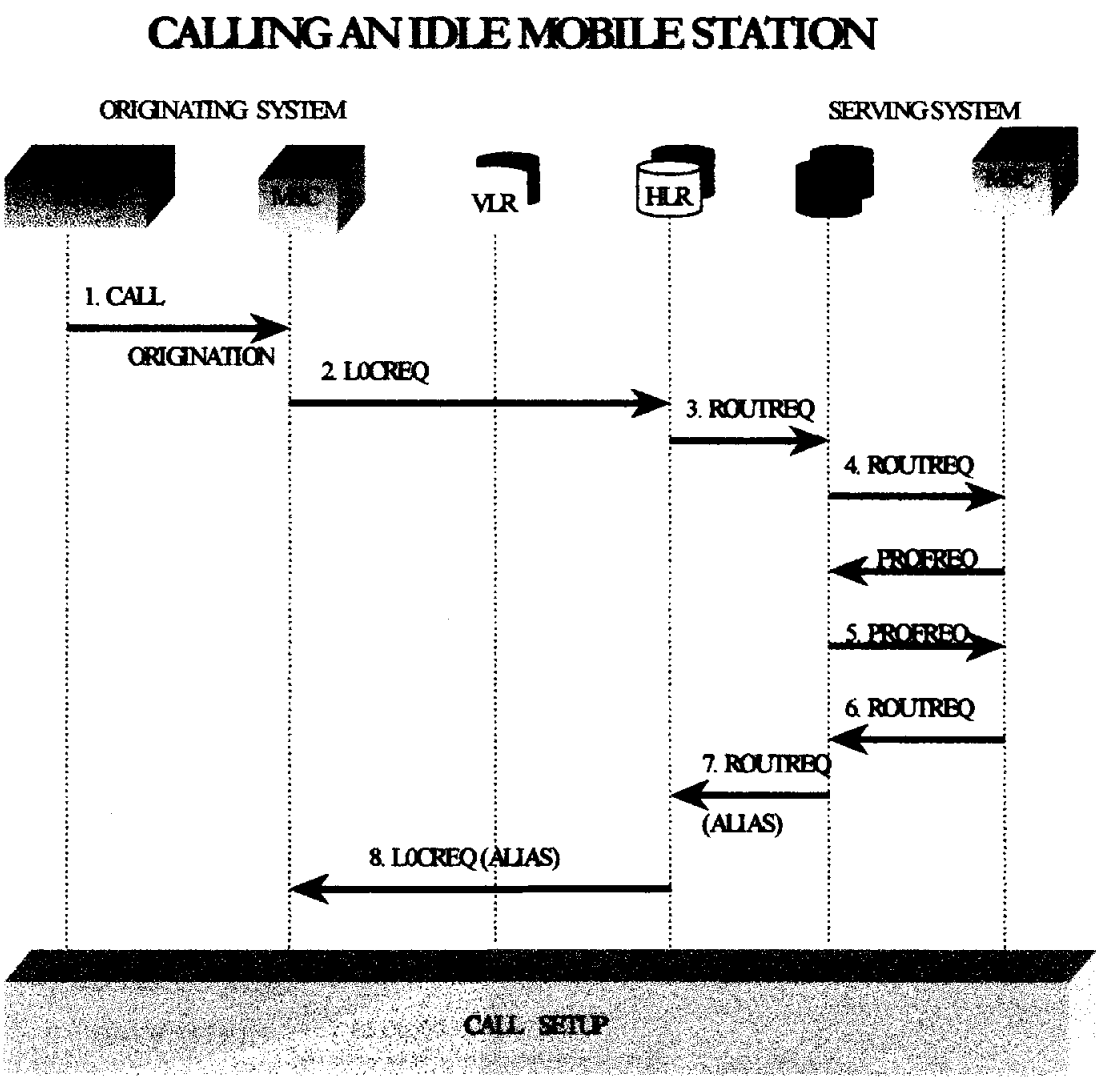
3.2.-LLAMADA A UNA ESTACION MOVIL LIBRE EN UN SISTEMA VISITADO

La figura muestra un ejemplo de una llamada hecha a una estación móvil que esta fuera del area de servicio de un MSC el cual participa en la originación de una llamada. En este ejemplo, la estación móvil no esta ocupada. La llamada tiene lugar a través de la red convencional PSTN y es enviada al sistema MSC originador a través del numero directorio identificador de la estación móvil. En el evento 2, el MSC originador envía un mensaje de Location request invoke al HLR que se asocia a la estación móvil. Una vez mas esta asociación es hecha a través de los dígitos marcados del móvil. Estos dígitos pueden ser o no el MIN.

El HLR realiza varios chequeos de validación para estar seguro de que el abonado es legitimo y que el reenvío de la llamada esta permitido. Si todo va bien, en el evento 3 el HLR envía un mensaje de Routing Request Invoke al ultimo VLR que dio información de localización del abonado. Esta información ha sido provista tempranamente por el VLR a través del mensaje de Registration Notification. El VLR reenvía este Routing Request al MSC-V actual. El VLR debe conocer que la estación móvil habría estado rondando dentro del dominio del VLR servidor y si es así la estación ya ha reportado de la nueva localización a través del MSC servidor.

Si el MSC aun no ha obtenido información acerca de esta estación móvil, esta puede obtener el perfil de servicio de la estación móvil a través del VLR. El perfil de servicio debería ser conocido también por el MSC, en caso de que esta información no se necesite. Este ejemplo muestra al MSC enviando un profile request al VLR con el VLR respondiendo con un result (evento 5). En el evento 6, el MSC responde al VLR con el profile request result que fue pedido en el evento 4. En el evento 7 el VLR del MSC servidor localiza una ruta alias y retorna esta información al HLR en un mensaje de routing request response. Una vez recibido este mensaje, el HLR construye un location request response para dársela al MSC originador (evento 8). Esta operación se realiza poniendo los valores del MIN y ESN en el mensaje de location request response. Una vez que el MSC originador recibe esta información del HLR, este establece una interface de voz hacia el MSC servidor, usando el protocolo existente como es el SS7.

El MSC originador realiza esta troncal a través del routing alias que es especificado en el location request response que le vino del HLR.

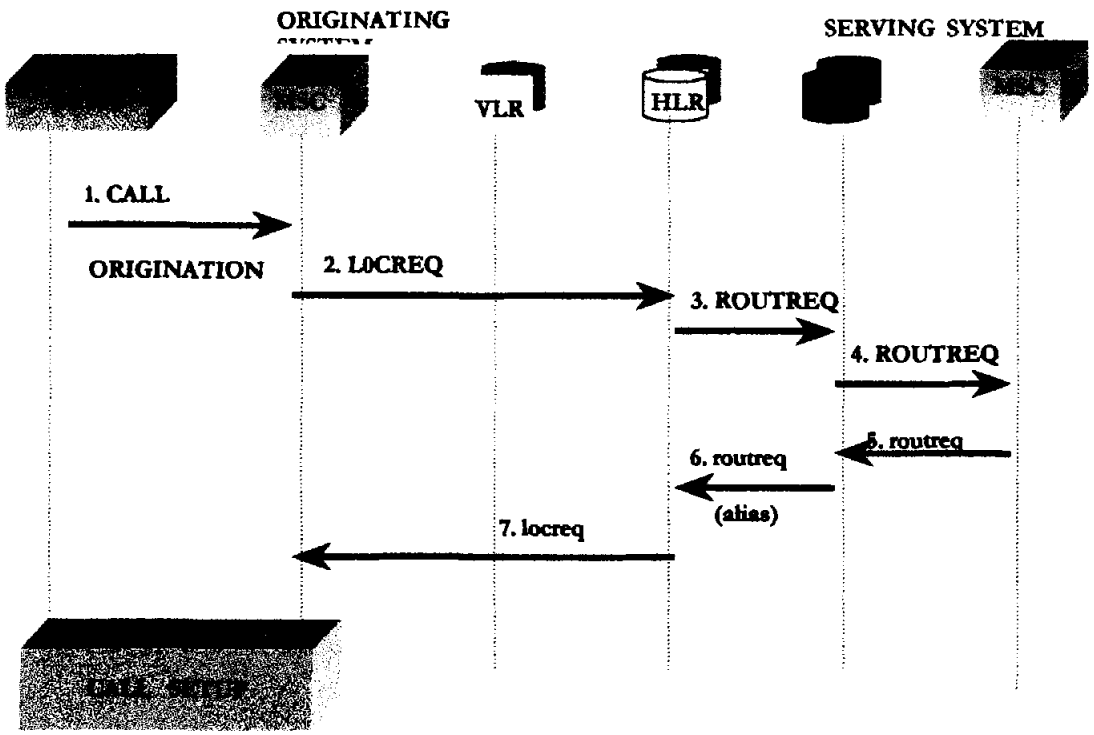


3.3.-SECUENCIA DE UNA LLAMADA EN UNA ESTACION MOVIL OCUPADA.

Si la estación móvil esta ocupada cuando una llamada es dirigida a ella, la operación procederá como se describió en la sección previa (evento 1 – 4 de la figura anterior), con las siguientes alteraciones presentada en la figura. El servidor MSC, sobrechequea sus listas internas y determina que la estación móvil esta ocupada con otra llamada.

Este chequea los resultados con el envío del mensaje de estado ocupado (estación móvil) al servidor VLR (evento 5), y entonces al HLR en un mensaje de respuesta a la ruta requerida (evento 6). El HLR observa en el perfil de la estación móvil y determina que (en este ejemplo) no tiene ninguna determinación especial privilegiada (bloqueo de llamada etc.) y retorna una señal de estado ocupado al originario MASC en el requerimiento de respuesta de localización (evento 7) lo que significa que el originario MSC debe retornar a una indicación ocupada al llamamiento PSTN (evento 8).

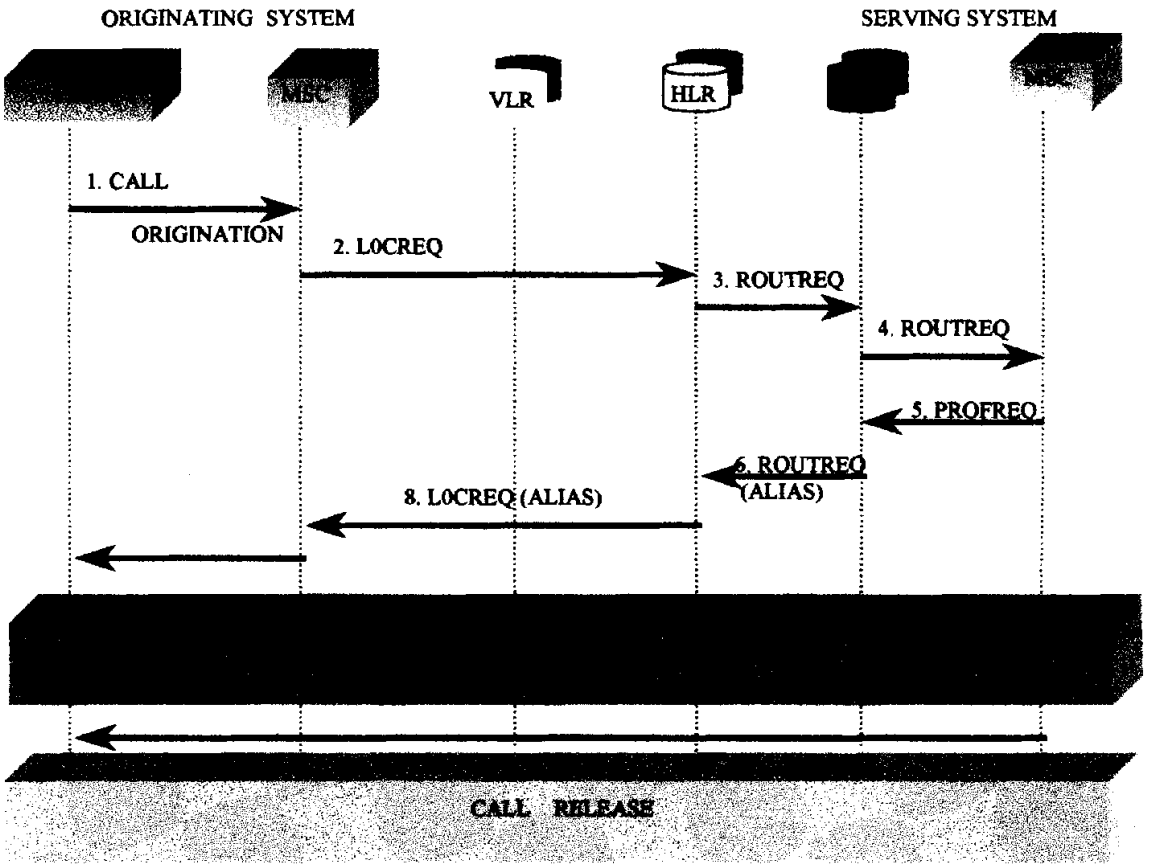
MOBILE STATION IS BUSY



3.4.-SECUENCIA DE LLAMADA SIN RESPUESTA

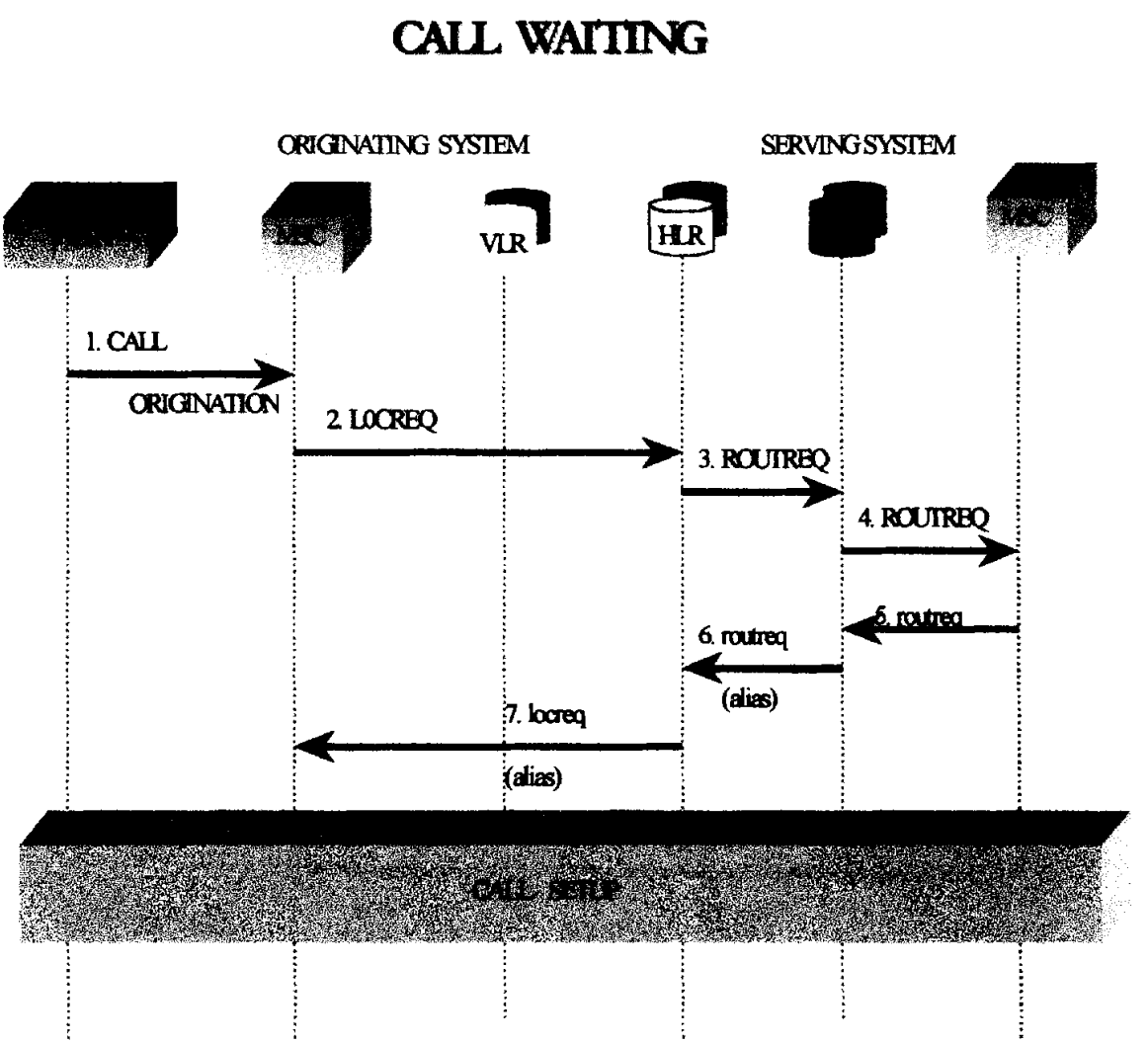
La figura presenta las acciones cuando la estación móvil no envía de regreso la respuesta búsqueda o no contesta a un mensaje de control. Recogemos las actividades en el evento 6. El servidor MSC determina que la estación móvil esta desocupada y retorna a una ruta alias al HLR en la solicitud de respuesta de mensaje. El HLR entonces añade el MIN y el ESN a su información de enrutamiento y retorna un LOCREQ (requerimiento de mensaje de localización) con el alias al MSC original (evento 7). Después de que estos procedimientos de registro han sido completados, la llamada es recibida en el servidor MSC el cual esta representado en la figura como la puesta o arreglo de operación de la llamada. En este ejemplo la estación móvil no responde a un mensaje de pagina, ni al mensaje de alerta. Por lo tanto el servidor MSC, en el evento 8, encamina la llamada al originario con a una apropiada señal (la satisfacción actual de la señal depende de la naturaleza del sistema implementado). La llamada es desconectada con la operación descrita en la figura 7.9 como llamada libre.

SECUENCIA DE UNA LLAMADA SIN RESPUESTA



3.5.-CALL WAITING (LLAMADA EN ESPERA)

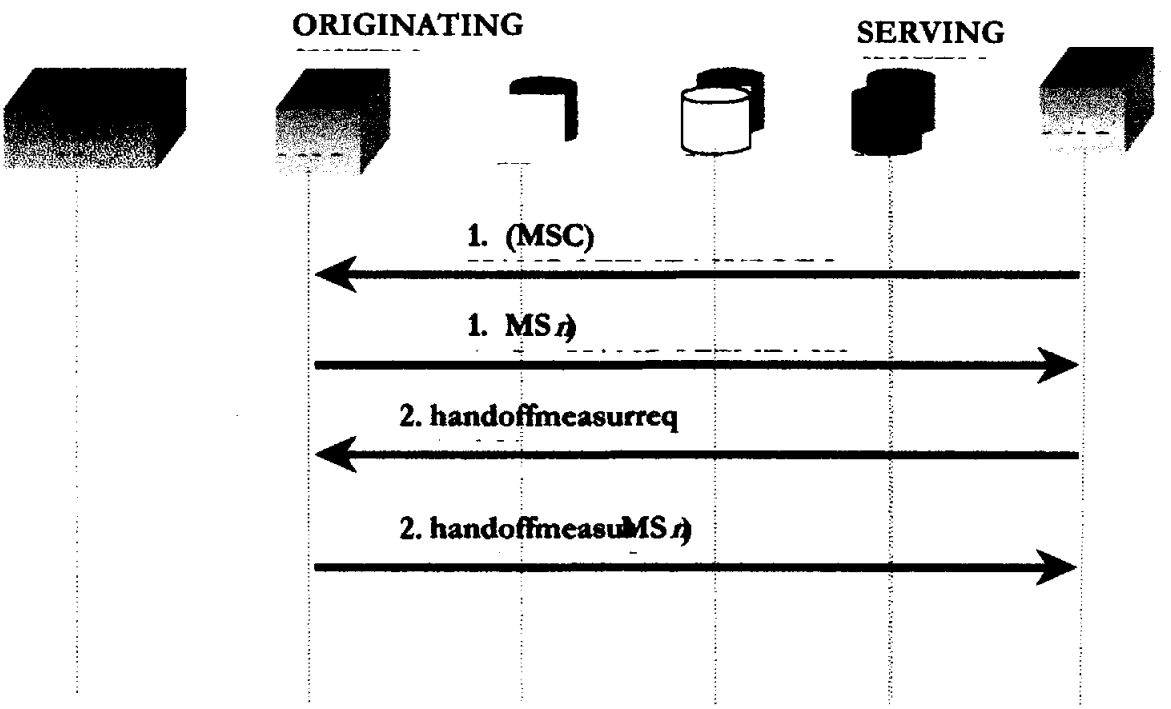
Los procedimientos de llamada en espera son mostrados en la figura. Nosotros recogemos estas operaciones en los eventos 5,6 y 7. Se aprendió tempranamente que el MSC puede descubrir que una estación móvil esta ocupada. Además examinando el perfil de servicio de esta estación se puede determinar si esta ha sido activada para una llamada en espera. En el evento 6 el servidor MSC retorna esta información hacia la ruta del HLR solicitada en un mensaje de respuesta. En el evento 7 el HLR ejecuta sus propias OPERACIONES DISCUTIDAS EN EJEMPLOS ANTERIORES. La llamada arreglada toma lugar con las operaciones convencionales descritas anteriormente. Cuando la segunda llamada llega al MSC-V el servicio móvil recibe la llamada amenazante en espera del MSC como muestra en la figura.



3.6.-PEDIDO DE MEDIDA DEL HANDOFF

Un servidor MSC puede dudar de sus MSC adyacentes para determinar si el sistema móvil podría ser relocalizado hacia otro sistema servidor. Esta operación es realizada con el cambio de los mensajes de pedido de medida del handoff, como esta descrito en la figura 7.17. En el evento 1 el servidor MSC envía a sus MSC adyacentes el nivel de pedido de medida sobre un canal especifico. El pedido de medida incluye una marca de estación de clase (SCM) campo de la estación suscriptora, el identificador de la celda servidora para el canal especifico, el código de color del SAT, el código de atenuación móvil de la voz y él numero de canal especifico. Estos campos son descritos en él capitulo de AMPS. En el evento 2 los MSC adyacentes responden con la respuesta del pedido de medida de handoff, los cuales contienen el identificador de la celda de respuesta y la calidad de la señal (señal fuerte) que esta siendo recibida por el canal especifico. El servidor MSC examina cada respuesta para determinar si un handoff es o no apropiado.

HANDOFF MEASUREMENT REQUEST



4.- Revisiones del protocolo IS-41

A medida que a pasado el tiempo desde su creación se han creado diferentes revisiones entre las cuales tenemos:

1. IS-41 Revisión 0
2. IS-41 Revisión A.
3. IS-41 Revisión B.
4. IS-41 Revisión C.
5. IS-41 P

4.1.-IS-41 REVISION 0

- ***Intersystem call handoff***
- ***Roamer Validation***

- **Intersystem call handoff.-** es un proceso por el cual una llamada activa en un canal de radio bajo el control de un MSC servidor es automáticamente transferido a un canal diferente de radio bajo el control de otro MSC sin interrupción de comunicación. En otras palabras, un abonado que hace roaming desde un area de servicio a otra sin ninguna interrupción a su llamada celular.

- **Roamer Validation.-** es un procedimiento general mediante el cual se autentifica la cuenta del abonado establecido. Es usado solo para Follow Me Roaming (FMR)

4.2.-IS-41 REVISION A

Todas las propiedades de IS-41 revisión 0, más

- ***Automatic Roaming***
- ***Call delivery***
- ***Remote Feature Control***
- ***Call Forwarding***
- ***Three-way Calling / Conferencing***
- ***Call waiting***

- **Automatic Roaming.-** permite a un abonado , sin importar su situación , a hacer llamadas automáticamente desde cualquier lugar dentro de la red celular.

- **Call Delivery.-** es un proceso por el cual las llamadas dirigidas a un abonado celular son entregadas mientras este esta haciendo roaming a un area de servicio visitante. Esta capacidad requiere que el MSC-O (usualmente el MSC-H) , el HLR y el MSC-V estén conectados en red.

- **Remote Feature Control.-** es la capacidad de un abonado móvil de activar o desactivar propiedades disponibles desde el Sistema Visitado usando Los códigos de propiedades asignados para este uso. Los clientes móviles tendrán acceso a las propiedades de su MSC-H y de cada MSC-V usando Los mismos códigos de propiedades.

- **Call Forwarding.-** provee la capacidad de redireccionar una llamada a un lugar diferente o un numero móvil diferente cuando el sistema móvil esta ocupado o fuera del area de servicio.

- **Three-way calling / conferencing.-** permite a un abonado a hablar con dos personas mas al mismo tiempo.

- **Call waiting.-** provee a un abonado la capacidad de tener un indicador de una llamada entrante cuando ya tienen una llamada en proceso.

4.3.-IS-41 REVISION B

Todas las propiedades del IS-41 revisión A, más:

- ***Dual-mode handoff***
- ***Control of vertical features after handoff***
- ***Global title traslations (GTT)***

- **Dual-mode handoff.-** Dual-mode handoff es un proceso por el cual se hace un handoff desde un modo análogo a un modo digital, o digital a digital, o digital a análogo.

- **Control of vertical features after handoff.-** Cuando una llaman es trasladada a otro sistema, el switch local continua controlando las funcionalidades de propiedades verticales, como es el call forwarding, call waiting y conference calling. Entonces, si un abonado móvil tiene capacidad de conference calling en su sistema local y es trasladado a un sistema que no soporta call forwading, el servicio no se afecta. Si el usuario esta haciendo una conferencia , el traslado es transparente, por que la propiedad continua siendo controlada por el MSC-H

- **Global title traslations.-** Un Global Title (GT) es una aplicación de información , como los dígitos que se ha marcado, esto no provee información de ruteo. Esta aplicación GT usa las capacidades del Global title Traslations (GTT) para cambiar el GT a una dirección ruteable. Mas específicamente en celulares, el GT permite al VLR pedir la información del perfil del abonado de un HLR sin conocer el código del puntero en el HLR. Con IS-41 revisión B y mejores, el VLR usa el MIN del abonado como GT. El VLR envía el MIN al Singnaling Transfer Point (STP) pidiendo que el GTT lo transforme. El STP traduce el GT (MIN) en un código de puntero y un numero del subsistema para poderlo buscar el HLR.

4.4.- IS-41+ (Nortel Propietary)

Todas las propiedades de IS-41 revisión B , más :

- ***Roaming do not disturb (RDND)***
- ***Status information***
- ***Answer after intersystem handoff***
- ***Network boundary paging***
- ***Verify authorization code***
- ***Billing request***
- ***Message tandeming***

- **Roaming do not disturb Cancellation (RDND).-** es una propiedad vinculada con la propiedad de Call delivery (CD) . Esta permite a Los abonados de un MTX (MSC en Nortel) que tienen línea con CD a temporalmente desactivar esta propiedad. Entonces cuando RDND esta activo , el CD esa inactivo , y cuando el RDND esta inactivo el CD esta libre de operar. Por default , RDND esta inactivo, entonces el CD operará hasta que sea específicamente desactivado por el usuario. Cuando el RDND esta activo solo inhibe la operación de CD. No inhibe la entrega de llamadas del MSC remoto y el abonado esta habilitado a hacer llamadas.

- **Status information.-**El mensaje de Status Information provee información de estatus (por ejemplo el número de llamada entrante) al MSC-S desde el MSC-A/VLR después del intersystem handoff.

  Entonces si el MS recibe un mensaje de correo de voz , .Después de hacer un intersystem handoff , el Status information Message es enviado al MSC-S para informarle que el MS que tiene un mensaje esperando en su casilla.

- **Answer After Intersystem Handoff.-**Permite a un MS que esta sonando con una llamada entrante a hacer un intersystem handoff (IHO) sin que deje de sonar el MS. El Standard IS-41 asume que el MS es el originador de la llamada en el MSC-V, por lo tanto será el MS el que termine la llamada. Entonces el MS esta habilitado para hacer un IHO mientras esta sonando sin peligro de que deje de sonar. Una vez

que el MS hizo en IHO este contesta y un answer messages es enviado hacia el MSC-A indicando que el MS ha contestado y que se puede empezar la tasación.

- **Network Boundary Paging.**-Cuando se intenta rastrear a un MS , el area de servicio por donde se empieza a buscarlo es el MSC al cual MS se registro por ultima vez; entonces, habrá una situación en donde dos diferentes MCSs convergen en áreas adyacentes donde el MS tiende a quedarse por un largo periodo (un MS permanece en un area de sobreposicion de coberturas por un tiempo muy extendido, causando que la información de su localidad sea incorrecta) . En esta situación es posible que existan 3 casos de falla , los mismos que se detallan a continuación:

  1. Si el MS fue sintonizado en un CCH (canal de control) de un MSC , pero actualmente entra en un area de servicio de otro MSC , cuando el MS recibe el rastreo , este sé resintoniza al nuevo CCH (que es mas fuerte) y envía un mensaje de respuesta del rastreo al nuevo MSC . El nuevo MSC no ha sido avisado de la llamada del MS y la terminación falla.
  2. Si un MS es resintonizado al CCH del nuevo switch pero no ha recibido todavía el mensaje de global action registration , entonces la terminación falla por que el MS nunca oye el mensaje de rastreo.
  3. Si un MS es sintonizado a un CCH en un MSC y dentro del rango de un CCH de otro MSC, entonces la mitad del tiempo cuando el MS se registra y ambos CCHs escuchan al MS, la localidad del MS es almacenada incorrectamente.

  Network Boundary Paging nos da la capacidad de enviar un mensaje de respuesta dirigido al MS cuando una respuesta de rastreo inesperada es recibida. Esto significa que cuando el caso #1 ocurra, al MS es enviado un mensaje de respuesta directo diciéndole que sé resintonice al CCH que originalmente envío el rastreo.
  Esto da el efecto de conectar al MS a la celda original donde fue sintonizado, para todos esos MSs a los cuales la señal de la celda original es suficientemente fuerte, esto provee una respuesta exitosa al problema de rastreo de celdas aun estando lo suficientemente cerca de su celda original, la cual tiene un nivel de señal aceptable.

- **Verify Authorization Code.**-Mandatory Authcode Collection (MAC line option) permite a un MS especificar de tres a siete dígitos que tienen que ser ingresados y

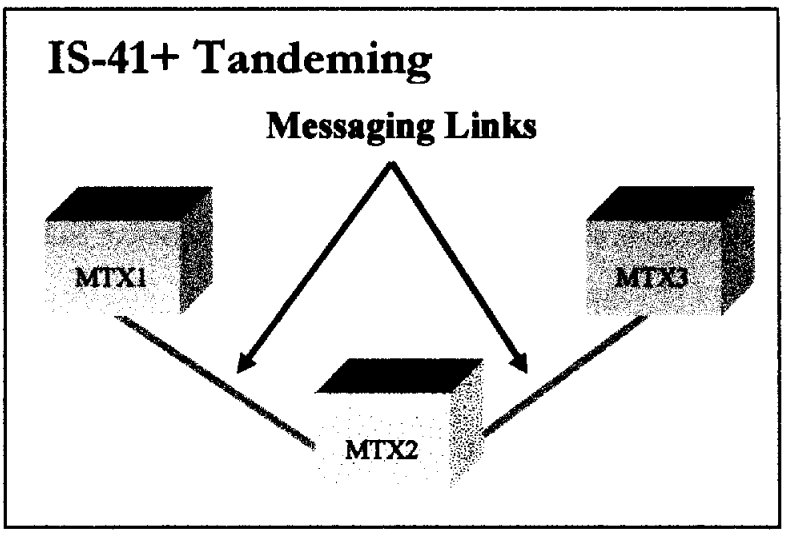
verificados cada vez que el MS origina una llamada. Esto permite al abonado MS restringir el uso no autorizado de su MIN y SNR.

Cuando un MS esta haciendo roaming el mensaje de Verify Authorization Code es enviado al HLR por el MSC servidor para verificar el código de autorización antes de originar llamadas.

- **Billing Request.**-El mensaje de Billing Request es usado por un CSN para comunicar información de facturación al MSC-O/S por llamadas en donde el CSN esta involucrado en algún punto. La información de facturación llega en forma de un parámetro indicador de servicio IN en el mensaje. El CSN relaciona la llamada y el MS para asociarlos con el Billing Request message incluyéndole un Billing ID y el MIN del MS.

4.4.1.-Tandeming

Tandeming network messages a través de MTXs es una función propietaria de Nortel. Esta funcionalidad fue introducida para ahorrar a la compañía operadora la Instalacion de enlaces adicionales. La figura ilustra tres switches en red vía tandeming y esto es usado a lo largo de esta sección.



MTX1 esta habilitado para enviar networking messages a MTX2 a través de una conexión directa entre estos dos switches. En este orden para que MTX1 envíe networking messages a MTX3 estos deben ser enviados a través del tamdeming de MTX2 ya que no existe conexión directa con MTX3.Con la mensajería de IS41P cada nodo en la red tiene un único MSCID asociado con él . IS41P no requiere que el MTX tenga una entrada en el campo SYSCON por cada nodo en la red. La Tabla SYSCON se refiere como la tabla de rutas. Cada MSCID con el que el MTX pudiera comunicarse vía IS41P tandeming , debe ser ingresado en la tabla MSCIDRTE. La tabla MSCIDRTE asocia el MSCID con una ruta definida con SYSCON.

Los mensajes en el tandeming son enviados de dos formas. La primera forma es usando como destino el MSCID en el Paramento de Mensajes de Rutas. El procesamiento de estos mensajes en Los nodos intermedios es simplemente mira el destino MSCID y redireccionar el mensaje , de acuerdo con el MSCIDRTE, cuando el MSCID no corresponde con ninguno en la tabla es el propio MSCID.

La segunda forma para el tandeming es hecho mediante el MIN que esta en el mensaje. Esto es solo invocado por mensajes que son destinados para el HLR. La razón por la que el MIN es usado en vez del Parámetro de Mensajes de Rutas es por que el destino MSCID no siempre esta disponible y es veraz , y el MIN esta siempre disponible y es veraz.

Para otro tipo de mensajes , el destino MSCID es conocido, entonces el ruteo de mensajes es usado. El nodo tandeming mira el MIN en el mensaje invocado y después mira en la tabla de SERVCNG . Si el MIN en la tabla SERVCHNG no es LOCAL roamer , entonces Los mensajes son forwardeados de acuerdo al campo HLRRTE en la tabla SERVCHNG. El MS ha contestado , un answer messages es enviado al MSC-A indicando que el MS ha respondido y la facturación empieza.

4.5.-IS-41 REVISION C

Las especificaciones del IS-41 REVISION C contienen modificaciones e innovaciones significantes sobre la IS-41 revisión B. Un área significante en las innovaciones es el Modelo propio de red de la IS-41 revisión C, la cual representa la funcionalidad de las entidades y asocia interfaces definidas dentro de las especificaciones que comprometen lógicamente a la red celular.

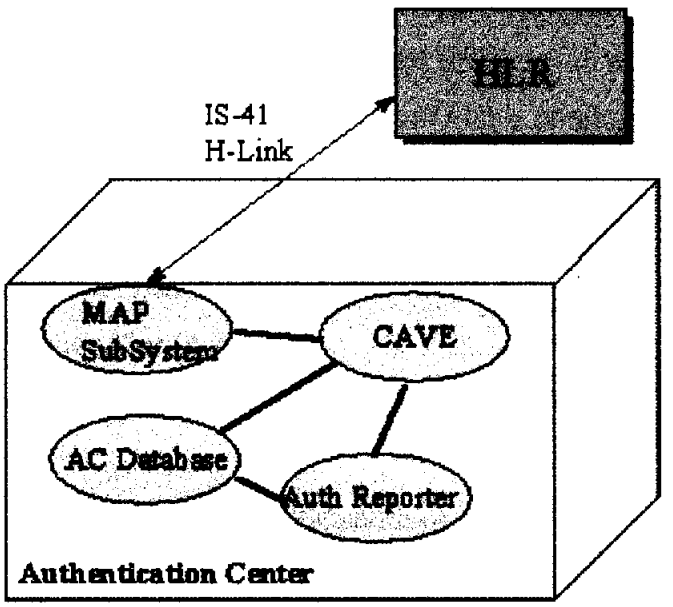
La interface IS-41 C provee sucesos basados en el mecanismo para la comunicación con la plataforma del hardware produciéndose así cambios en algunos parámetros y mensajes de las ultimas versiones.

Dentro de estas especificaciones, las operaciones de mensajería son definidas primero, luego las usaremos para construir secuencias completas de mensajes o escenarios. En esta parte primero definiremos las operaciones de mensajería usados por el Celular Autentificación Center, que combinadas estas operaciones crearemos los escenarios de autenticaciones, así como también veremos el Centro de Mensajes Cortos

5.- CENTRO DE AUTENTIFICACION

La característica de la autentificación es una capacidad de la red que permite que las redes celulares validen la identidad los teléfonos de tal modo reduzcan el uso desautorizado de redes celulares. El proceso es transparente a los suscriptores.

Mas adelante explicamos de manera general el proceso de autentificación y describimos cómo coordinar la autentificación entre los diferentes MSCs , para lo cual debemos de acotar algunos conceptos importantes para el entendimiento de este.



- **La A-Key**

La clave de autentificación (A-key) es un valor secreto que es único en cada teléfono celular. Este es registrado por el proveedor de servicios celulares y almacenado en el teléfono y en el centro de autentificación (AuC). El A-key es programada en el teléfono por el fabricante. Este puede ser también ingresado manualmente desde el menú del teléfono, o por un terminal especial en el punto de venta. El teléfono y el aun deben tener el mismo A-key para producir los mismos cálculos. Los A-keys nunca son enviados por la interface aérea o la red SS7. El usuario no debería estar habilitado de mostrar del A-key en el teléfono. La función primaria del A-key es ser usado como parámetro para calcular el SHARED SECRET DATA (SSD).

- **El Algoritmo CAVE**

CAVE mantiene la autentificación celular y la encriptación de voz. CAVE es un algoritmo para calcular varios elementos usados en la autentificación, como son las respuestas de recusación y los SSD. Este puede ser usado eventualmente para encriptar canales de voz, pero el uso primario del CAVE no incluye la encripción de voz.

- **El Shared Secret Data (SSD).**

El SSD es usado como una entrada para los cálculos de autentificación en el teléfono y en el AC, es almacenado en ambos lugares. El SSD puede ser modificado sobre la red. Puede ser enviado a través de la red SS7 pero no puede ser enviado sobre una interface aérea. El centro de autentificación (AC) y el teléfono móvil comparte 3 elementos que van en él calculo del SSD:

1. el Electronic Serial Number (ESN)
2. El Authentication Key (A-Key)
3. Un numero aleatorio para él calculo del SSD (RANDSSD)

El ESN y el RANDSSD son transmitidos a través de la red y a través de interfaces aéreas. El SSD es actualizado cuando el teléfono hace su primer acceso al sistema, y periódicamente después de eso. Cuando el SSD es calculado, da como resultado dos valores por separado, SSD-A y SSD-B. SSD-A es usado para la autentificación. SSD-B es usado para la encripción y privacidad de voz.

Dependiendo de la capacidad del sistema servidor, SSD puede ser compartido o no entre el Centro de Autentificación y el Centro de Conmutación de servicio móvil (MSC). Si datos secretos son compartidos, esto significa que el AC enviara esto al MSC servidor y el MSC servidor debe de estar en la capacidad de ejecutar el algoritmo CAVE. Si no es compartido, el AC mantiene los datos para sí mismo.

Las formas de compartir afecta como una recusación de autentificación es conducida. Con datos secretos compartidos, la recusación es manejada por el MSC servidor. Con datos secretos no compartidos, la recusación es manejada por el AC. Para datos secretos compartidos, se puede minimizar él trafico enviado a través de los enlaces SS7 y hacer que las recusaciones sean más rápidas en el MSC servidor.

- **Subsistema MAP**

Este componente se comunica con el HLR usando una H-link. El subsistema MAP puede utilizar el TCP/IP, el X.25 o una link SS7 en el centro de la autentificación.

- **Base de datos De la CA**

La base de datos de la CA es la base de datos cifrada que mantiene el A-Key de los suscriptores, y la otra información semipermanente requerida para la CAVE

- **AuthReporter**

El AuthReporter genera los informes del estatus y de los incidentes de la autentificación. Estos informes están disponibles en la CA así como en el HLR vía la capa MAP (mensajes de IS-41 C: Authentication Failure Report, Authentication Status Report)

- **El Challenge**

El proceso de la autentificación consiste en un diálogo entre la recusación y la respuesta. Si se comparte el SSD, el diálogo se ejecuta entre el MSC y el teléfono. Si el SSD no se comparte, el diálogo se ejecuta entre el HLR/AC y el teléfono. Dependiendo del tipo del conmutador, el MSC puede ser capaz de cualquiera al Unique Challenge, un Global Challenge, o ambos. Algunos MSCs no son actualmente capaces de Global Challenge.

a) **Unique Challenge** – la recusación ocurre durante intentos de llamada o cuando una llamada termina al móvil solamente. , Porque utiliza el canal de la voz. Presenta una autentificación a un solo teléfono durante creaciones de la llamada y la salida de la llamada.

b) **Global Challenge** – la recusación ocurre durante el registro, creaciones de la llamada, y la salida de la llamada. Presenta una recusación de la autentificación a todos los MSs que estén utilizando un determinado canal de radio de control. Se llama Global Challenge porque es difusión en el canal de radio del control, y el Challenge es utilizado por todos los teléfonos que tienen acceso a ese canal de control.

5.1.-Subsistemas

La autentificación se ejecuta en mensajería de IS41C usando los subsistemas siguientes:

1. Mobile Application Part (MAP)
2. Home Location Register (HLR)
3. Visitor Location Register (VLR)
4. Mobile Switching Center (MSC)
5. Authentication Center (AuC)

Entre el HLR y el MSC, se necesita los subsistemas 1, 2, 3, y 4 activos. El subsistema 5 se utiliza entre el HLR y la AuC.

5.2.-AUTHENTICATION MESSAGE OPERATIONS

Las operaciones de mensajes son agrupadas en bloques usados para construir secuencias de mensajes más complejas. Esta parte del modulo define la autentificación celular por roaming automático.

Los siguientes mensajes TCAP de IS-41 revisión C están asociados con la autentificación:

- AUTHENTICATION REQUEST (AUTHREQ)
- AUTHENTICATION DIRECTIVE (AUTHDIR)
- BASE STATION CHALLENGE (BSCHALL)
- AUTHENTICATION STATUS REPORT [1] (ASREPORT)
- AUTHENTICATION FAILURE REPORT [1] (AFREPORT)
- SECURITY STATUS REPORT (TSB-51) (SSREPORT)

Estos mensajes logran 3 funciones básicas de autentificación. Estas funciones son:

1. Autentificación del MS
2. SSD Updating (el MS es instruido para calcular un nuevo valor de SSD)
3. Actualización del contador de historial de llamadas. (MS indica cuando incrementar el Call History Counter)

5.2.1.-AUTHENTICATON REQUEST

Una Authentication Request (AUTHREQ) es un mensaje de autentificación iniciado por el MSC para autentificar a un MS. Sí el SSD no esta compartido con el VLR, la AUTHREQ siempre ira al AC. Si el SSD se comparte con el VLR, entonces según el tipo del acceso del sistema se determinará si el VLR puede mantener el AUTHREQ o si debe ser enviado al AC.

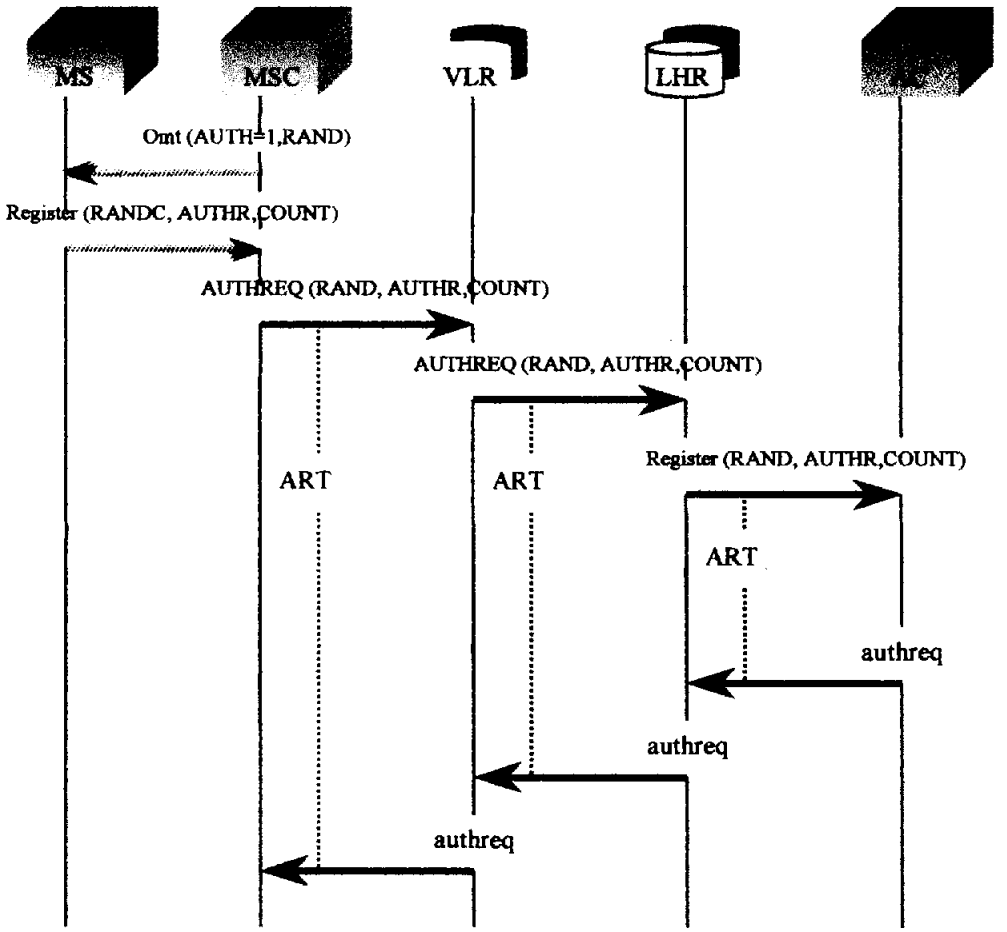
- La autentificación por control de canal de radio (MSC soporta global Challenge) que resulta en un AUTHREQ enviado por el MSC da lugar a:
    - Initial Registration (Registro Inicial)
    - Call Origination (Origen de llamada)
    - Page Response (Call Termination)

  Nota: Si el VLR tiene SSD del MS, entonces el VLR procesara la autentificación y el AUTHREQ no será reenviado al AC.

- La autentificación del canal de voz (MSC hace uso de Unique Challenge.) que resulta en una AUTHREQ enviada por el MSC dando lugar a:
    - El MSC no soporta recusación global en canal de radio.
        - Initial Registration (Registro Inicial)
        - Call Origination (Origen de llamada).
        - Page Response (Llamada en espera o conferencia de llamada)
    - Flash Request (llamada en espera o conferencia)

  Nota: Si el VLR tiene SSD del MS, entonces el VLR procesara la autentificación y hace una petición al MSC para que inicie un Unique Challenge. El AUTHREQ no se reenviara al AC.

AUTHENTICATION REQUEST



5.2.2.- AUTHENTICATION DIRECTIVE

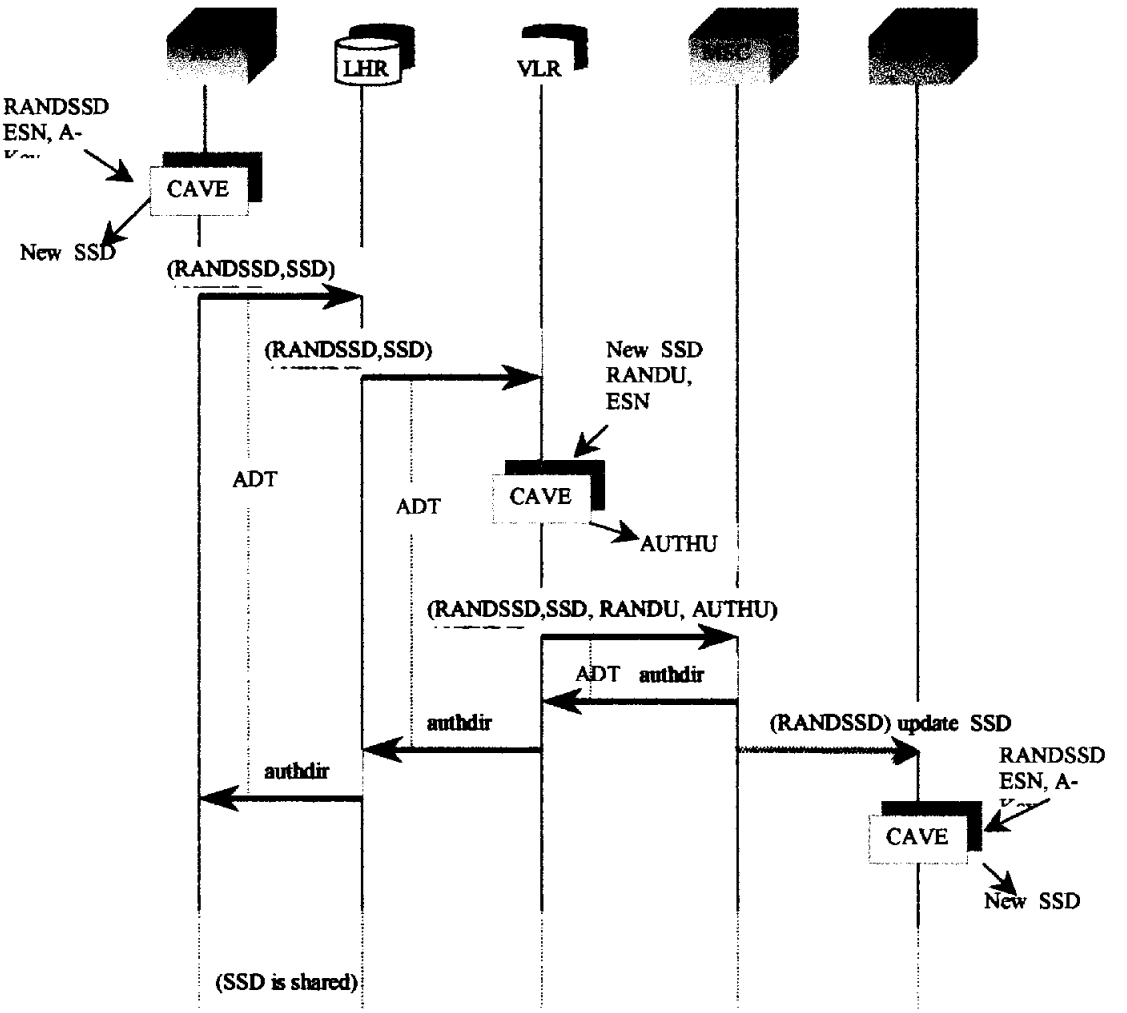
El Authentication Directive (AUTHDIR) es un mensaje de autentificación usualmente iniciado por el AuC. Si el SSD esta compartido con el VLR, el VLR puede iniciar un AUTHDIR con una petición de recusación única para el MSC que enviara al MS.

El mensaje Authentication directive inicia cualquiera de Los siguientes escenarios de autentificación de mensaje:

1. Actualización del SSD cuando el SSD esta compartido
2. Actualización del SSD cuando el SSD no esta compartido
3. VLR inicia una recusación única cuando el SSD esta compartido
4. AuC Inicia una recusación única cuando el SSD no esta compartido
5. Revocación de la comparición del SSD
6. Actualización del valor de parámetro Call History Count (COUNT)

En este ejemplo, AuC envía una AUTHDIR pidiendo al MS actualizar el SSD usado el RANDSSD como una entrada de valor aleatorio para el algoritmo CAVE. El SSD esta compartido en este ejemplo.

AUTHENTICATION DIRECTIVE



5.2.3.-BASE STATION CHALLENGE

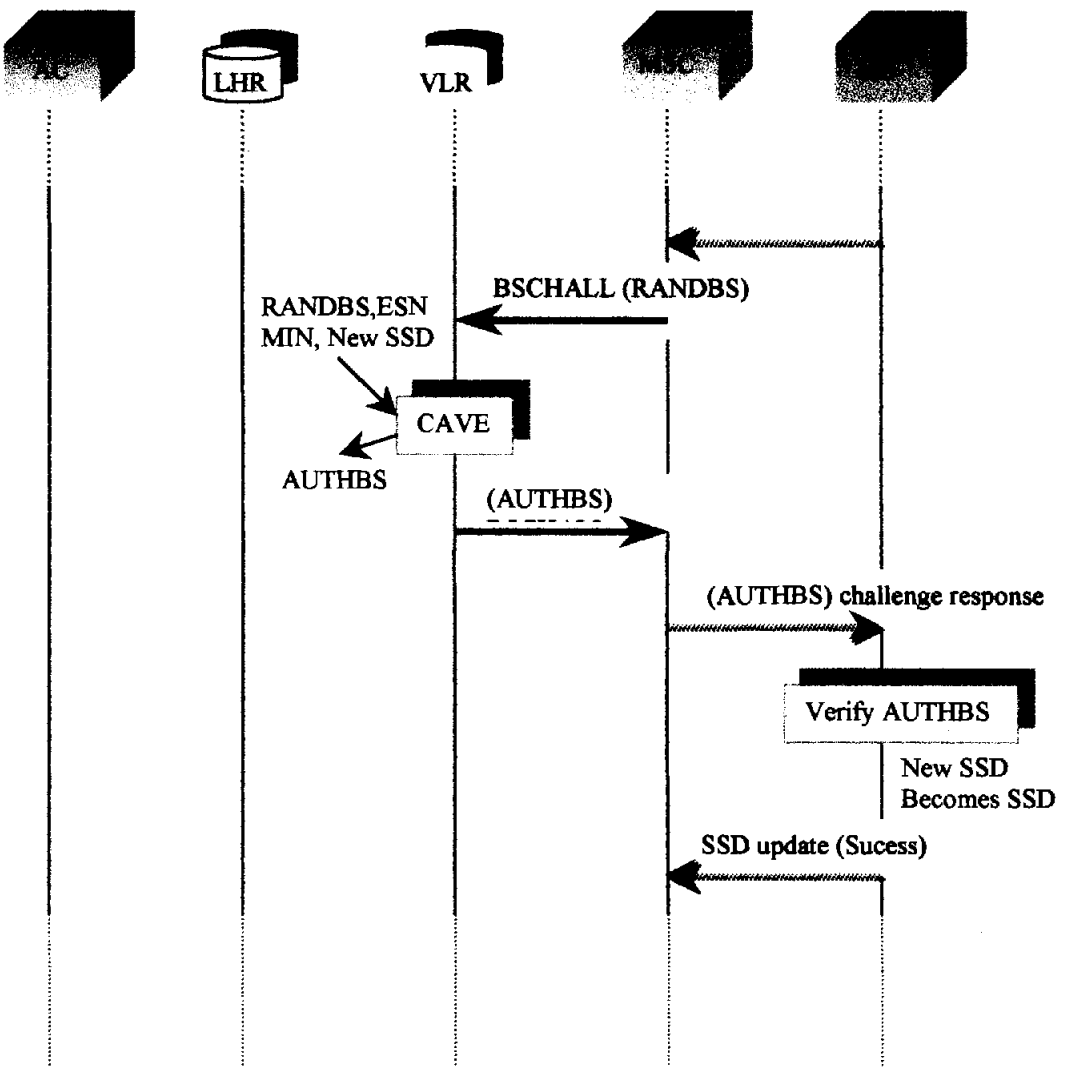
La Base Station Challenge (BSCHALL) es una secuencia de mensajes que permite al MS verificar el nuevo valor calculado del SSD

El MS usa este nuevo SSD, MIN, ESN y un numero aleatorio (RANDBS) como valor de entrada para el algoritmo CAVE. El MS envía la Base Satino Chalanee al MSC sobre la interface aérea de radio la cual contiene la entrada del numero aleatorio (RANDBS). El MSC pasa esta información al VLR en un mensaje Base Satino Chalanee (BSCHALL). El VLR usa esta copia del nuevo SSD, MIN, ESN y él numero aleatorio (RANDBS) que fue recibido del MS como una entrada para el algoritmo CAVE.

El VLR envía él numero resultante de la salida del CAVE al MSC en una respuesta BSCHALL. El MSC pasa el BSCHALL al MS sobre la interface aérea de radio.

Una vez que el MS recibe el BSCHALL desde el MSC, el MS compara el RANDBS que ha calculado con el RANDBS que ha recibido del MSC. Si Los valores coinciden entonces el MS reemplaza el antiguo SSD con el nuevo SSD. Después que el MS ha actualizado el SSD, este envía un mensaje de Successful SSD Update al MSC.

BASE STATION CHALLENGE



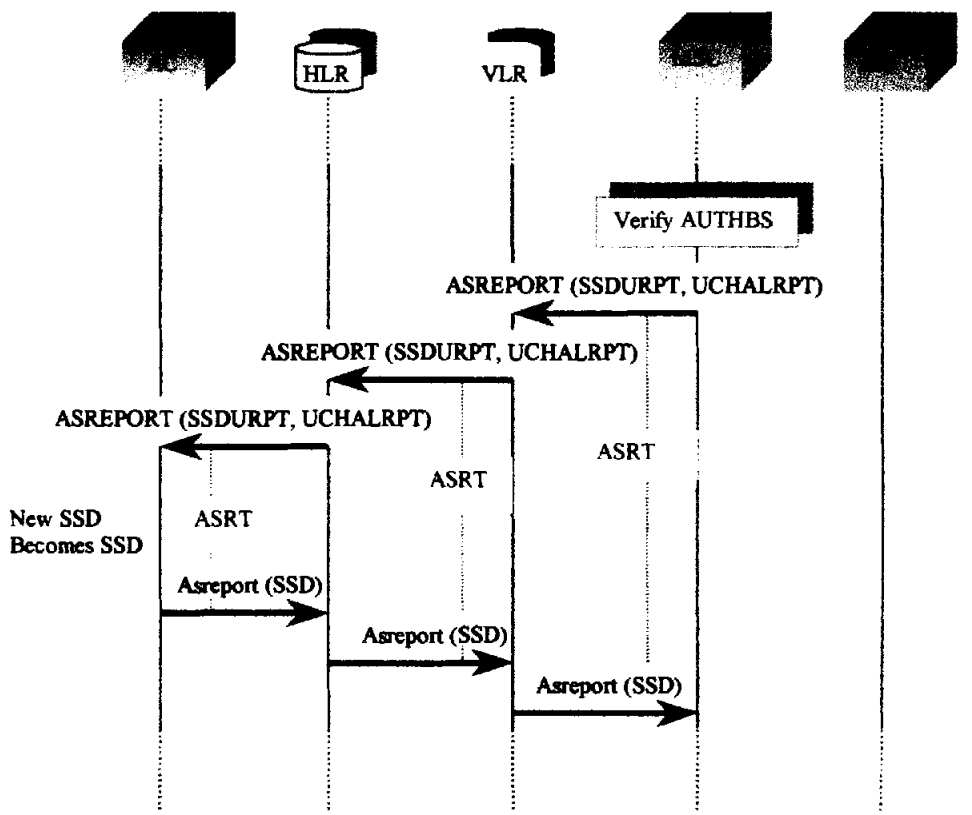
5.2.4.-AUTHENTICATION STATUS REPORT (ASREPORT)

El mensaje Autentificación Status Report (reporte de estado de Autentificación, ASREPORT) es usado para reportar la seguridad de algún evento asociado al MSC que fue iniciado por AuC o VLR.

Después de que el MSC verifique el valor del AUTHU que recibió del MS, este enviaría un ASREPORT con una indicación de suceso o no suceso para la actualización del SSD y del Unique Challenge

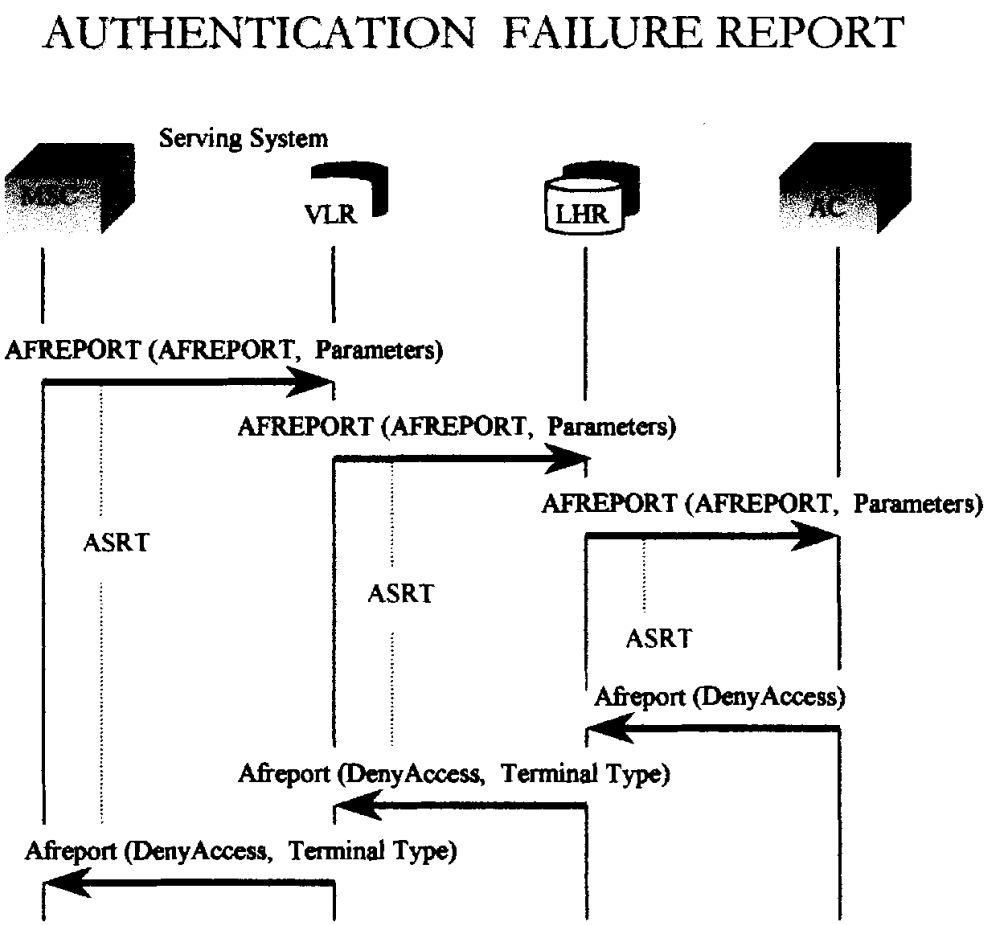
Si el ASREPORT indica que sé a completado la operación iniciada por el VLR, entonces el VLR envía de vuelta una respuesta *asreport* al MSC, en caso contrario el VLR reenviara el ASREPORT al AuC (vía HLR). El AuC retorna una respuesta *asreport* al MSC (vía HLR y VLR).

AUTHENTICATION STATUS REPORT (ASREPORT)



5.2.5.-AUTHENTICATION FAILURE REPORT (Reporte de falla de autentificación)

El Authentication Failure Report message (AFREPORT) se usa para reportar la falla de un evento de seguridad asociado con un MSC el cual no es iniciado por el AC o VLR.

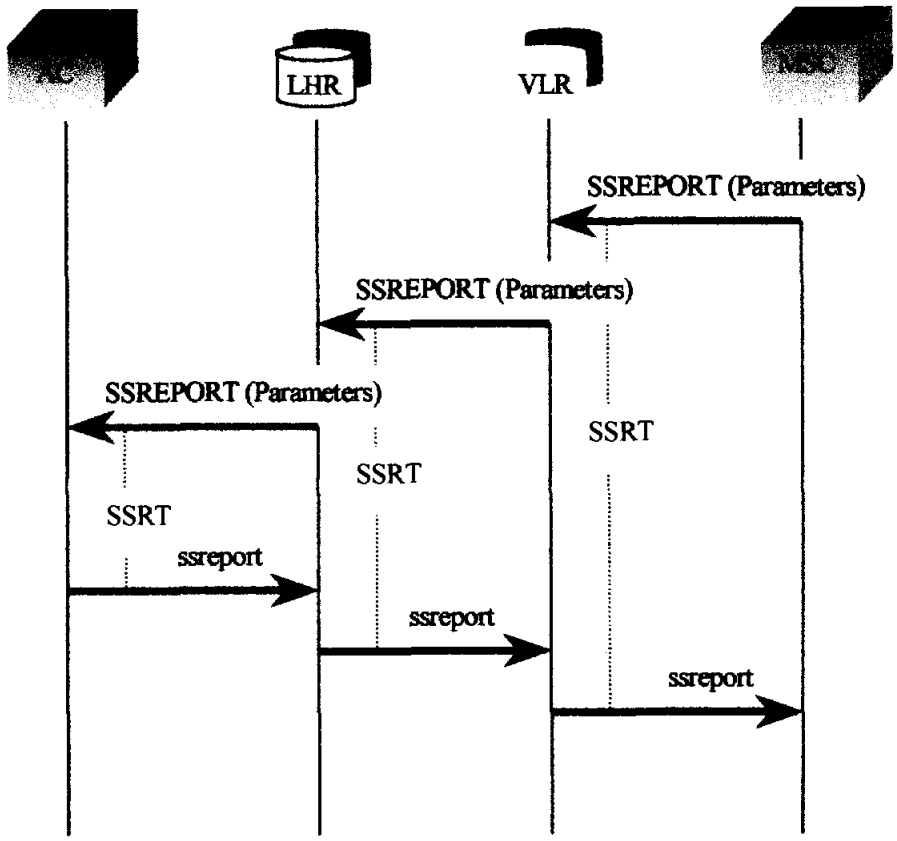


5.2.6.-SECURITY STATUS REPORT

El Security Status Report message (SSREPORT) fue definido por el Boletín de Sistemas de Telecomunicaciones #15 (TSB-51) el cual reconoce las actualizaciones y modificaciones del IS-41.

Debido a cierta confusión creada por la implementación de solo este mensaje, el SSREPORT message fue reemplazado por dos mensajes en la nueva revisión IS-41C, el mensaje ASREPORT y el mensaje AFREPORT.

SECURITY STATUS REPORT



5.3.-OPERACIONES DE LOS MENSAJES DE AUTENTIFICACION

En este momento todos las operaciones de mensajes que se aplican al Centro de autentificación ya han sido discutidas. Ninguno de estos mensajes pueden proveer autentificación por sí solos. Tienen que ser usados juntos en un flujo de mensajes para completar la autentificación celular.

5.3.1.-SECUENCIA DE MENSAJES DE AUTENTIFICACION

Ahora que conocemos los mensajes básicos de operaciones de autentificación, lo siguiente es poner todos estos mensajes juntos para manejar los diferentes escenarios.

Todas las posibles secuencias de autentificación de mensajes no se cubren en este documento. Los siguientes flujos de mensajes han sido seleccionados para ser discutidos:

- Registro Inicial con autentificación sobre canal de radio
- Originación con autentificación sobre canal de radio
- Terminación con autentificación sobre canal de radio
- Autentificación sobre canal de voz
- VLR Initiated Unique Challenge
- Actualización del SSD con SSD compartido.

5.3.1.1.-INITIAL REGISTRATION WITH AUTHENTICATION OVER RADIO

a) El MS determina del Overhead Message Train (OMT) que un nuevo sistema servidor ha entrado y que es requerida una autentificación (AUTH=1). El número aleatorio (RAND) que es usado para la autentificación también puede ser obtenido por el MS en ese momento. El MS ejecuta el algoritmo CAVE usando el SD almacenado, el ESN, el MIN y el valor RAND para producir el Registration Authentication Result (AUTHR)

b) El MS se registra en el nuevo MSC-V, enviándole el MIN, ESN y el AUTHR, y el RANDC derivado del RAND usado para calcular el AUTHR.

c) El MSC-2 verifica el RANDC enviado por el MS y envía el apropiado valor de RAND en un AUTHREQ al nuevo VLR servidor VLR-2.

d) VLR-2 reenvía el AUTHREQ al HLR asociado con ese MIN, donde el HLR reenvía el AUTHREQ a su AC.

e) El AC verifica el MIN y el ESN entonces ejecuta él CAVE usando el SSD-A actualmente almacenado, el ESN, el MIN1 y el RAND para producir un registration Authentication Result (AUTHR). El AC verifica que el AUTHR recibido por el MS coincida con el calculado por él CAVE.

f) El AC envía un authreq al HLR. El authreq pude incluir el SSD y las directivas para manejar una recusación única, para actualizar el SSD del MS o par actualizar el contador del MS de acuerdo con la forma de administración local del AC/HLR.

g) El HLR reenvía el AUTHREQ al VLR-2 el cual lo reenvía al MSC-2

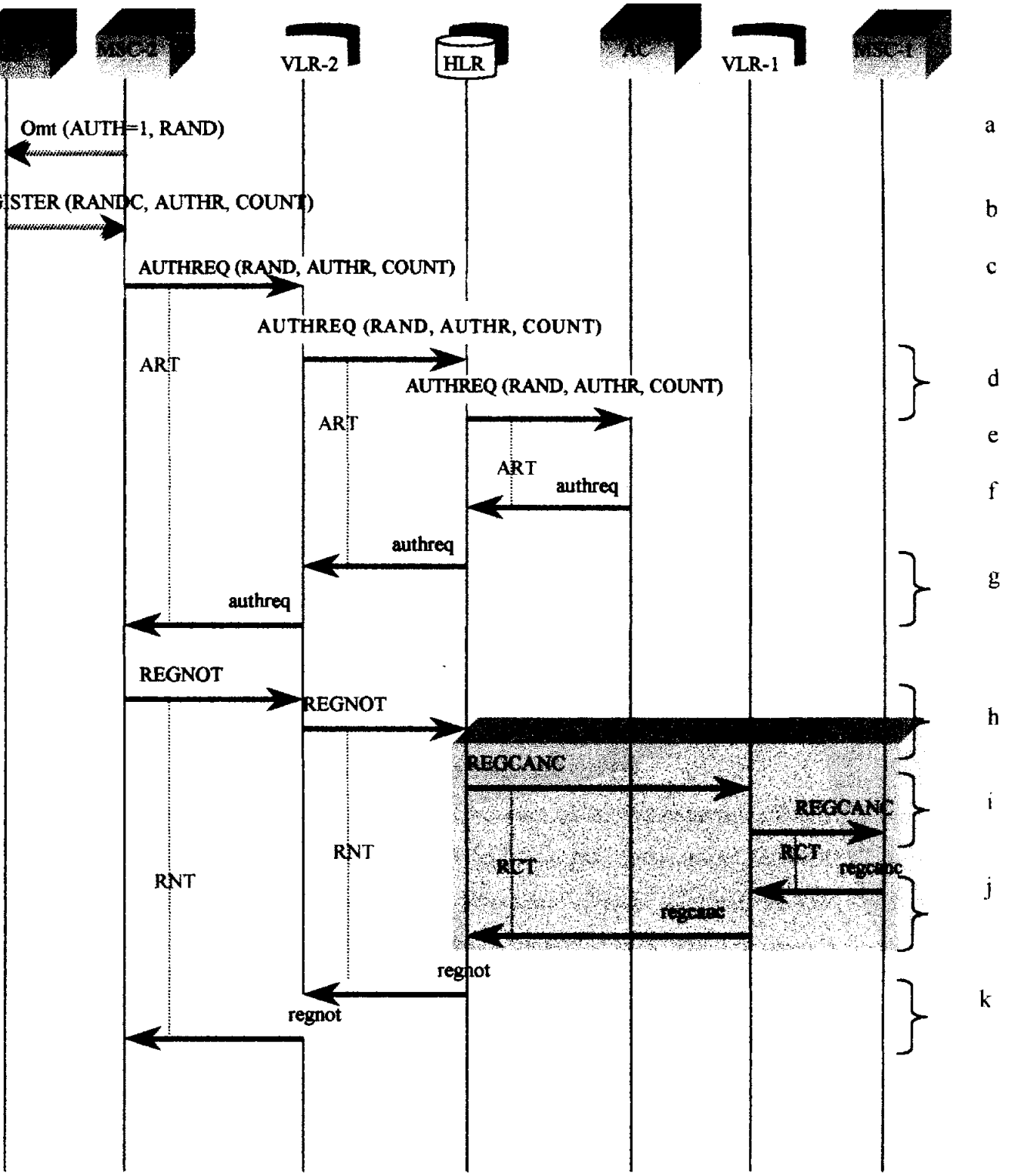
h) Siguiendo con una autentificación exitosa del MS, el MSC-2 envía un REGNOT a al VLR-2. El VLR-2 reenvía el REGNOT al el HLR

i) Si el MS fue previamente registrado en otro sistema, el HLR envía un REGCANC al antiguo VLR-1. El VLR-1 reenvía el REGCANC al antiguo MSC-1.

j) El MSC-1 regresa el regcac al VLR-1 y este al HLR.

k) El HLR graba la nueva localización del MS en su memoria local y responde el regnot con un regnot que incluye la información requerida por el VLR-2. El VLR-2 reenvía el regnot al MSC-2

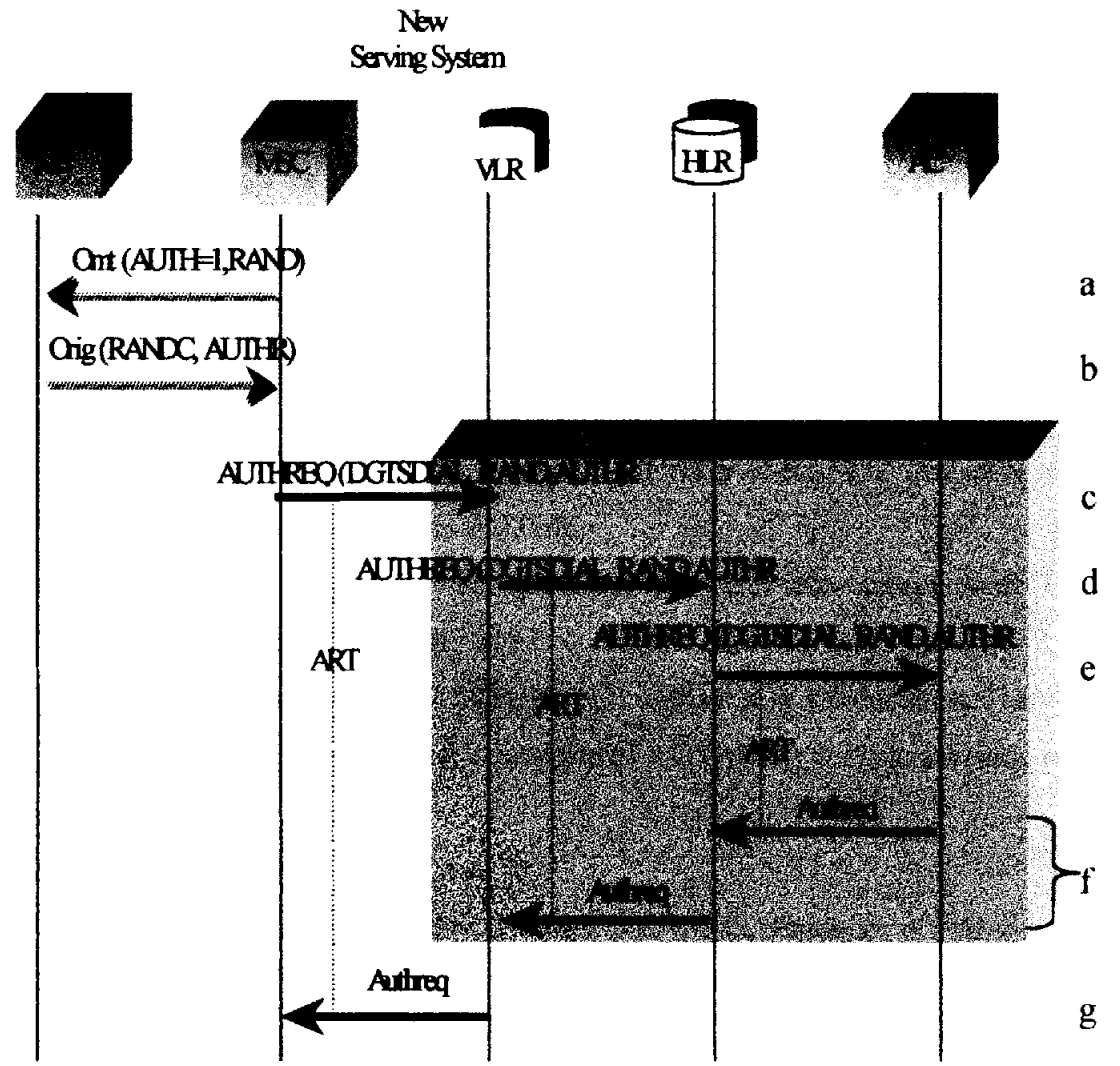
INITIAL REGISTRATION WITH AUTHENTICATION OVER RADIO CHANNEL



5.3.1.2.-ORIGEN CON AUTENTIFICACION SOBRE CANAL DE RADIO

a. El MS determina del Overhead Message Train (OMT) que una autentificación es requerida (AUTH=1). El número aleatorio usado para autentificar (RAND) puede también ser obtenido por el MS en este momento. Si no es así, el valor de cero es usado por el MS, como lo indica la autentificación TR-45. El MS ejecuta él CAVE usando los números digitados, el RAND, el ESN y el SSD almacenado, para producir el Origination Authentication Request.
b. EL MS envía un mensaje de originación al nuevo MSC-V, enviándole los números digitados, el MIN, el ESN, el Authentication Result (AUTHR) y el RANDC que es el RAND usado para calcular el AUTHR.
c. El MSC verifica el RANDC enviado por el MS y envía los números digitados al nuevo VLR con el valor apropiado de RAND en el AUTHREQ.
d. Si el SSD esta actualmente compartido con el VLR, el VLR realizara la validación del MS han e ira al paso h; caso contrario, el VLR reenviara el AUTHREQ al HLR asociado con el MIN.
e. El HLR reenviara el AUTHREQ al AC.
f. El AC verifica el MIN y el ESN reportados por el MS y entonces ejecuta él CAVE usando el SSD, el MIN y el ESN actualmente asociado con el MS a través del valor de RAND y los dígitos marcados provistos por el MSCV para producir el Origination Authentication Response (AUTHR). El AC verifica que el AUTHR recibido del MS coincide con el resultado del CAVE.
g. El authreq incluiría el SSD y directivas para editar una recusación única (Unique Challenge), para actualizar el SSD del MS, o para actualizar el MS COUNT de acuerdo con las practicas administrativas del AC local. Alternativamente, el authreq incluiría Deny Access. El AC envía un authreq al HLR. El HLR reenvía el authreq al VLR.
h. El VLR regresa el authreq al MSC. Siguiendo una autentificación segura del MS, el MSC asigna el MS a un canal de voz analógico o a un canal de trafica digital o conserva la asignación actual.

ORIGINATION WITH AUTHENTICATION OVER RADIO CHANNEL



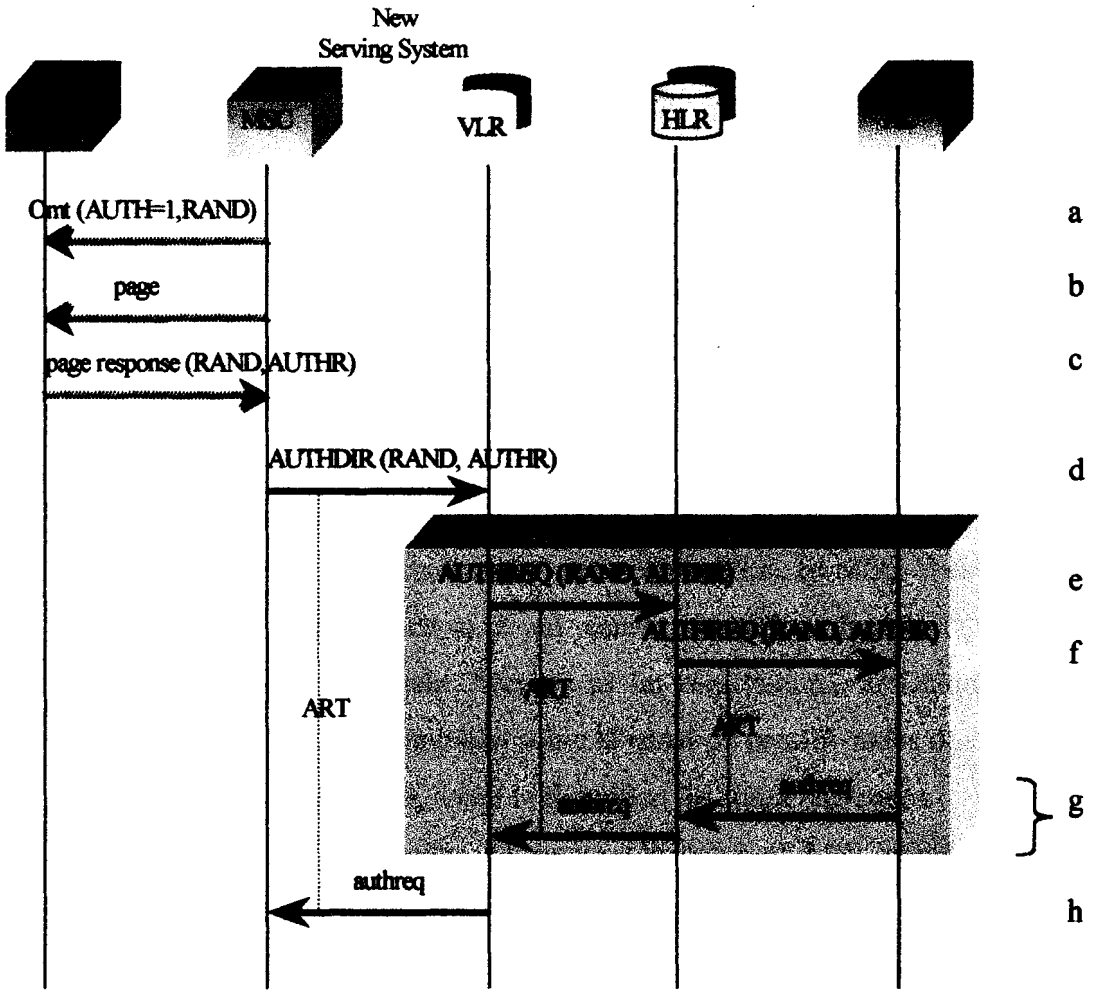
Note: Voice/traffic channel shall be assigned by this time

5.3.1.3.-TERMINACION CON AUTENTIFICACION SOBRE CANAL DE RADIO

a. El MS determina del Overhead Message Train (OMT) que una autentificación es requerida en los sistemas de acceso con AUTH=1. El número aleatorio usado para la autentificación (RAND) puede ser obtenido también por el MS en este momento; Si no es así el valor de cero es usado por el MS, como lo indica la autentificación por TR-45.
b. El MS reconoce un mensaje de rastreo con su MIN y ejecuta él CAVE usando el SSD que tiene almacenado, el ESN, el MIN y el valor RAND para producir el Termination Authentication Result (AUTHR)
c. El MS envía un mensaje de respuesta de rastreo al nuevo MSC-V entregándole el MIN, el ESN, el Authentication Result (AUTHR), y el RANDC que es el mismo del RAND usado para calcular el AUTHR.
d. El MSC verifica el RANDC enviado por el MS y envía el valor apropiado de RAND en un AUTHREQ al nuevo VLR.
e. Si el SSD es compartido con el VLR, el VLR realizaría la validación del MS e iría al paso i; caso contrario, el VLR reenviaría el AUTHREQ al HLR asociado con el MIN.
f. El HLR reenvía el AUTHREQ a su AC.
g. El AC verifica el MIN y el ESN enviados por el MS. Entonces el AC ejecuta él CAVE usando el SSD almacenado, el ESN, el MIN asociado al MS, y el RAND entregado por el sistema servidor para producir un termination Authentication Response (AUTHR). El AC verifica que el AUTHR recibido por el MS coincida en los resultados del CAVE.
h. El authreq incluiría directivas de edición de la recusación única, para actualizar el SSD del MS, o para actualizar el MS COUNT de acuerdo con las practicas administrativas del AC local. Alternativamente, el authreq incluiría un DenyAccess. El AC envía un authreq al HLR. El HLR reenvía el authreq al VLR.

i. El VLR retorna un authreq al MSC. Seguido de la autentificación exitosa del MS, el MSC asigna un canal de voz analógica, o un canal de trafica digital, o conserva la asignación existente.

TERMINATION WITH AUTHENTICATION OVER RADIO CHANNEL



Note: Voice/traffic channel shall be assigned by this time

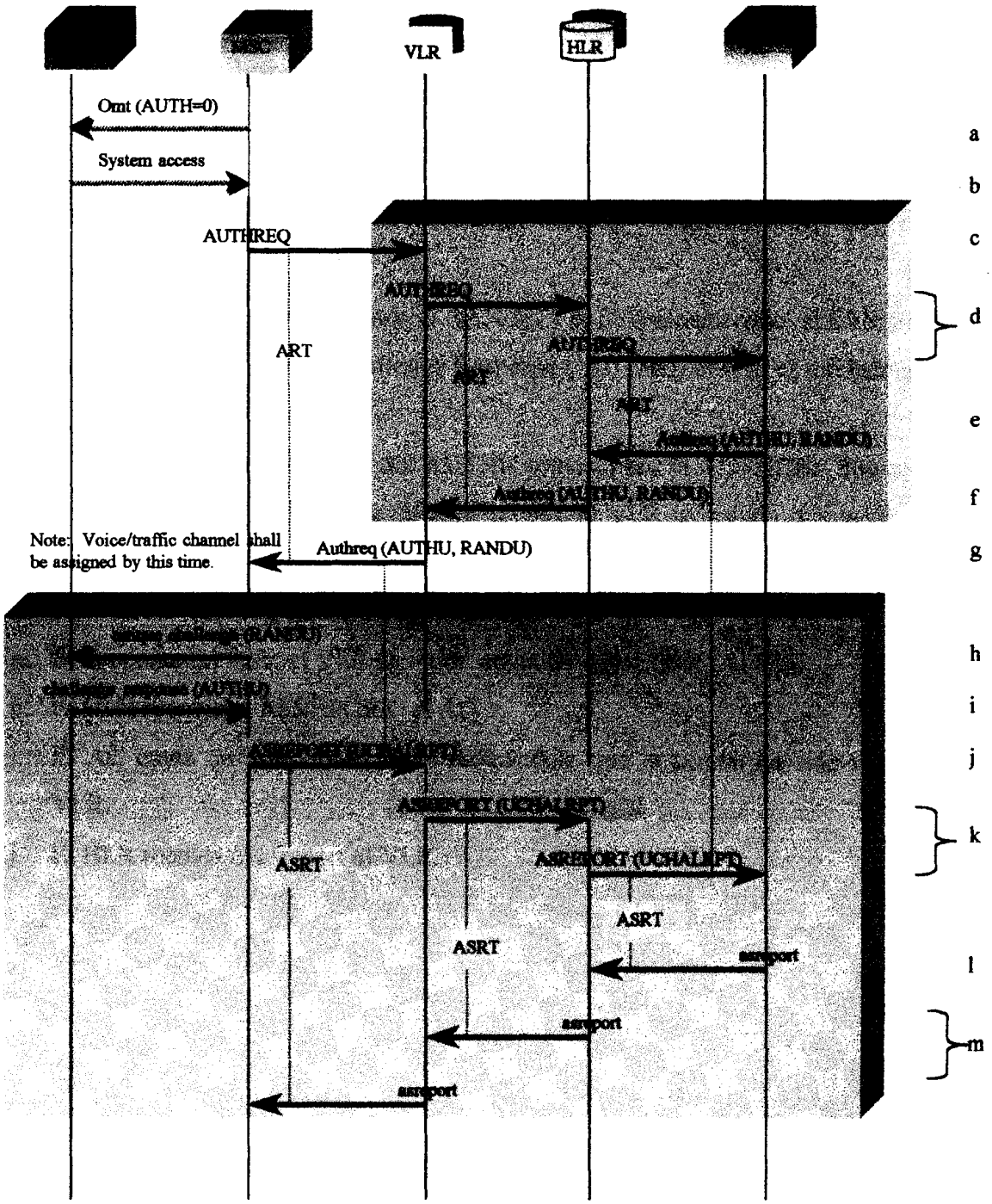
5.3.1.4.-AUTENTIFICACION SOBRE CANAL DE VOZ

a. El MS determina por el Overhead Message Train (OMT) que una autentificación no es requerida sobre los sistemas de acceso (AUTH=0)
b. El MS envía un Message system Access (registration , origination o page response) al MSC-V , enviándole solo el MIN y el ESN.
c. El MSC-V envía un AUTHREQ al VLR servidor con el System Access Type seteado como UNSPECIFIED.
d. El VLR reenvía el AUTHREQ al HLR asociado con el MIN. El HLR reenvía el AUTHREQ al AC.
e. El AC verifica el MIN y el ESN enviados por el MS. El AC escoge una variable aleatoria única (RANDU) y ejecuta él CAVE usando el SSD almacenado, el ESN y el MIN asociados con el MS , para producir un Unique authentication Response (Authu) El AC envía un authreq al HLR incluyendo el RANDU y el resultado del AUTHU esperado.
f. El HLR reenvía el authreq al VLR servidor.
g. El VLR servidor ENVIA UN authreq al MSC-V, conteniendo los valores del AUTHU y el RANDU recibidos en el authreq del HLR. El MSC-V asigna el MS a un canal de voz analógico o a un canal de tráfico digital. Opcionalmente (específicamente si el system Access es un registration), el Unique Challenge Messages podría ser intercambiado sobre el canal de control, antes de la asignación del canal de voz o de tráfico, como lo describen los siguientes pasos.
h. El MSC –V envía una orden de recusación única al MS usando el RANDU provisto por el authreq.
i. El MS ejecuta él CAVE usando el RANDU y el SSD almacenado , el ESN y el MIN para producir el Authentification Result (AUTHU) el cual es enviado al MSC –V. El MSC-V compara los valores de AUTHU provistos en el authreq con los recibidos del MS.
j. El MSC-V envía un ASREPORT al VLR servidor indicando suceso o falla en la recusación única.
k. El VLR reenvía el ASREPORT al HLR. El HLR reenvía el ASREPORT a su AC.

l. El AC responde con un asreport que incluiría el SSD y las directivas para denegar el acceso o la actualización del SSD.

m. El HLR reenvía el asreport al VLR servidor. El VLR servidor envía un asreport al MSC-V.

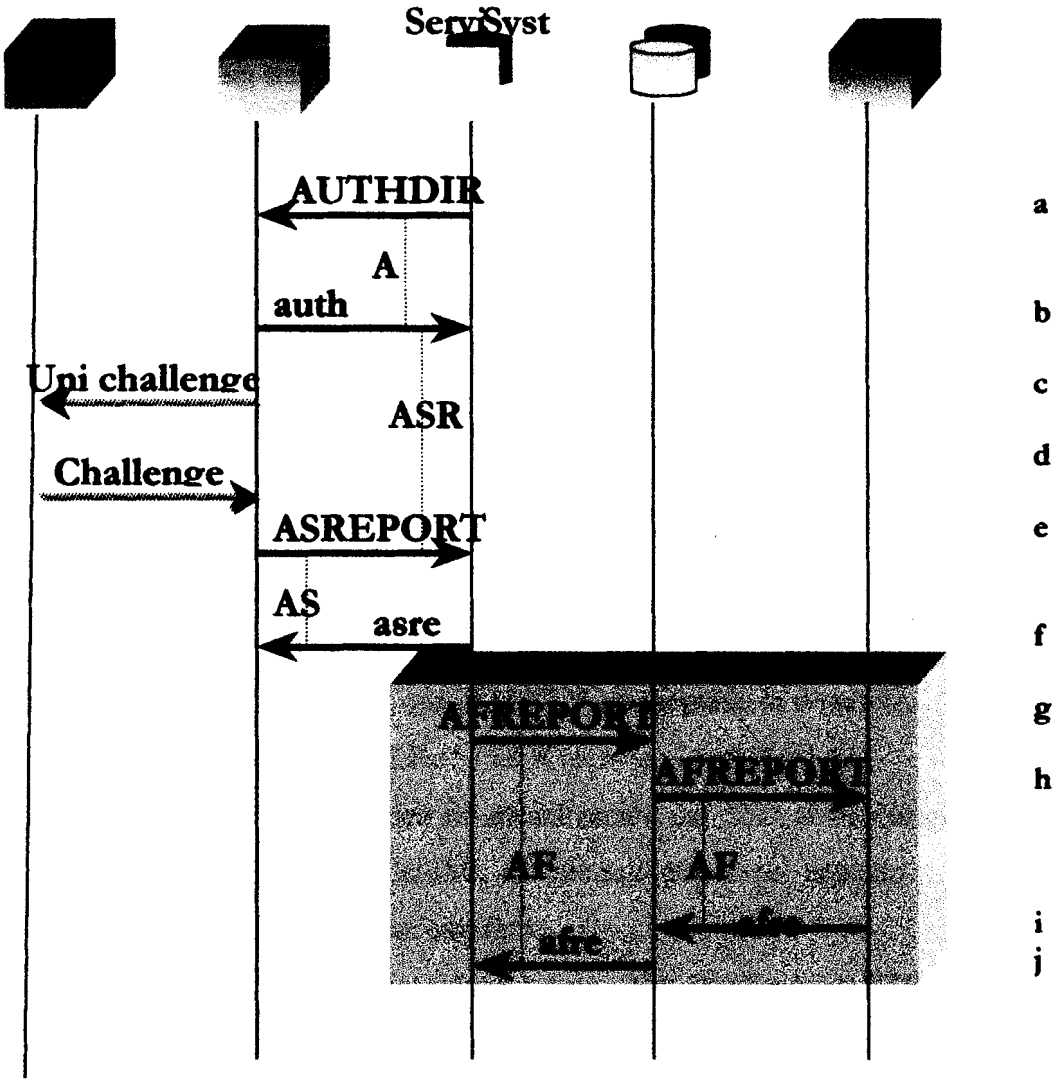
AUTHENTICATION OVER VOICE CHANNEL



5.3.1.5.-VLR INICIANDO UN UNIQUE CHALLENGE

a. El VLR servidor escoge una variable aleatoria única (RANDU) y ejecuta el CAVE usando el SSD almacenado, el ESN y el MIN asociado con el MS, para producir el Authentication Response para la recusación única (AUTHU)
b. El authdir del MSC-V hacia el VLR sirve solo para informar al VLR que el MSC-V ha aceptado la directiva.
c. El MSC-V envía una orden de recusación única al MS usando el RANDU provisto por el AUTHDIR.
d. El MS ejecuta él CAVE usando el RANDU y el SSD almacenado, el ESN y el MIN para producir un Unique Challenge Response (AUTHU) el cual es enviado al MSC –V,
e. El MSC-V compara el valor del AUTHU provisto por el AUTHDIR con el recibo por el MS. El MSC-V envía un ASREPORT al VLR indicando que la recusación única se ha completado.
f. El VLR servidor regresa un asreport al MSC-V
g. Si la operación falla, el VLR servidor envía un AFREPORT al HLR.
h. El HLR reenvía el AFREPORT al AC.
i. El AC envía un afreport al HLR, indicándole que la acción ha sido recibida del VLR.
j. El HLR reenvía el afreport al VLR.

VLR INITIATED UNIQUE CHALLENGE



5.3.1.6.-ACTUALIZACION DEL SSD CON EL SSD COMPARTIDO

a. El AC determina que el Shared Secret Data (SSD) debe ser actualizado. Esto puede ser por el resultado de un procedimiento administrativo en el AVC, expiración de un intervalo de tiempo de autentificación en el AC, o el reporte de violación de seguridad de un sistema ajeno.
b. Un AUTHDIR es enviado desde el AC al HLR asociado con el MS.
c. El HLR reenvía el AUTHDIR al VLR servidor actual.
d. El SSD pendiente seria usado para calcular el RANDU , el AUTHU y el AUTHB para la operación de actualización del SSD. El VLR escoge una variable aleatoria única (RANDU) y ejecuta él CAVE usando el valor pendiente de SDD, el ESN, y el MIN asociado con el MS para producir una Unique Authentification Response. (AUTHU).
e. El VLR reenvía el AUTHDIR al MSC incluyendo el RANDU y el resultado AUTHU esperado.
f. Un AUTHDIR vacio es enviado desde el MSC-V al VLR servidor. El authdir sirve solo para informar al VLR que el MSC-V ha aceptado la directiva. El VLR servidor reenvía el AUTHDIR al HLR. El HLR reenvía el authdir al AC.
g. El MSC-V envía una orden de actualización del SSD al MS usando el valor de RANDSSD provisto por el AC. El mensaje puede ser enviado por el canal de control o por el canal de voz o trafico.
h. El MS ejecuta él CAVE para producir un valor pendiente de SSD usando el valor RANDSSD provisto por el SSD Update order, el ESN y el A-key.
i. El MS selecciona un numero aleatorio (RANDBS) y envía una orden de recusación de estación base al MSC-V incluyéndole el valor de RADS
j. El MS ejecuta él CAVE para producir un Authentication Result (AUTHBS) usando el valor pendiente de SSD, el ESN, el MIN y el número aleatorio (RANDBS). El VLR también ejecuta él CAVE para producir un Authentication Result (AUTHBS) usando el valor pendiente del SSD, el ESN ,el MIN del MS y el número aleatorio (RANDBS) provisto por el MS.
k. El VLR provee su valor calculado de AUTHBS al MSC-V en un bschall.

l. El MSC-V pasa eta información a través del MS en un Base Station Challenge response Message.

m. Si el AUTHBS resultante provisto por el VLR coincide con el valor calculado por el MS, el MS almacena en valor del SSD pendiente para subsecuentes ejecuciones del CAVE.

n. Si el resultado de AUTHBS provisto por el VLR coincide con el valor calculado por el MS, el MS almacena el valor pendiente del SSD para su uso en ejecuciones subsecuentes de CAVE.

o. El MS envía un mensaje de confirmación de actualización de SSD al MSC-V

p. El MSC-V envía una orden de recusación única al MS usando el RANDU provisto en el AUTHDIR

q. El MS ejecuta él CAVE usando el RANDU y el SSD actualmente almacenado, el ESN, y el MIN para producir una Authentication Response para la recusación única. (AUTHU)

r. El MS envía un AUTHU al MSC-V

s. El MSC-V envía un ASREPORT al VLR servidor indicando que la actualización del SSD se ha completado exitosamente.

t. El VLR servidor reenvía el ASREPORT al HLR y remueve el SSD pendiente.

u. El HLR reenvía el ASREPORT al AC.

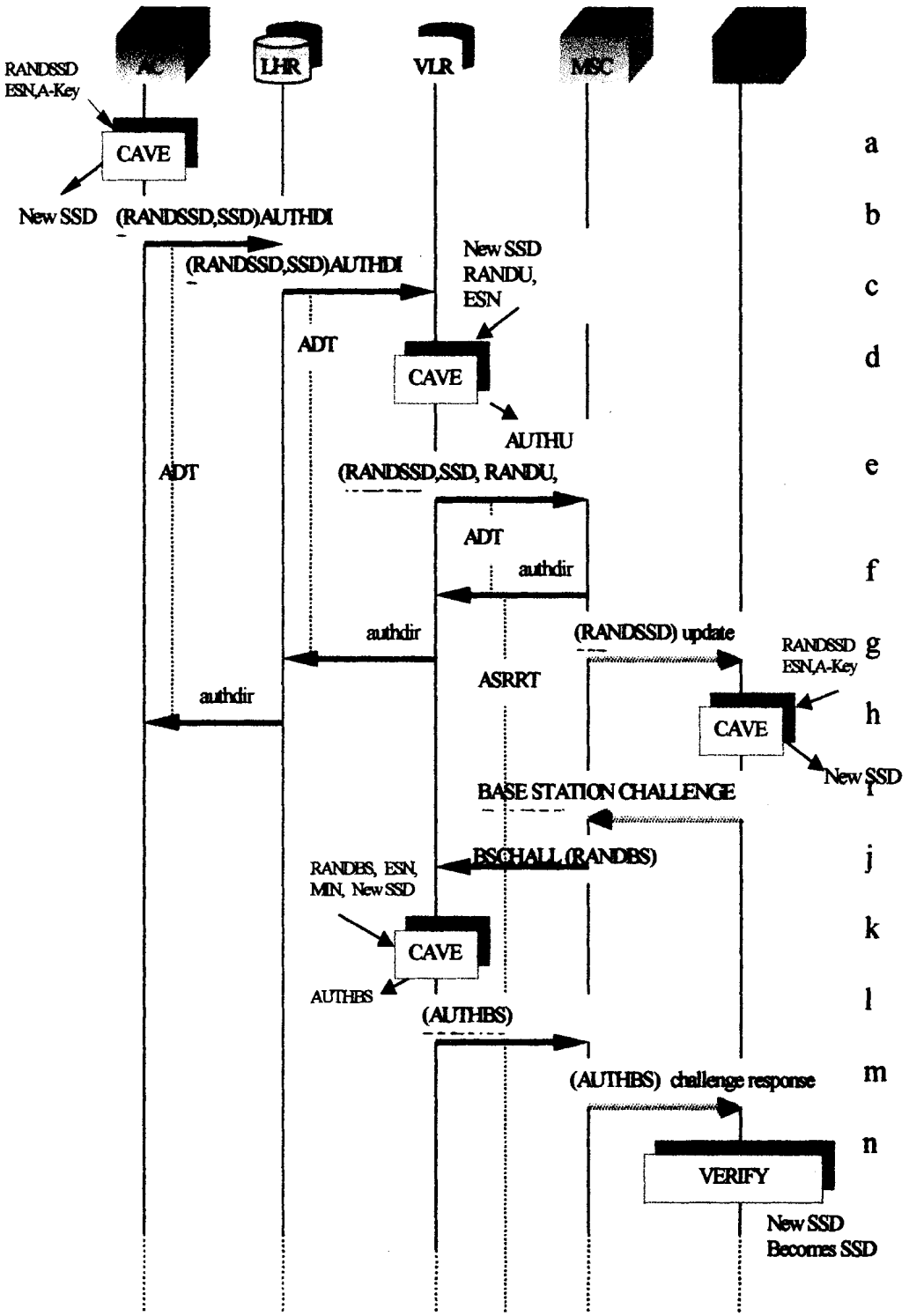
v. El AC almacena el valor pendiente de SSD para su uso en ejecuciones subsecuentes de CAVE por el MS si la actualización de SSD ha sido exitosa

w. El AC envía un asreport indicando que servicio será provisto al MS. El AC incluye el nuevo SSD en el asreport para compartirlo con el VLR.

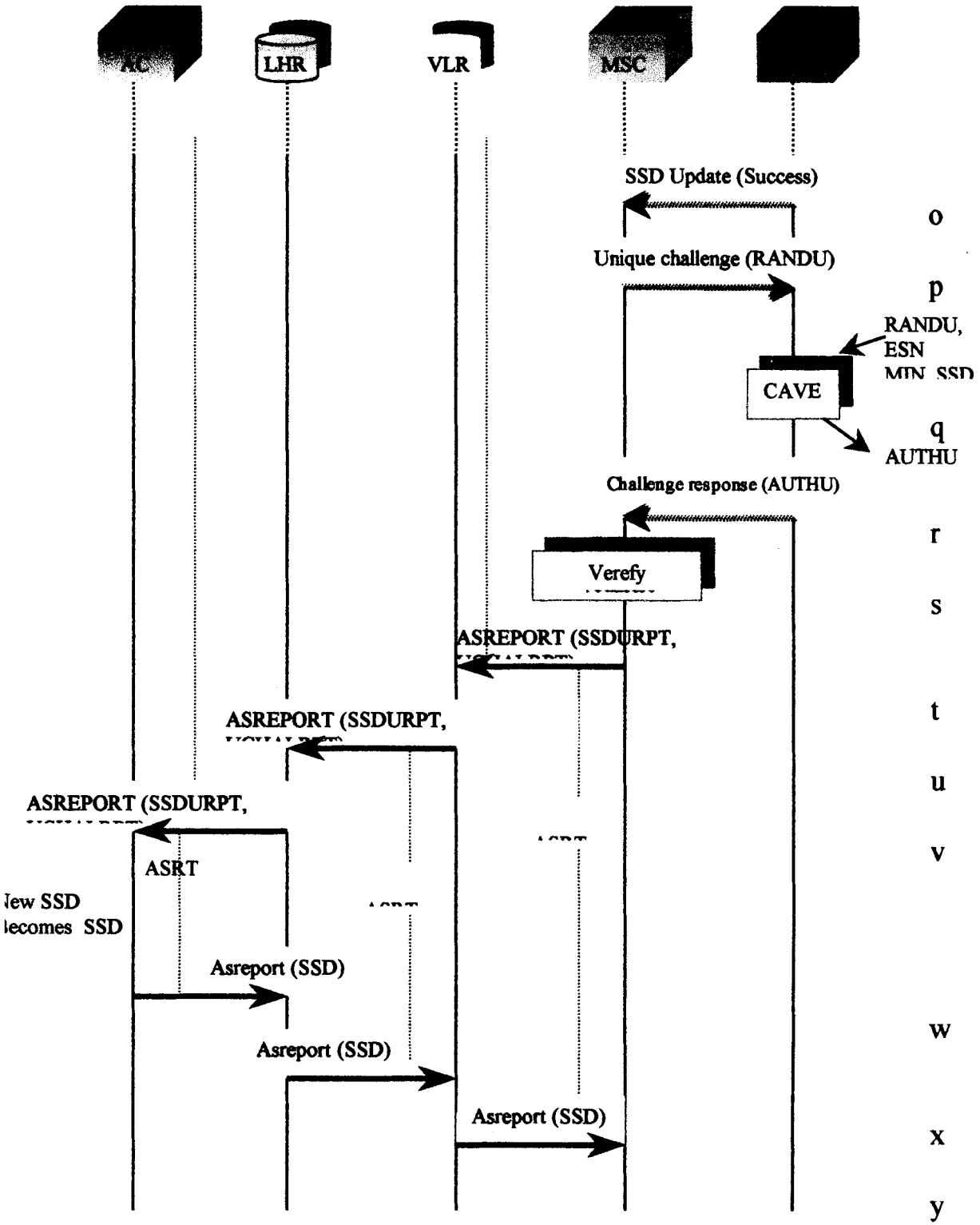
x. El HLR reenvía el asreport al VLR servidor. El VLR el SSD recibido

y. El VLR servidor reenvía el asreport al MSC servidor.

UPDATE SSD WITH SSD SHARED



UPDATE SSD WITH SSD SHARED (CONTINUED)

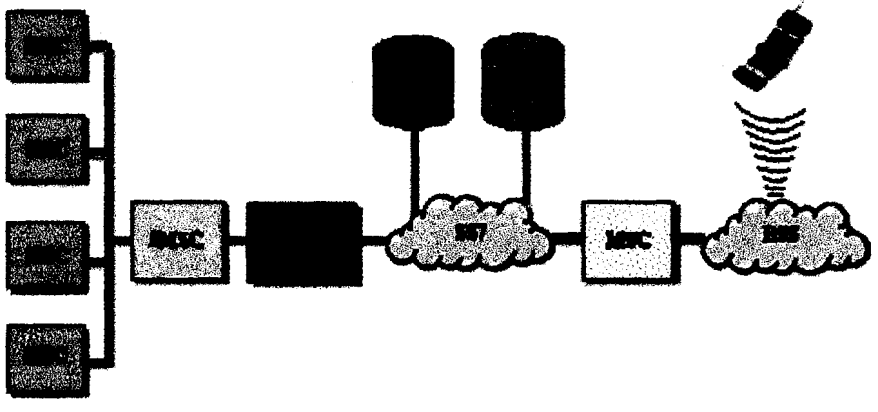


6.-Short Message Service Center (SMSC)

SMS es conocido por varios nombres, tales como mensajería de PCS, mensajería de texto, correo de voz, mensaje celular Teleservice (CMT), Celular Alpha Paging, etc. Es la transmisión de los mensajes cortos del texto a un teléfono portátil, similar al alpha-numeric paging.

Para enviar un mensaje de texto a un móvil, usted puede enviar un email, enviar un page, utilizar un software con lógica especial para hacer llamadas, o enviando mensajes desde un teléfono a otro.

El mensaje debe ser corto, cerca de 110 caracteres, e incluye solamente caracteres alfanuméricos, y no contener cuadros ni gráficos.



Entre los elementos que se utilizan ya conocemos algunos como el MSC, VLR, HLR y el MS que es un terminal capaz de recibir y de originar mensajes cortos así como llamadas de voz, los otros los detallamos continuación:

- **Short Messaging Entities**

(SME) es una entidad que puede recibir o enviar mensajes cortos. El SME se puede situar en la red fija u otro centro de servicio.

- **Short Message Service Center**

El centro de servicio corto de mensaje (SMSC) es responsable del almacenamiento y la retransmisión de un mensaje corto entre un SME y MS.

- **SMS-Gateway/Interworking Mobile Switching Center**

El MSC gateway de un SMS (SMS-GMSC) es un MSC capaz de recibir un mensaje corto de un SMSC, de interrogar un (HLR) para la información de encaminamiento, y de entregar el mensaje corto al MSC " visitado " de la estación móvil receptora.

El MSC que intertrabaja con un SMS (SMS-IWMSC) es un MSC capaz de recibir un mensaje corto de la red móvil y de someterlo al SMSC apropiado. Los SMS-GMSC/SMS-IWMSC se integran típicamente con el SMSC.

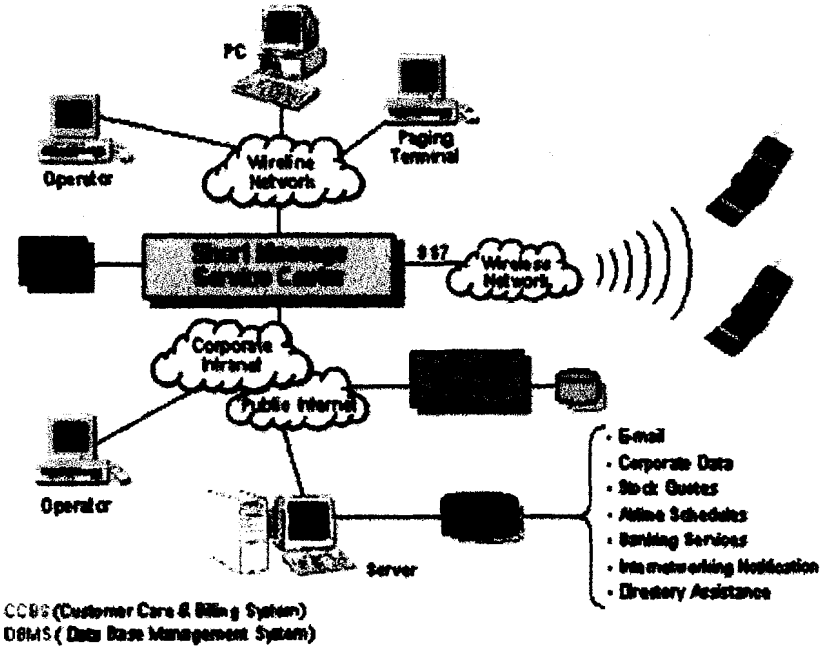
6.1.-Servicios Del Suscriptor

SMS abarca dos puntos básicos para señalar servicios:

1. Mensaje Corto originado por el Móvil- (MO-SM).
2. Mensaje Corto terminado en el Móvil (MT-SM).

1.- Los mensajes cortos originados por el Móvil- se transportan del microteléfono al SMSC y pueden ser destinados a otros suscriptores móviles o para los suscriptores en redes fijas tales como redes de la paginación o redes del correo electrónico.

2.- Los mensajes cortos terminados en el Móvil se transportan del SMSC al microteléfono y se pueden someter al SMSC por otros suscriptores móviles vía MO-SM o por otras fuentes tales como sistemas del correo de voz, paginando redes, o a operadores.



Para MT-SM, un informe ser siempre regresa al SMSC para confirmar que el corto mensaje salida llego al microteléfono. Semejantemente, para MO-SM, un informe se vuelve siempre al microteléfono que confirma la salida corta del mensaje al SMSC.

6.2.-Descripciones de los Mensajes de SMS

Para la utilización de este servicio se utilizan tres tipos de mensajes del IS-41 que son los siguientes:

1. Short Message Delivery Point to Point.

Este mensaje se envía a un MSC o a un MC para entregar un mensaje corto. Este mensaje es reconocido por una respuesta.

2. Short Message Request.

Este mensaje se envía al HLR para solicitar el enrutamiento de la dirección del SMS en el que se encuentra el móvil. Este mensaje es reconocido por una respuesta.

3. Short Message Notification.

Este mensaje se envía al MC para informarle que el móvil esta listo recibir el mensaje previamente pospuesto. Este mensaje es reconocido por una respuesta

6.3.-Funcionamiento del SMSC

Ahora que ya conocemos la estructura y el tipo de mensajes a utilizar explicaremos como se realiza el proceso de Short Message en los siguientes pasos:

1.-El Email Gateway consigue el mensaje del Centro de Servicio Mensaje Corto:

Se utiliza un email Gateway para enviar un email al número de teléfono subscriptor, direccionando el email con el número telefónico. El remitente pone el tema y el mensaje y lo envía, el mensaje será truncado de modo que la longitud total no exceda la longitud máxima.

El mensaje va a un email gateway. El email gateway convierte el mensaje a una forma que el centro del mensaje entienda y luego lo envía.

2. El Centro de Servicio de Mensaje Corto determina en donde está el suscriptor.

El Centro de Servicio de Mensaje Corto (SMSC) es responsable de conseguir el mensaje al teléfono. El SMSC es un periférico inteligente que utiliza señalización ANSI-41.

Primero, el centro del mensaje envía un SMS Request (una petición de SMS) al registro casero de la localización (HLR) para saber en donde está el cliente. El SMSC puede utilizar un título global de traducción en el punto de transmisión de señalización (STP) par determinar a que HLR se envía el mensaje. La razón para utilizar el título global de traducción es que el centro de mensaje puede no tener bastante espacio para cargar todo el HLR y la identificación del número (MIN). El centro de mensaje conoce solamente la capacidad del puntero de código del par STP que realizará el título global. El STP determinará el HLR chequeando el MIN con la tabla de traducción de títulos globales.

Una vez que el HLR reciba la petición de SMS, controla el estatus de los subscriptores y responde con un resultado de vuelta. El resultado de vuelta dirá el

SMSC si el suscriptor es inactivo, o en donde está el suscriptor, por el código del puntero y la identificación del centro de conmutación móvil (MSCID).

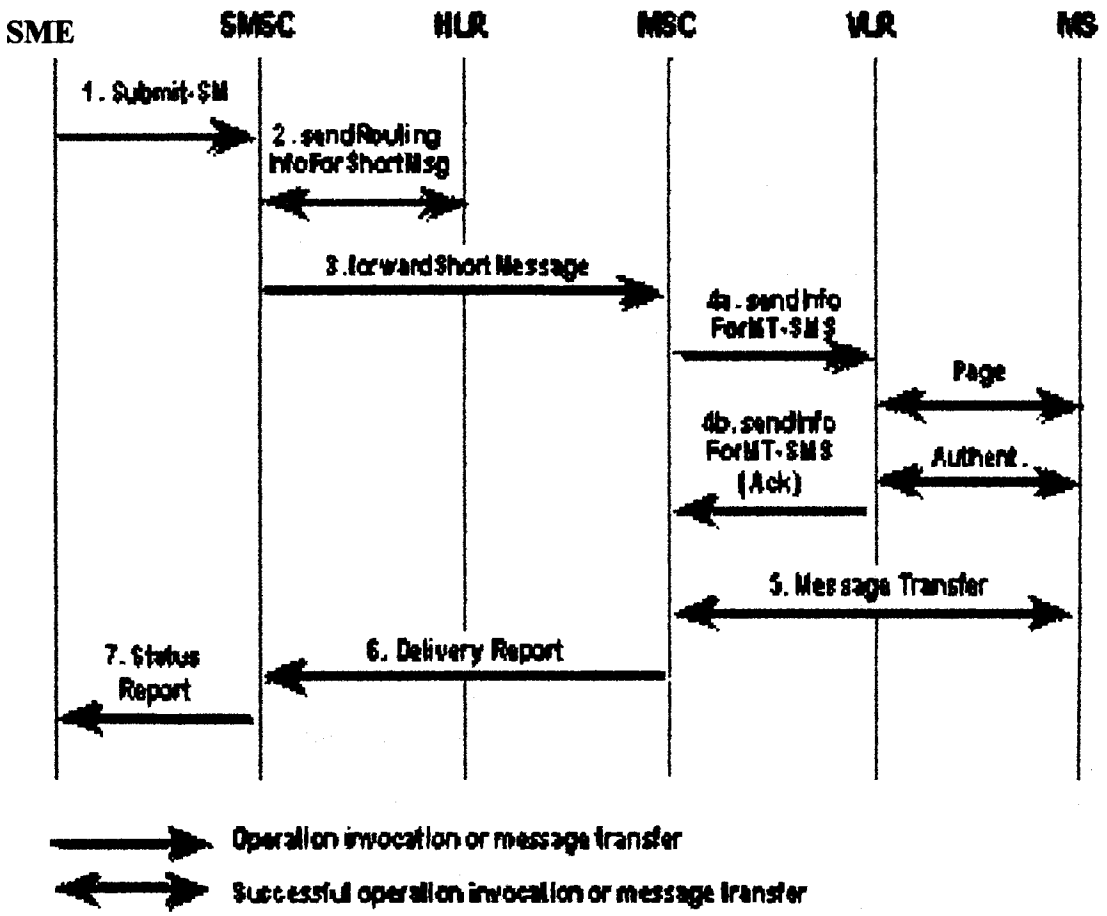
El HLR también sabe si el sistema de servicio es capaz de recibir señala del mensaje corto. Si no, el HLR responderá con un estatus inactivo a la petición de SMS. Si el suscriptor es inactivo, el SMSC mantendrá el mensaje en cola por un período de tiempo. Este período puede ser generalmente ajustado de modo que el centro del mensaje no consiga tener muchos mensajes en cola. El HLR guardará un indicador que muestre que mensaje está esperando. Si el suscriptor viene a su propia área de servicio, o entra a un sistema capaz de SMS, el HLR envía una notificación de SMS (*SMSNOT Notification*) al SMSC. El SMS envía una señal de retorno (*SMSREQ Notification Return Result*) diciendo al HLR " gracias, " y el SMSC procurará entregar el mensaje.

3. El centro del mensaje entrega el mensaje:

El centro del mensaje enviará un *Short Message Delivery Point to Point* (*SMDPP*) al sistema de servicio. El sistema de servicio hace page al móvil. Si el móvil responde, el sistema entrega el mensaje. Si la transmisión del mensaje es acertada, el resultado de vuelta de SMDPP va al centro del mensaje sin ningún error. El centro de mensaje fijará el estatus del mensaje " enviado " y no enviará el mensaje otra vez. El texto del mensaje está dentro del mensaje de SMDPP.

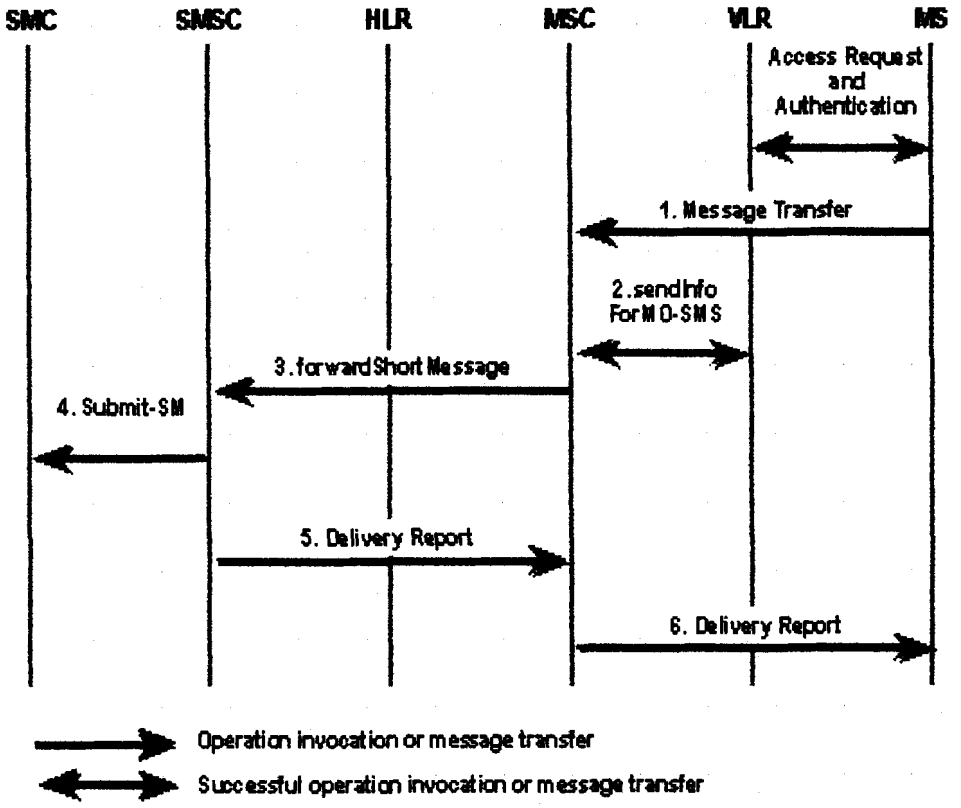
El siguiente ejemplo es Un Mensaje Corto terminado en el móvil.

1. El mensaje es enviado del SME al SMSC.
2. Después que termina su proceso interno, el SMSC interroga al HLR y recibe la información de encaminamiento para el suscriptor móvil.
3. El SMSC envía el mensaje corto al MSC usando la operación de forward Short Message
4. El MSC extrae la información del suscriptor del VLR. Esta operación puede incluir un procedimiento de la autentificación.
5. El MSC transfiere el mensaje corto al MS.
6. El MSC vuelven al SMSC el resultado de la operación de forward Short Message.
7. El SMSC vuelve un informe al SME que indica la salida del mensaje corto.



Mensaje Corto originado por el Móvil-

1. El MS transfiere el SM al MSC.
2. El MSC interroga al VLR para verificar que la transferencia del mensaje no viola los servicios suplementarios invocados o las restricciones impuestas.
3. El MSC envía el mensaje corto al SMSC usando la operación de forward Short Message.
4. El SMSC entrega el mensaje corto al SME.
5. El SMSC reconoce al MSC el resultado acertado de la operación de forward Short Message.
6. El MSC vuelve al MS el resultado de la operación de MO-SM.



7. CONCLUSIONES

El protocolo IS41 es un estándar de le EIT/TIA el cual permite la mensajería entre centrales telefónicas. Por medio del IS41 se puede hacer roaming entre abonados de dos MSC diferentes, es decir que un abonado podrá usar la infraestructura de otro MSC sin perder ninguno de sus beneficios y además siendo facturado este consumo en su MSC original. Este protocolo permite que no exista interrupción de llamadas cuando se pasa de un area de servicio a otra area es decir que un usuario puede estar hablando mientras hace el cambio de MSC sin que tenga ningún efecto sobre la llamada, siendo así un proceso transparente al usuario.

Como todo estándar ha pasado por múltiples revisiones desde su origen, así tenemos las revisiones A, B, C y la de Nortel, las cuales se diferencian entre ellas por que las ultimas revisiones tienen además de las funciones anteriores mejoras permitiendo actualizaciones en sus métodos de acceso y por tanto mas beneficios para el usuario. Ya que el roaming se hace mas rápidamente y con mas eficiencia en cuanto a su transparencia. En la primera revisión como método de acceso se utilizaba tecnología FDMA con la cual se estandarizo el AMPS, pero desde la revisión B se utiliza tecnología de acceso CDMA.

En la primera revisión de IS41 se manejaban solo dos propiedades: Intersystem call handoff y roamer validation , una vez que se hizo la siguiente , la revisión A , se añadieron otras propiedades entre las cuales se destacan el call delivery, el remote feature control, el call forwardin , la conferencia, y el call waiting. En la revisión C se hicieron modificaciones que afectan mas al MSC que al usuario como son el Dual-mode handoff, el Control of Vertical features, y el GTT. La ultima revisión es la revisión P la cual es propietaria de NORTEL en las cuales se incluyen propiedades de Roaming do not disturb, Status Information , Network boundary paging y message tandeming entre otras.

El AC centro de autentificación es el organo en el cual se ejecuta el chequeo de los parametros de validacion que son enviados en mensajes desde el HLR . Estos parametros son analizados y si coinciden con las comparaciones predeterminadas el movil es validado. En la autentificación se toman una serie de seguridades como se explico anteriormente ya que los parametros de los que hablamos son cambiados periodicamente de manera automatica (como es el parametro del SSD) esto brinda un nivel de seguridad en la autentificación unico, ya que lo unico que se mantiene fijo es el A-key que se almacena en el telefono y el HLR en el momento de la primera inscripcion.

8.- ANEXOS

Message Name	IS-41 A	IS-41 B	IS-41 C	IS-41 D
AuthenticationDirective	NA	NA	Yes	Yes
AuthenticationDirectiveForward	NA	NA	Yes	Yes
AuthenticationFailureReport (SecurityStatusReport)	Yes	Yes	Yes	Yes
AuthenticationRequest	NA	NA	Yes	Yes
AuthenticationStatusReport	NA	NA	Yes	Yes
BaseStationChallenge	NA	NA	Yes	Yes
Blocking	Yes	Yes	Yes	Yes
Billing Request	NA	NA	NA	Yes
BulkDeregistration	NA	NA	Yes	Yes
CallDataRequest	Yes	Yes	Yes	Yes
CountRequest	NA	NA	Yes	Yes
CSS Inative	NA	NA	NA	Yes
FacilitiesDirective2	NA	NA	Yes	Yes
FacilitiesDirective	Yes	Yes	Yes	Yes
FacilitiesRelease	Yes	Yes	Yes	Yes
FeatureRequest (RemoteFeatureControlRequest)	Yes	Yes	Yes	Yes
FlashRequest	NA	Yes	Yes	Yes
HandoffBack2	NA	NA	Yes	Yes
HandoffBack	NA	Yes	Yes	Yes
HandoffMeasurementRequest2	NA	NA	Yes	Yes
HandoffMeasurementRequest	Yes	Yes	Yes	Yes
HandoffToThird	Yes	Yes	Yes	Yes
HandoffToThird2	NA	NA	Yes	Yes
InformationDirective	NA	NA	Yes	Yes
InformationForward	NA	NA	Yes	Yes
InterSystemAnswer	NA	NA	Yes	Yes
InterSystemPage	NA	NA	Yes	Yes
InterSystemPage2	NA	NA	Yes	Yes
InterSystemSetup	NA	NA	Yes	Yes
LocationRequest	Yes	Yes	Yes	Yes
MobileOnChannel	Yes	Yes	Yes	Yes
MSInactive (CCSInactive)	Yes	Yes	Yes	Yes
Network Boundary	NA	NA	NA	Yes
OriginationRequest	NA	NA	Yes	Yes
QualificationDirective	Yes	Yes	Yes	Yes

QualificationRequest	Yes	Yes	Yes	Yes
RandomVariableRequest	NA	NA	Yes	Yes
RedirectionDirective	NA	NA	Yes	Yes
RedirectionRequest	Yes	Yes	Yes	Yes
RegistrationCancellation	Yes	Yes	Yes	Yes
RegistrationNotification	Yes	Yes	Yes	Yes
RemoteUserInteractionDirective	Yes	Yes	Yes	Yes
ResetCircuit	Yes	Yes	Yes	Yes
Routing do not distrub Cancellation	NA	NA	NA	Yes
RoutingRequest	Yes	Yes	Yes	Yes
Status Information	NA	NA	NA	Yes
ServiceProfileDirective	Yes	Yes	Yes	Yes
ServiceProfileRequest	Yes	Yes	Yes	Yes
SMSDeliveryBackward	NA	NA	Yes	Yes
SMSDeliveryPointToPoint	NA	NA	Yes	Yes
SMS Message Notification	NA	NA	Yes	Yes
RoutingRequest	Yes	Yes	Yes	Yes
SMSRequest	NA	NA	Yes	Yes
TransferToNumberRequest	Yes	Yes	Yes	Yes
TrunkTest	Yes	Yes	Yes	Yes
TrunkTestDisconnect	Yes	Yes	Yes	Yes
Unblocking	Yes	Yes	Yes	Yes
UnreliableRoamerDataDirective	Yes	Yes	Yes	Yes
UnsolicitedResponse	NA	NA	Yes	Yes
Total Number of Messages	26	28	54	59