

Gestión de la Movilidad y de las llamadas

Curso de Comunicaciones Móviles
UPB Bucaramanga

Introducción

- ▶ Hay dos situaciones en que puede estar el terminal móvil:
 1. Vinculado a la red, pero sin ninguna comunicación en curso
 2. Vinculado a la red y manteniendo una comunicación en curso (modo activo)

1. Vinculación sin comunicación en curso

▶ Debe asegurarse:

- ▶ La MS debe poderse incorporar a la red.
- ▶ La continuidad de la conexión de la MS a la red cuando se desplace por la zona de cobertura.
- ▶ Localización y aviso cuando existan llamadas destinadas a la MS.

▶ Además debe haber:

- ▶ Mecanismos de control de admisión a los servicios de la red (sólo MS habilitadas)
- ▶ Mecanismos de seguridad que protejan la información transmitida por la interfaz radio

2. Vinculación manteniendo una comunicación

- ▶ **Debe asegurarse que:**

- ▶ Haya continuidad en la comunicación en curso cuando la MS pasa de una celda a otra (solución: mecanismo de traspaso)

Gestion de la Movilidad

Introducción

- ▶ Se le llama así a las funciones de la red que permiten el acceso de la MS a los servicios de la red; estas funciones son:
 - ▶ Identificación de la MS
 - ▶ Seguridad en el acceso
 - ▶ Registro de la MS en la red
 - ▶ Localización (búsqueda) de la MS en la red

Identificación de la estación móvil

- ▶ En GSM una estación móvil se compone de dos partes:
 - ▶ El equipo físico (aparato)
 - ▶ La tarjeta SIM
- ▶ Por tanto, la identificación de una MS se compone de dos partes:
 - ▶ IMEI (International Mobile Equipment Identity): Identificación del aparato grabada por el fabricante.
 - ▶ IMSI (International Mobile Subscriber Identity): Identificación del usuario a nivel internacional que se incorpora en la SIM.

Números de identificación de la MS

IMEI:

TAC (6 cifras)	FAC (2 cifras)	SNR (6 cifras)	SP (1 cifra)
-------------------	-------------------	-------------------	-----------------

TAC: Type Approval Code
FAC: Factory Assembly code
SNR: Serial Number
SP: Spare

IMSI:

MCC (3 cifras)	MNC (2 cifras)	MSIN (10 cifras)
-------------------	-------------------	---------------------

MCC: Mobile Country Code
MNC: Mobile Network code
MSIN: Mobile Subscriber
Identification Number

NMSI: National Mobile Subscriber Identity

Características del IMSI

- ▶ No es conocido por el usuario
- ▶ Es un número usado por la red para el registro del abonado y el establecimiento de las llamadas
- ▶ Por seguridad se sustituye por otro número llamado TMSI (Temporary Mobile Subscriber Identity)
- ▶ El TMSI es asignado por el VLR donde está registrado el usuario (hay uno por cada usuario del VLR)

Número telefónico del abonado

- ▶ El número telefónico del abonado se conoce como MSISDN (Mobile Station ISDN) y se usa para efectuar llamadas a ese usuario

CC (2-3 cifras)	NDC (2-3 cifras)	Número de abonado
--------------------	---------------------	-------------------

CC: Country Code (código del país)

NDC: National Destination Code (prefijo del operador de red)

Funciones de Seguridad

Problema	Solución	Fase de la comunicación
Acceso Fraudulento	Autenticación de usuarios y verificación de equipos	Cada registro en la red; cada tentativa de llamada; obtención de servicios suplementarios
Escucha por usuarios no autorizados	Cifrado variable con el tiempo	Durante la llamada

Seguridad en el establecimiento de la llamada

- ▶ **PROBLEMA:**

- ▶ Durante la conexión no se cifra la información pues no se han transmitido aún los parámetros necesarios para el cifrado.

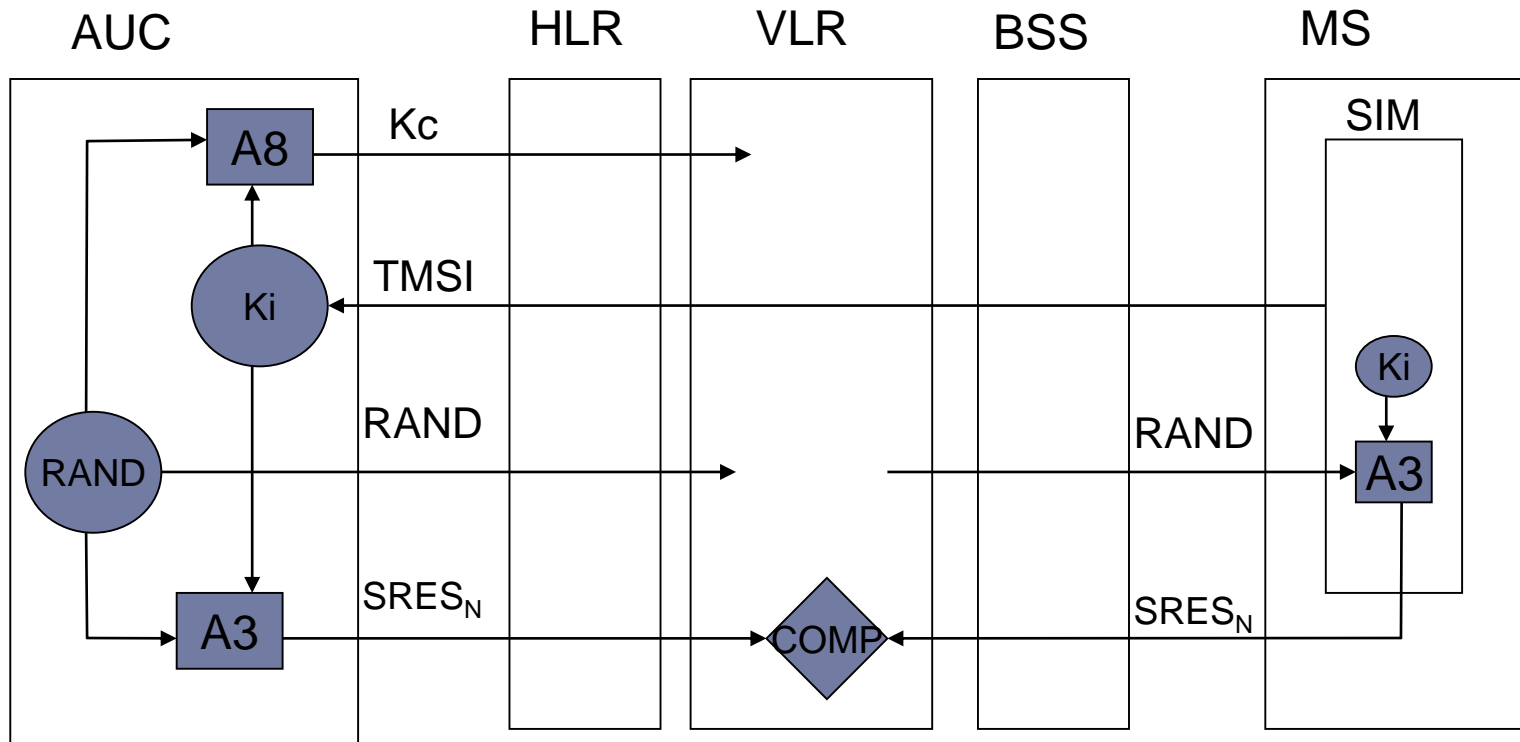
- ▶ **SOLUCION:**

- ▶ Una vez realizado el registro inicial, cualquier conexión de la MS con la red utiliza una **Identidad Prestada Temporalmente** a la MS (TMSI).
- ▶ Esto imposibilita la extracción de la identidad real por cualquier agente que escuche el canal de señalización.

Proceso de Autenticación en GSM

- ▶ Permite verificar si la MS que pretende una conexión está habilitada para ello.
- ▶ Claves usadas:
 - ▶ K_i : Clave de autenticación individual de abonado. Se almacena en el centro de autenticación (AUC) y en la tarjeta SIM del abonado.
 - ▶ K_c : Clave de cifrado para la transmisión
- ▶ Algoritmos usados:
 - ▶ A3: Algoritmo para la autenticación. Se ejecuta en el AUC y en la MS (lo almacena en la SIM).
 - ▶ A8: Algoritmo para la generación de la clave de cifrado. Residente en el AUC.

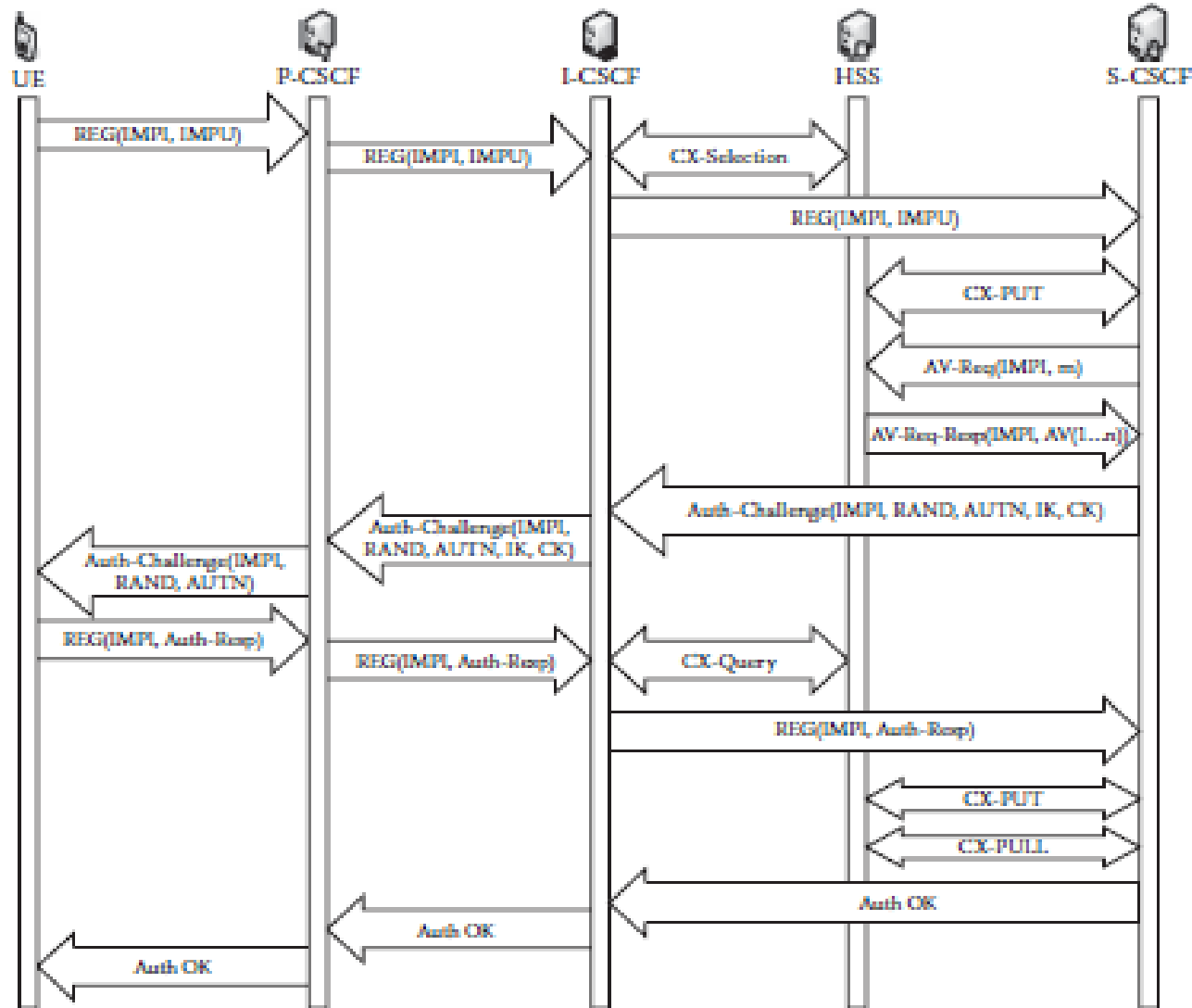
Proceso de Autenticación en GSM



Validación del aparato telefónico

- ▶ La MSC solicita a la MS su IMEI
- ▶ La MS envía su IMEI que es re-enviado hasta el EIR (Equipment Identification Register)
- ▶ El EIR verifica el IMEI en sus listas:
 - ▶ Lista Blanca: Las MS autorizadas
 - ▶ Lista Gris: Las MS con funcionamiento limitado
 - ▶ Lista Negra: Las MS que no pueden usar la red ya sea por robo o por falta de pago

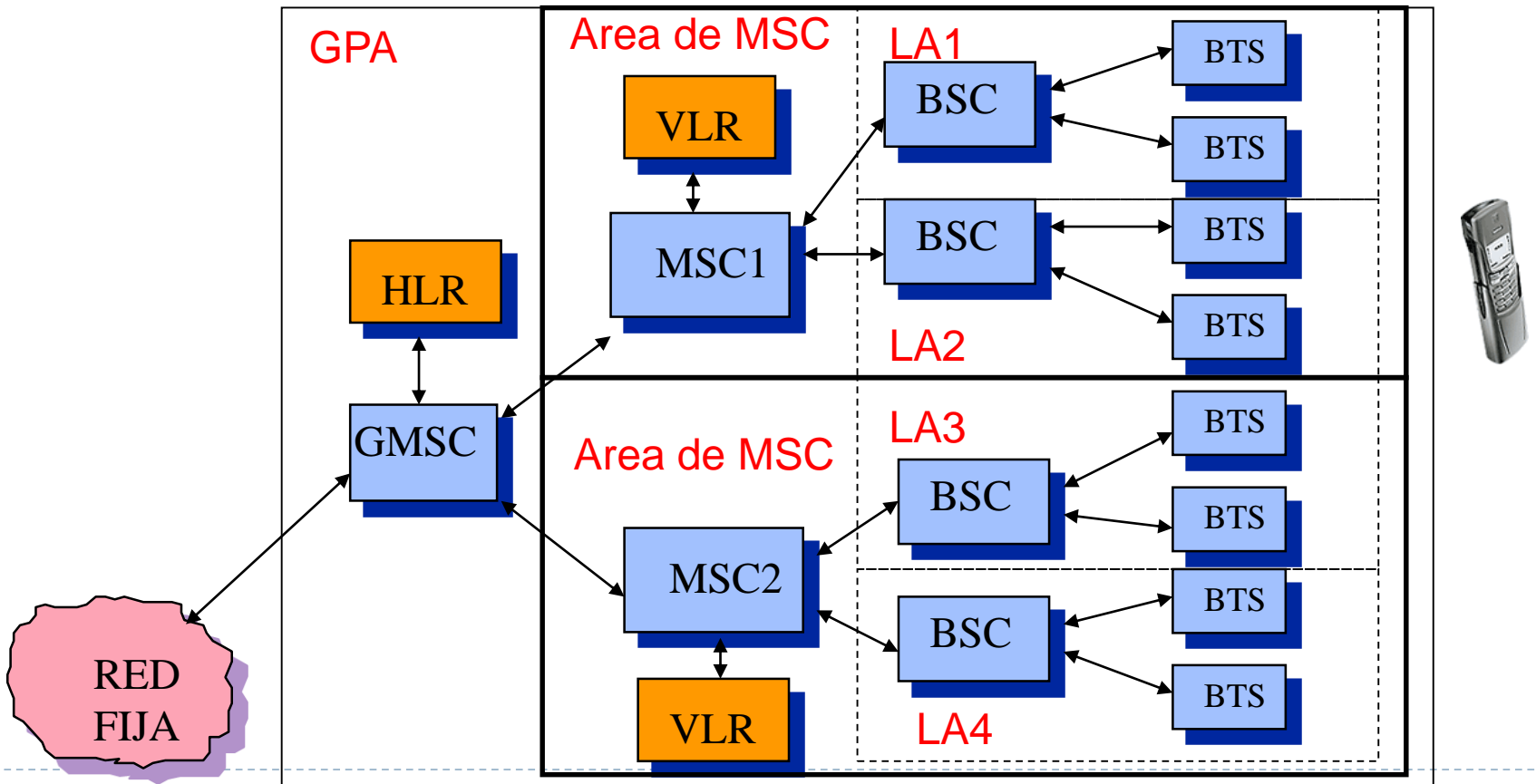
Proceso de autenticación en EPS/IMS



Registro y Localización de la MS

- ▶ Debe existir una organización jerárquica de la red
 - ▶ GPA: GSM PLMN Area, comprende un país
 - ▶ Area de MSC: Area que controla una MSC
 - ▶ LA: Location Area, comprende varias celdas
- ▶ Las funciones de registro y localización se realizan en el HLR y en el VLR.
- ▶ VLR: Almacena información de las MS que se encuentran temporalmente en el Area de una MSC.
- ▶ Hay un solo HLR que encamina las llamadas de otras redes hacia el MSC en cuyo VLR esté registrada la MS.

Organización jerárquica de una red GSM



Registro en una red GSM

- ▶ Qué celdas se utilizan para gestionar una llamada desde/hacia una MS?
 - ▶ Problema: Si se gestiona por una sola celda, puede perderse al haber un traspaso. Si se gestiona por todas las celdas de una GPA se inundaría la red con tráfico de señalización.
- ▶ Solución: La llamada se gestiona a través de todas las celdas que componen una *Location Area*. (compromiso Seguridad-eficacia)

Movilidad en una red GSM

- ▶ Toda MS, al registrarse en la red queda inscrita en una LA, pudiendo moverse libremente a través de ella sin necesidad de un nuevo registro.
- ▶ La MS únicamente actualiza su localización cuando, en su desplazamiento, pase de una LA a otra distinta.

Identificación del camino de una comunicación

- ▶ Para identificar el camino que debe seguir una comunicación con una MS se utilizan códigos de identificación para las diferentes zonas y áreas que atraviesa dicha comunicación:
 - ▶ LAI: Location Area Identification
 - ▶ LAI = MCC + MNC + LAC
 - ▶ MCC: Mobile Country Code (como en la IMSI)
 - ▶ MNC: Mobile Network Code (como en la IMSI)
 - ▶ LAC: Location Area Code
 - ▶ CGI: Cell Global Identification
 - ▶ CGI = LAI + Cell Identification

Situaciones de Registro

- ▶ Puede producirse un registro de la MS en tres situaciones:
 - ▶ Conexión/Desconexión a la red
 - ▶ Cambio de LA
 - ▶ Actualización periódica de la localización

Situaciones de Registro

▶ **Conexión/Desconexión a la red:**

- ▶ La MS debe enviar un mensaje ATTACH a la red para conectarse, el cual sirve para realizar el registro.
- ▶ La MS debe enviar un mensaje DETACH a la red para suprimir la inscripción en el respectivo VLR.

Situaciones de Registro

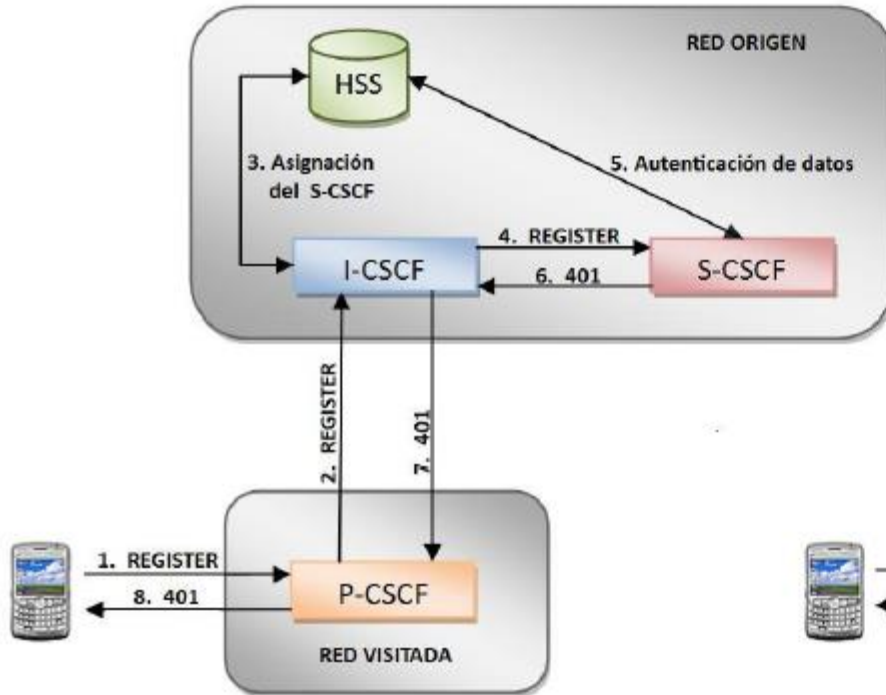
▶ **Cambio de LA:**

- ▶ Cuando una MS abandona una LA e ingresa a otra, debe realizar un nuevo registro.
- ▶ Procedimiento:
 - ▶ Las BTS difunden la identidad de la LA a la que pertenecen por el canal BCCH.
 - ▶ La MS escucha esta información de todas las BTS con cobertura en ese punto y detecta la intensidad de la portadora de todas ellas.
 - ▶ Si decide cambiarse a una BTS de otra LA, iniciará un nuevo proceso de registro.
 - ▶ Si la nueva BTS pertenece además a otra zona de MSC, deberá hacerse una inscripción en el nuevo VLR.

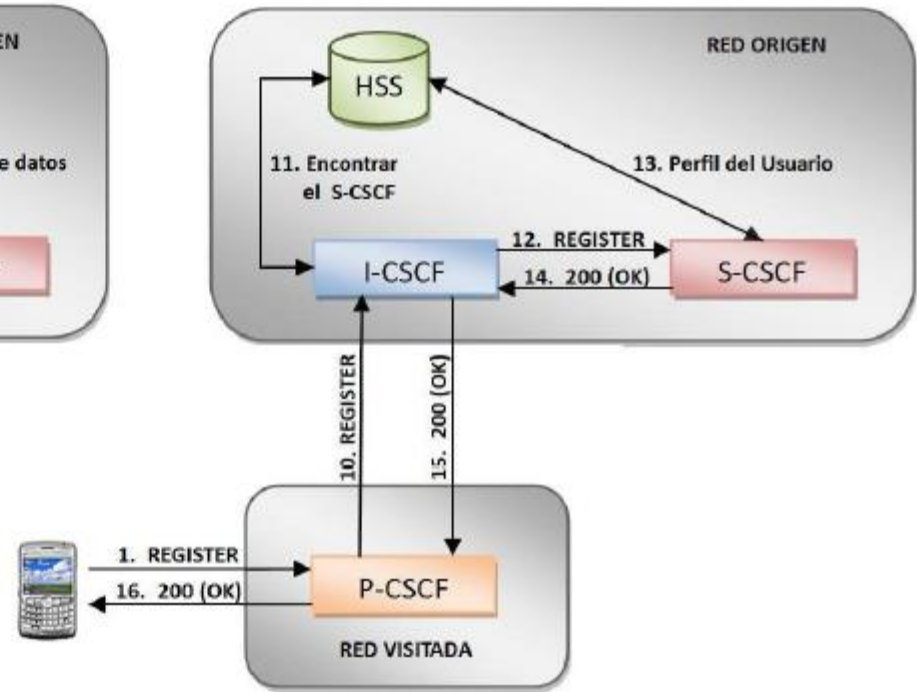
Situaciones de Registro

- ▶ **Actualización periódica de la localización:**
 - ▶ Busca restaurar los datos de los abonados en el HLR y VLR o pérdida de mensajes de desconexión en caso de situaciones anómalas (Fallos en HLR o VLRs).
 - ▶ La MS ejecuta un procedimiento de registro con un período elegido y difundido por la red (puede variar entre 6 minutos y 25 horas, o infinito si se quiere eliminar)
 - ▶ La MS tiene un temporizador de la actualización que indica el momento de realizarla.
 - ▶ Cada vez que la MS realiza o recibe una llamada, reinicia el temporizador.
 - ▶ Cuando se desconecta la MS se guarda en la memoria el valor del temporizador.

Procedimiento de Registro y Autenticación en EPS/IMS



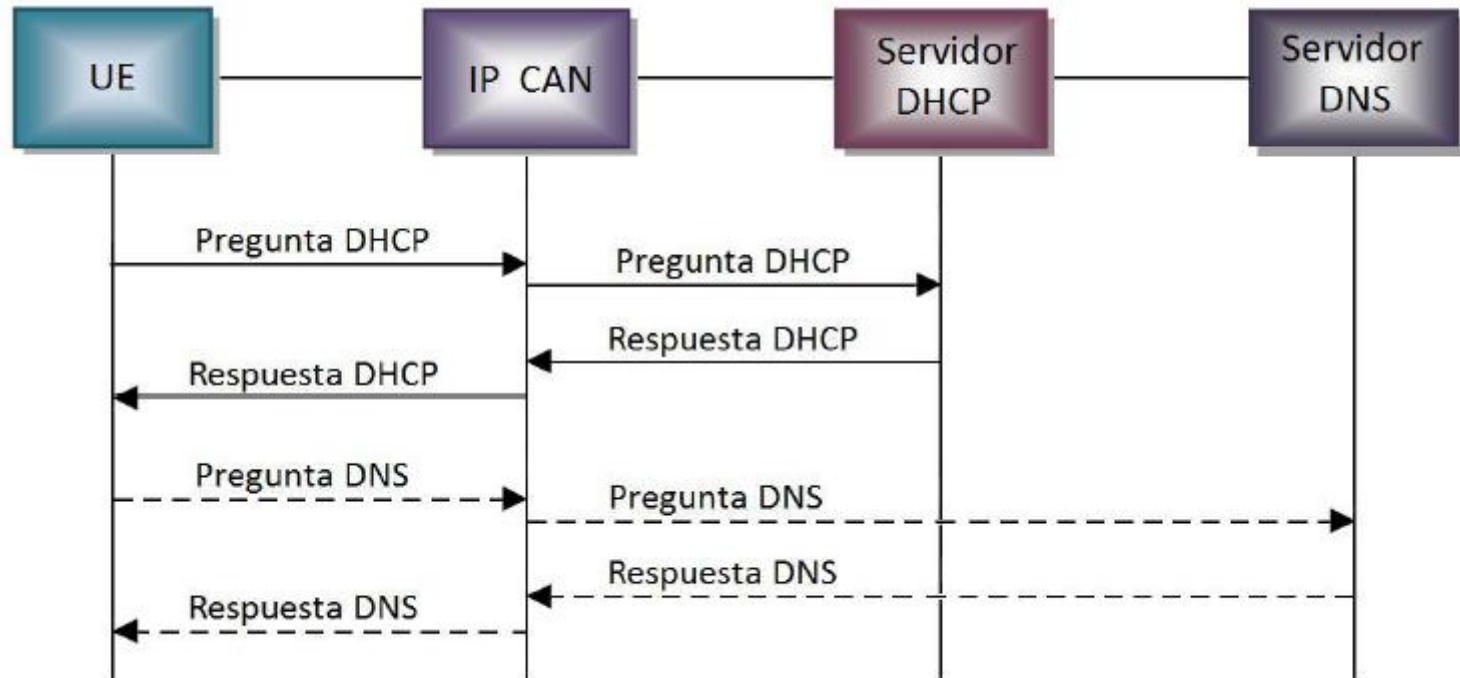
La red reta al Equipo de Usuario.
desafío.



El equipo de usuario responde el



Descubrimiento del P-CSCF



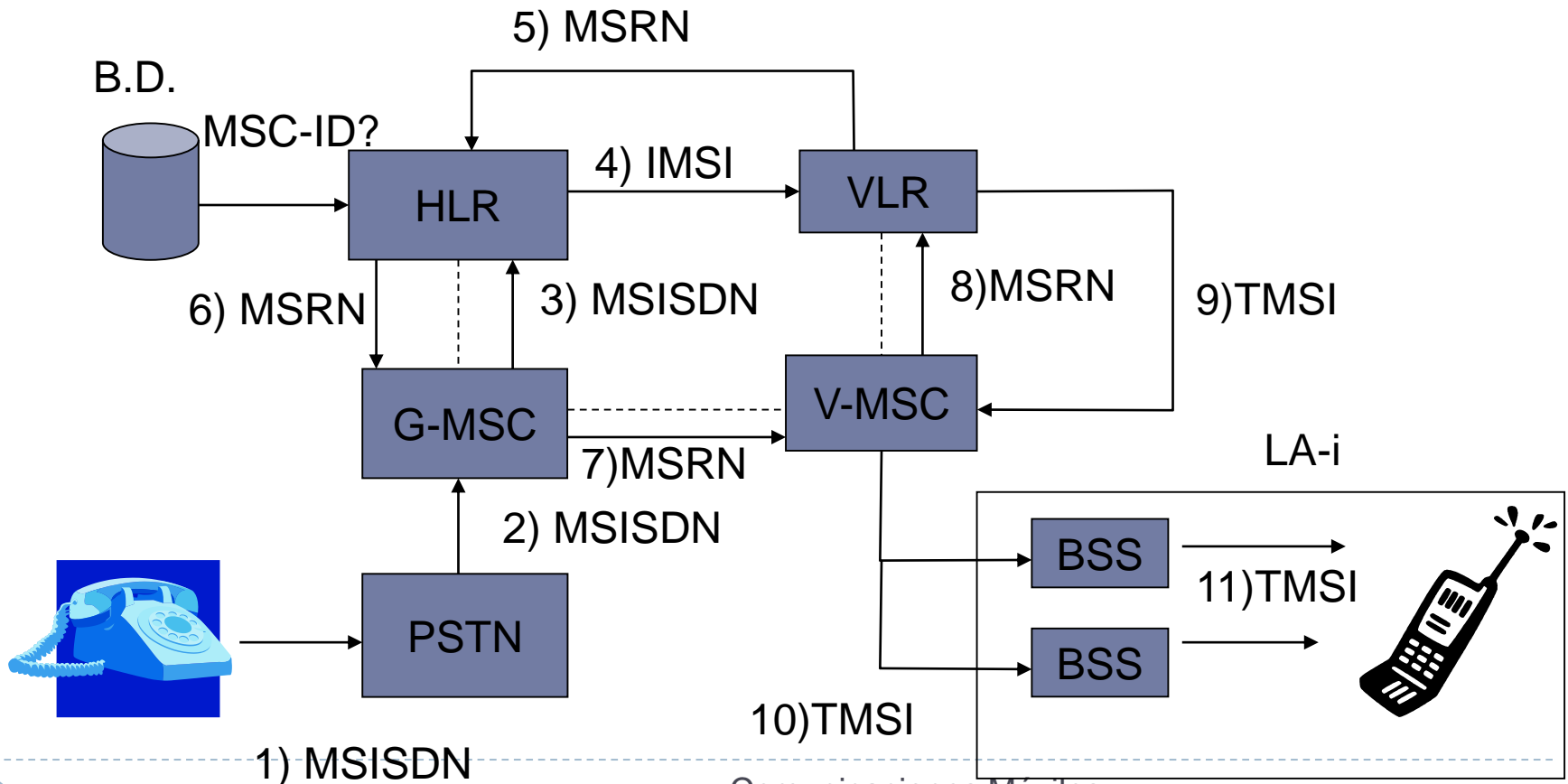
Objetivo: Obtener la dirección IP del P-CSCF por parte del Equipo de Usuario



Encaminamiento de una llamada PSTN a PLMN: Búsqueda de la MS

- ▶ Supongamos una llamada entrante desde una PSTN hacia una MS de una red GSM.
- ▶ Las redes son distintas y con sistemas de numeración diferentes. Se requiere conversión de numeración.
- ▶ El número MSISDN de la MS contiene un número de abonado, el cual a su vez tiene una parte que hace referencia a la MSC de la que depende la localidad donde se suscribió a la red (Home-MSC ó H-MSC).
- ▶ Para un caso más general, suponemos que la MS no está en su H-MSC, sino en otra diferente (Visited MSC ó V-MSC).
- ▶ El VLR de la V-MSC asignará un TMSI a la MS.

Proceso llamada PSTN a PLMN: Búsqueda de la MS



Gestión de las llamadas

Introducción

- ▶ Comprende las funciones necesarias para el establecimiento, mantenimiento y seguridad durante la comunicación.
- ▶ Hay tres casos de llamada:
 - ▶ MS a PSTN
 - ▶ PSTN a MS
 - ▶ MS a MS

Fases de una llamada en GSM

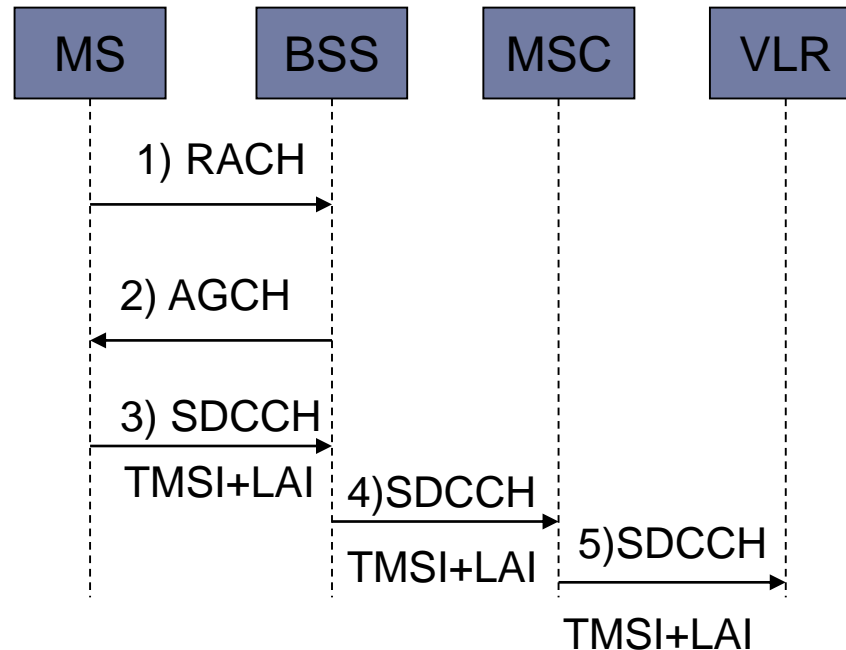
▶ Caso: MS a PSTN

- ▶ Petición del servicio por la MS
- ▶ Autenticación
- ▶ Cifrado
- ▶ Validación del equipo
- ▶ Establecimiento de la comunicación
- ▶ Traspaso
- ▶ Liberación

▶ Caso: PSTN a MS

- ▶ Búsqueda de MS
- ▶ Aviso a la MS destino
- ▶ Autenticación
- ▶ Cifrado
- ▶ Validación del equipo
- ▶ Establecimiento de la comunicación
- ▶ Traspaso
- ▶ Liberación

Llamada MS a PSTN: Petición del servicio por la MS

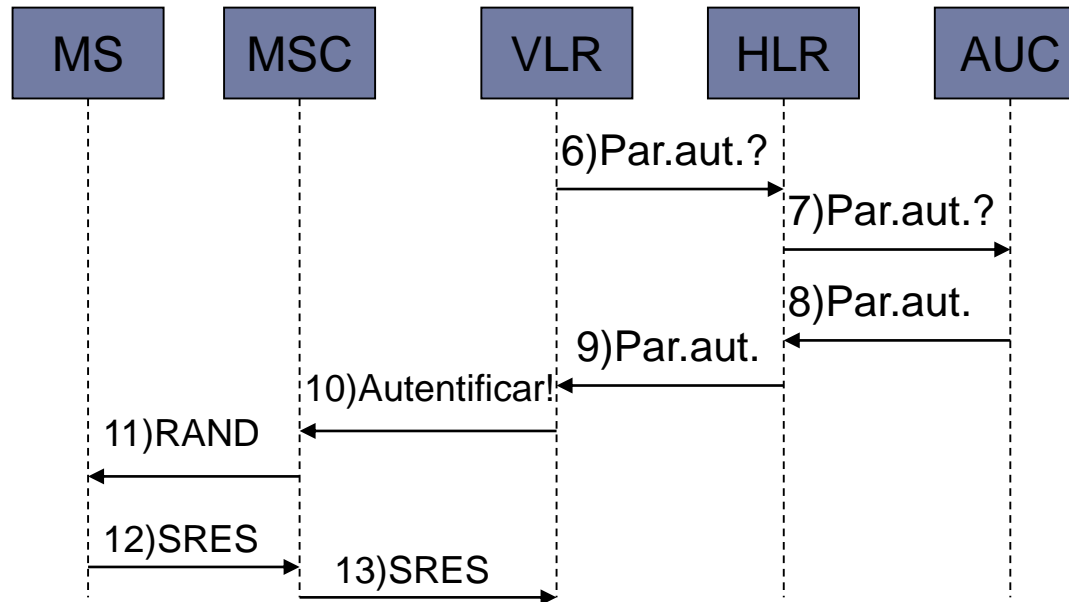


RACH: Random Access channel (msg: solíc. Canal)

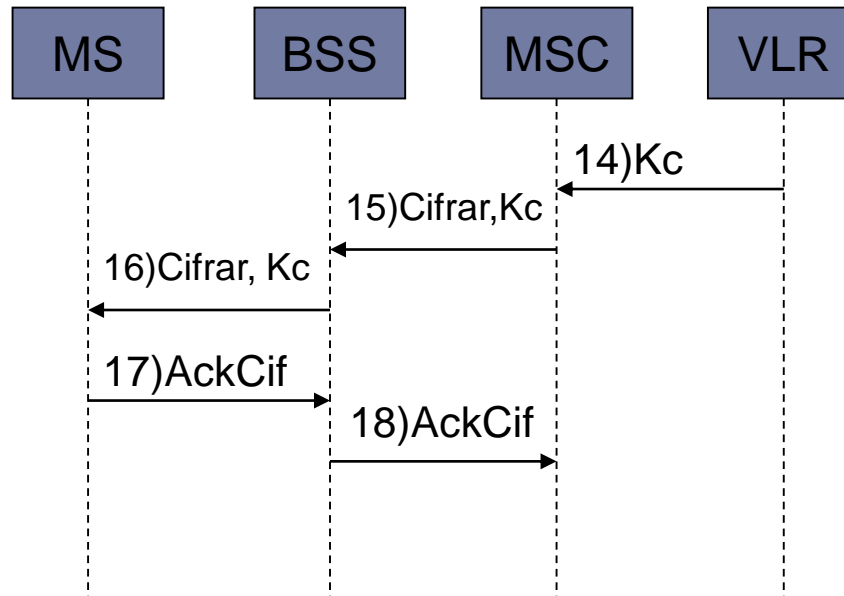
AGCH: Access Grant Channel (msg: notificación. Asignación canal)

SDCCH: Stand Alone Dedicated Control Channel

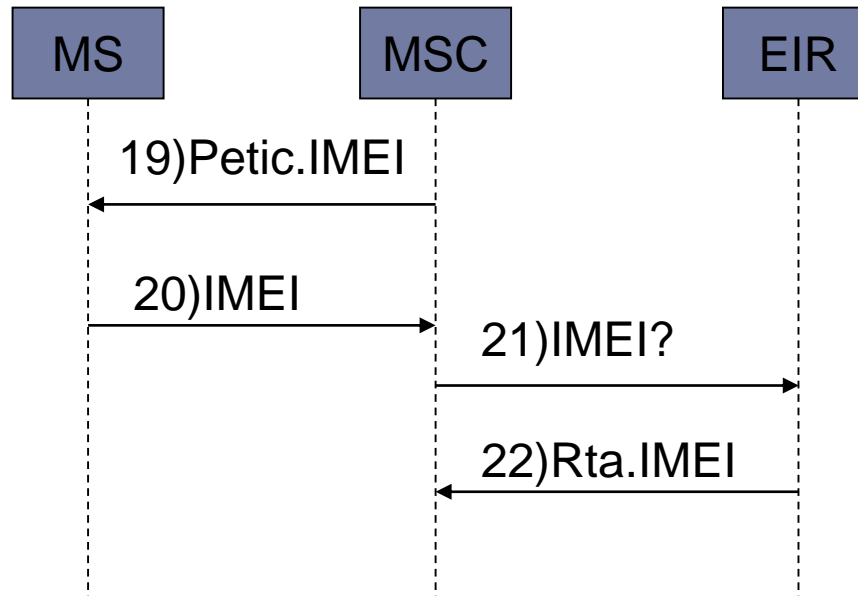
Llamada MS a PSTN: Autenticación



Llamada MS a PSTN: Cifrado

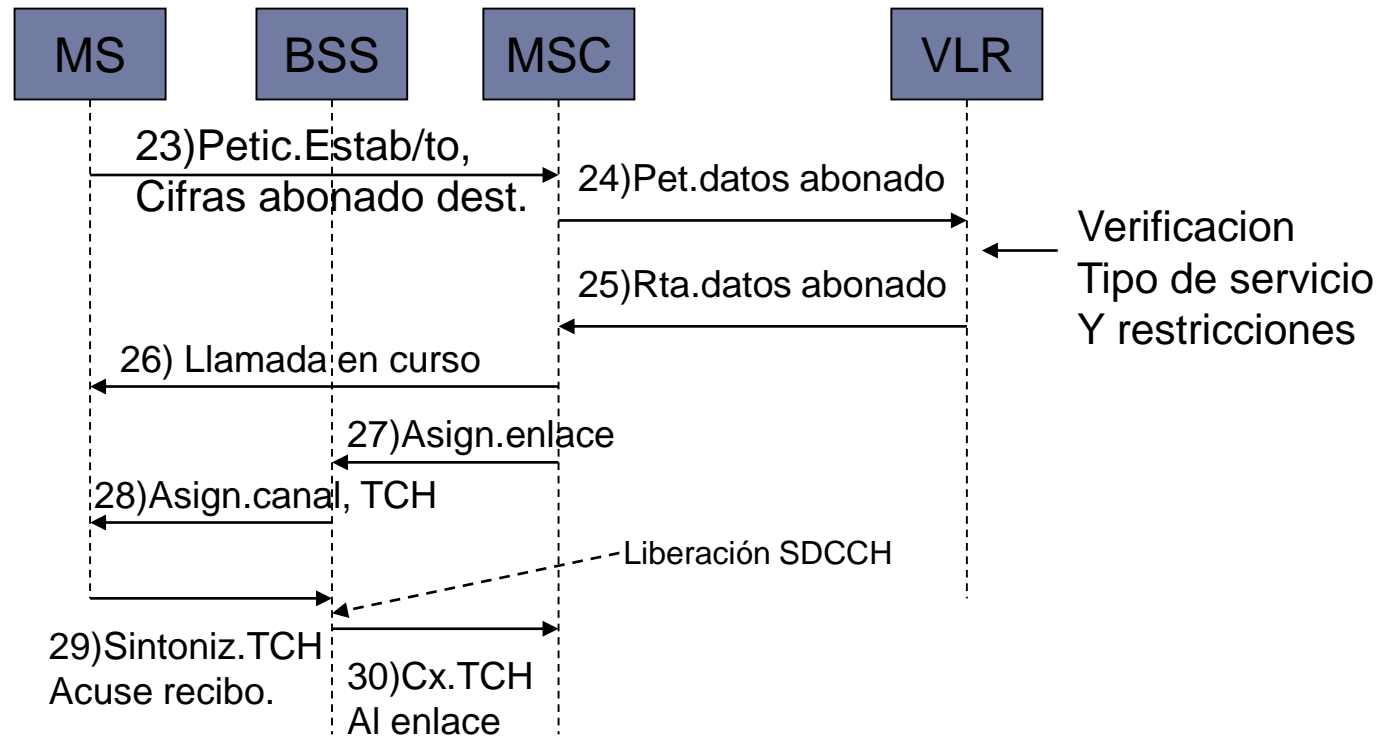


Llamada MS a PSTN: Validación



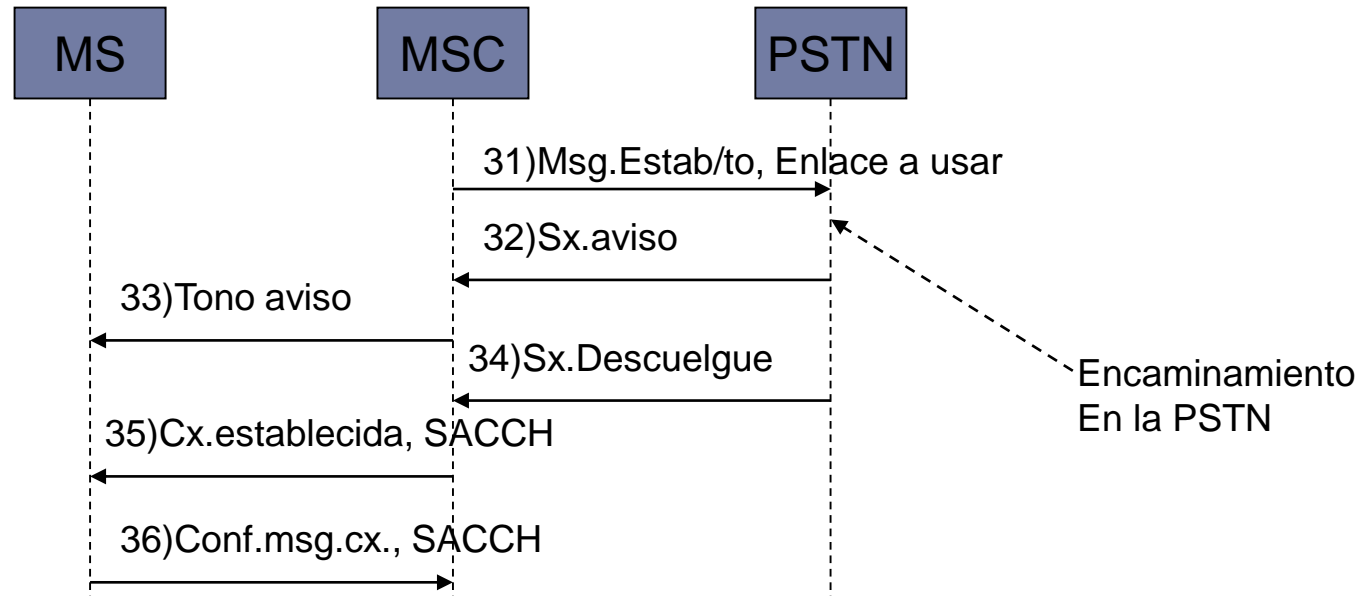
Este procedimiento se realiza utilizando el cifrado con la clave Kc

Llamada MS a PSTN: Establecimiento de la llamada en la MS



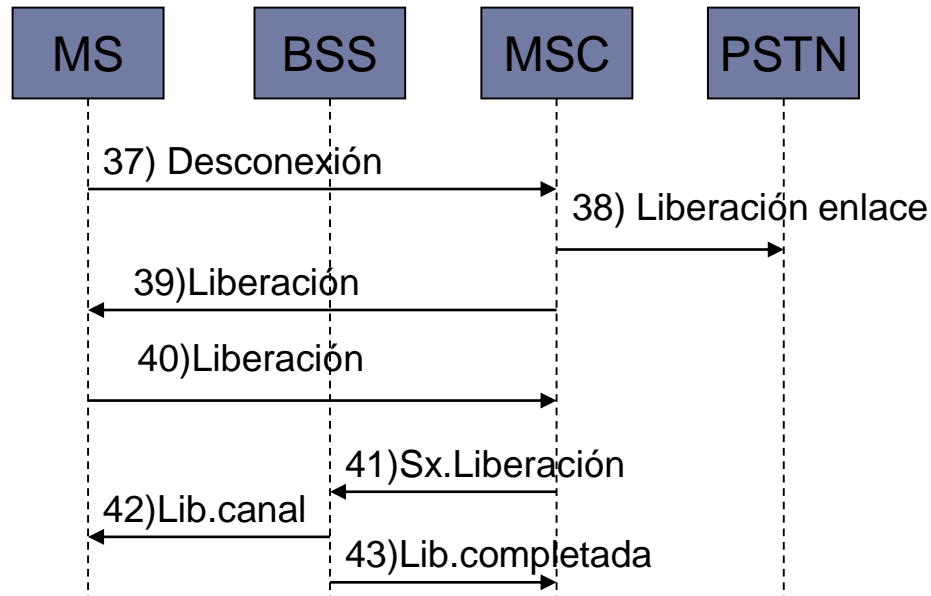
TCH: Traffic Channel

Llamada MS a PSTN: Establecimiento de la llamada en la red fija

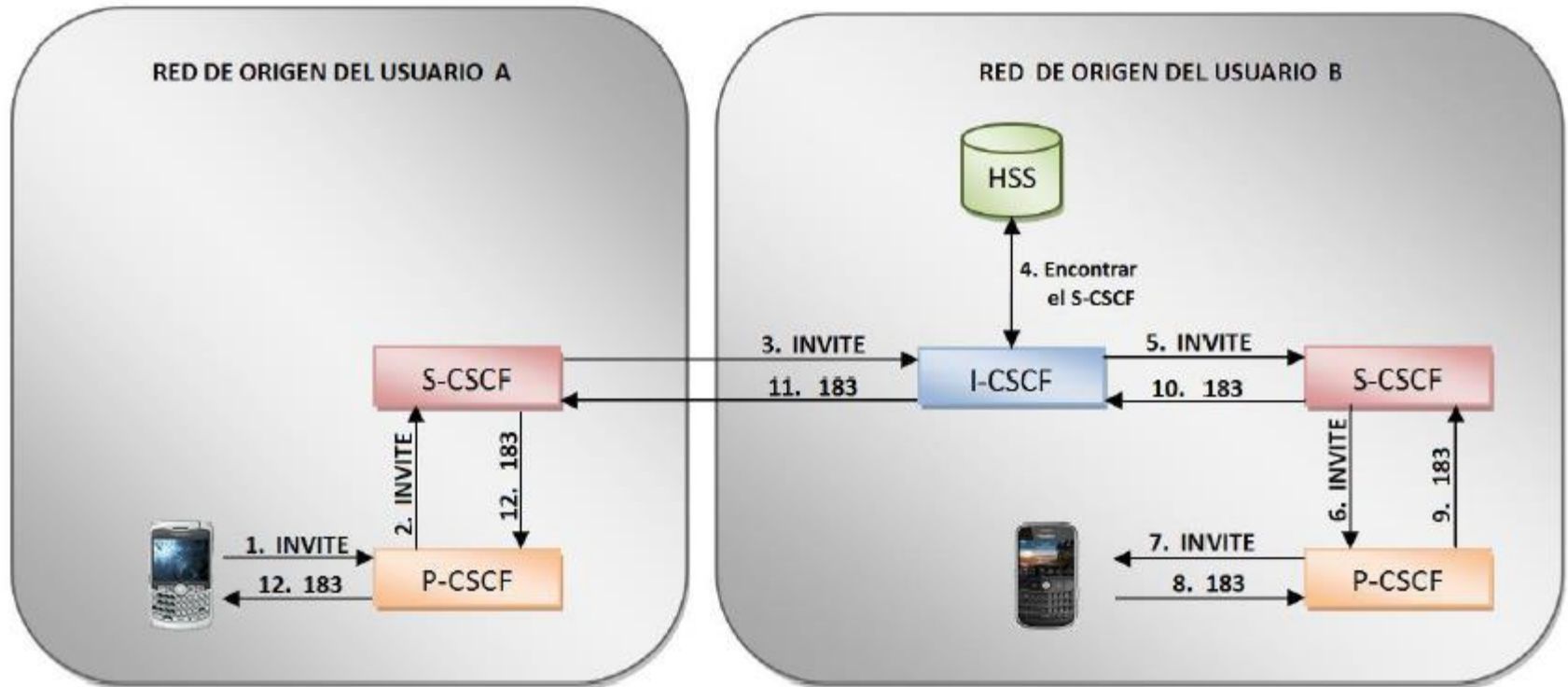


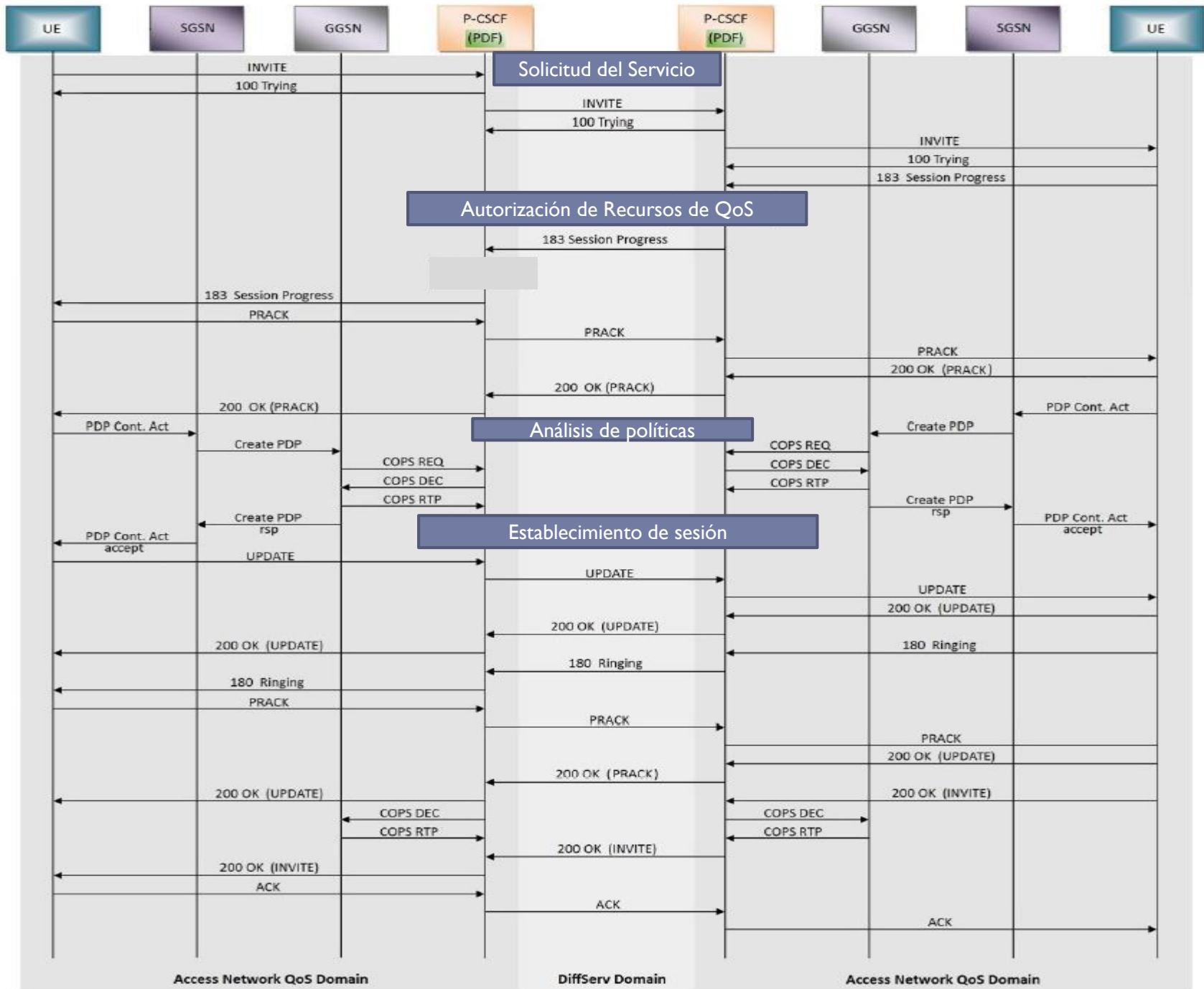
SACCH: Slow Asociated Control Channel
(Señalización de las llamadas)

Llamada MS a PSTN: Liberación



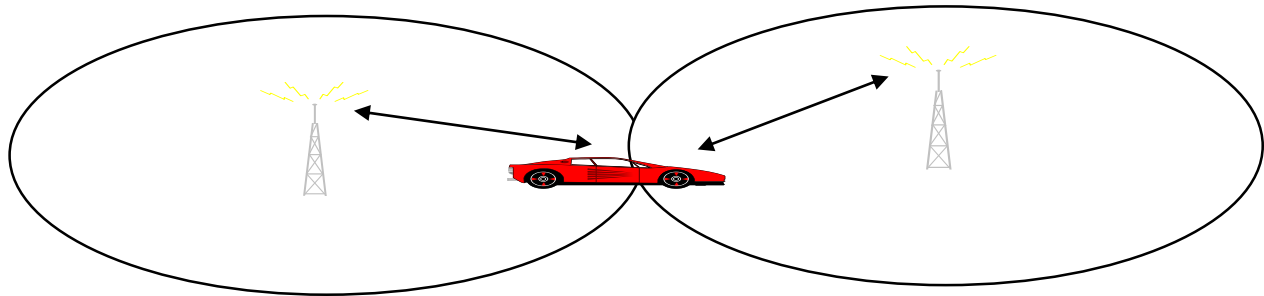
Establecimiento de la sesión en UMTS/IMS





Traspaso (Handoff o Handover)

- ▶ El traspaso es un mecanismo previsto para asegurar la calidad y continuidad de una llamada en curso cuando existe riesgo de que se pierda o de que su calidad se degrade a un nivel intolerable.
- ▶ También se usa para mantener el equilibrio de tráfico en las celdas y mantener el canal radio.
- ▶ Durante el traspaso se realiza la conmutación de la llamada de una celda a otra.



Traspaso

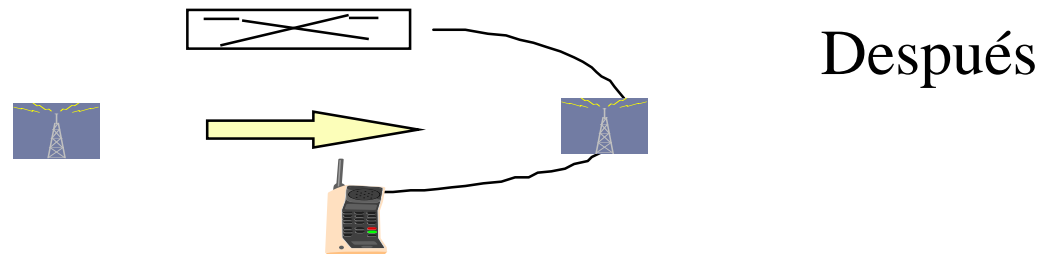
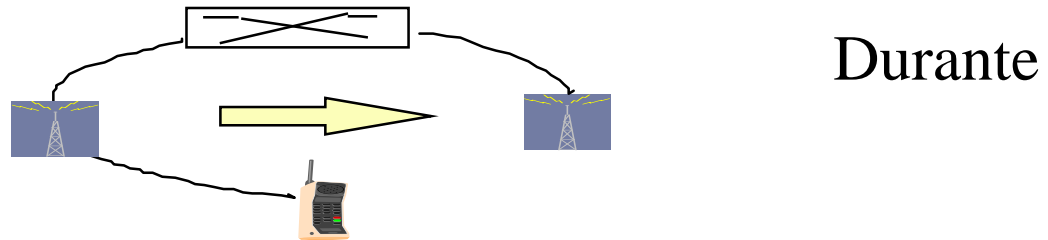
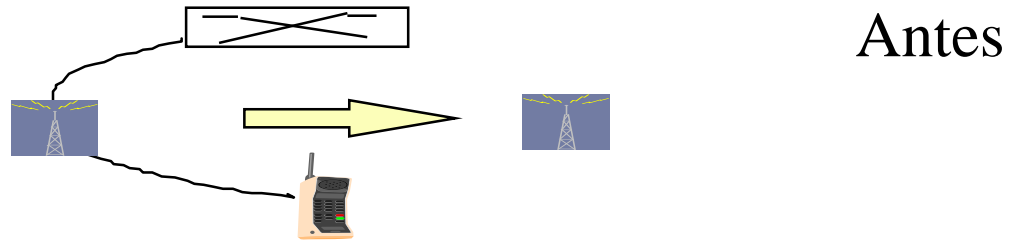
- ▶ **Casos en que se realiza traspaso:**
 - ▶ Intensidad de la señal reducida
 - ▶ Calidad de la señal mediocre
 - ▶ Mantenimiento del canal radio
 - ▶ Existencia de una celda con mejores posibilidades de atender la comunicación
 - ▶ Equilibrio de tráfico

Clases de traspaso

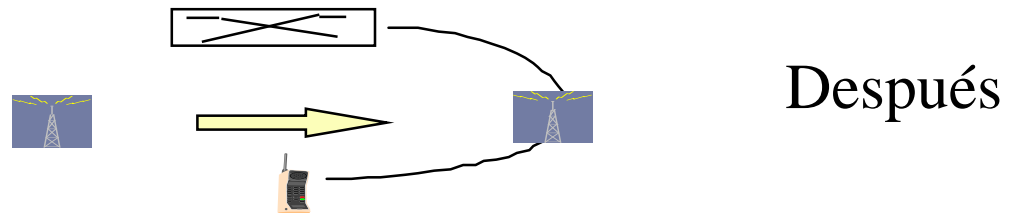
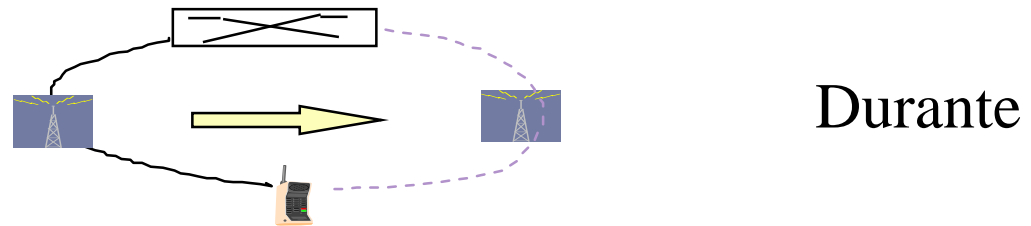
- ▶ Traspaso Interno (Dentro de una misma BSS). Puede suceder:
 - ▶ Entre canales de una misma BS
 - ▶ Entre distintas BS: Entre dos sectores de una misma BTS o entre diferentes BTS de una misma BSC.
- ▶ Traspaso externo (entre BSS's). Puede suceder:
 - ▶ Entre BTS de la misma MSC pero diferentes BSCs.
 - ▶ Entre MSC diferentes

Cada tipo de traspaso tiene exigencias de señalización diferentes.
Se explicará el caso más general:
Traspaso entre MSC's debido al deterioro del nivel/calidad de la señal.

Clases de traspaso: HARD HANDOVER



Clases de traspaso: SEAMLESS HANDOVER



Medidas de señal para el traspaso

- ▶ Ciertos sistemas se basan en medidas realizadas en la BS únicamente (TACS)
- ▶ En GSM se efectúan medidas tanto en la BS (Up-Link o U/L) como en la MS (Down-Link o D/L).
- ▶ A este tipo de traspaso se le conoce como MAHO (Mobile Assisted Handover).

Medidas de señal para el traspaso

- ▶ La MS mide dos magnitudes en el D/L:
 - ▶ Nivel de Recepción (RXLEV). Está relacionado con la potencia de la señal. Se expresa como un número entre 0 y 63.
 - ▶ Calidad de la señal (RXQUAL). Está relacionada con el BER. Se expresa como un número entre 0 y 7.

Medidas de la señal para el traspaso

RXLEV	Potencia(dBm)
0	<-100
1	-100 a -109
2	-109 a -108
-	-
61	-50 a -49
62	-49 a -48
63	>-48

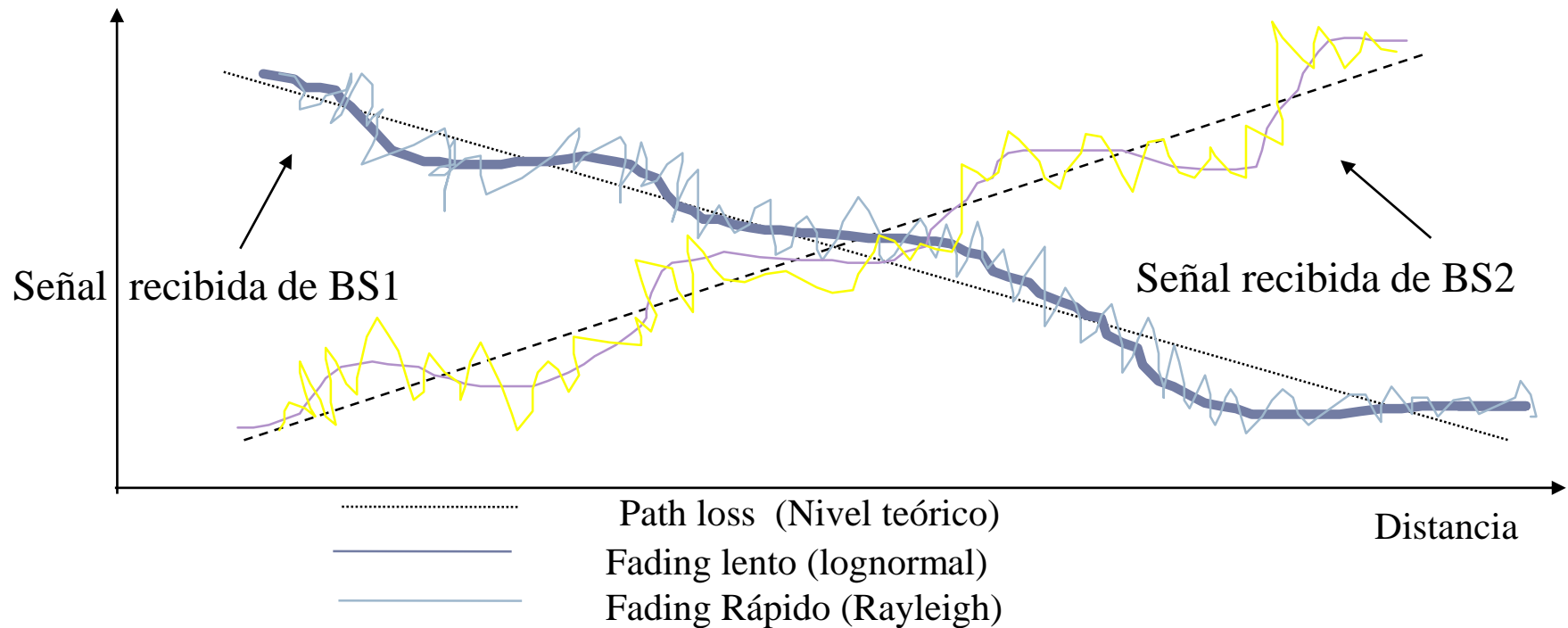
RXQUAL	BER (%)
0	<0.2
1	0.2-0.4
2	0.4-0.8
3	0.8-1.6
4	1.6-3.2
5	3.2-6.4
6	6.4-12.8
7	>12.8

Medidas de señal para el traspaso

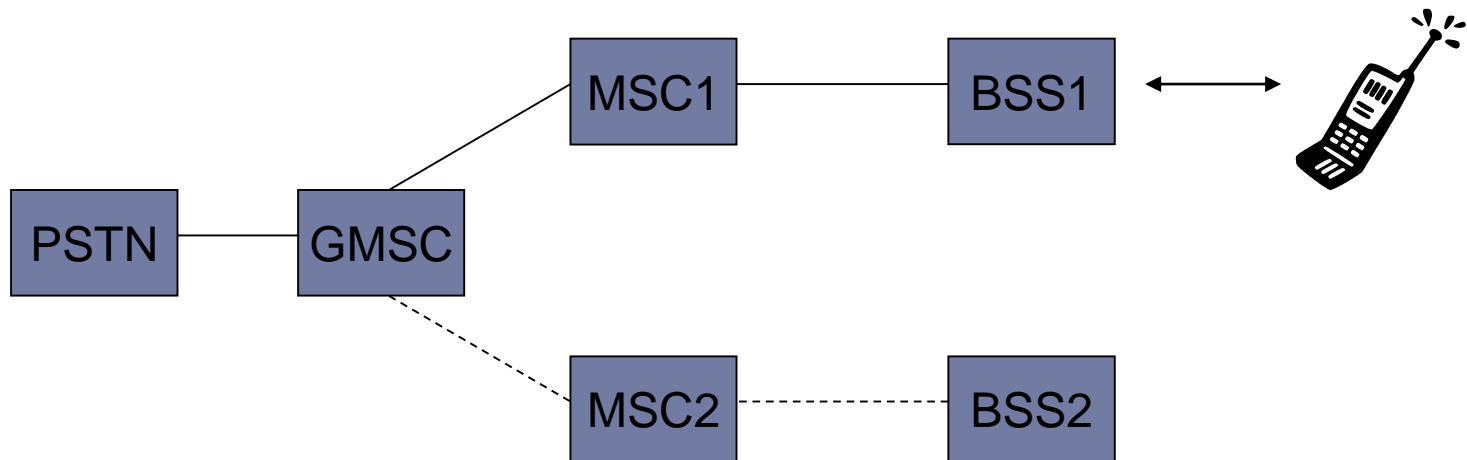
- ▶ Cada período de medición comprende 104 tramas TDMA (0.48mseg).
- ▶ Durante este tiempo, la MS transmite a la BS la siguiente información (utilizando un canal especial denominado SACCH-Slow Associated Control Channel):
 - ▶ Valores promediado de 100 tramas del RXLEV y RXQUAL de la celda servidora
 - ▶ Valores de RXLEV de las portadoras piloto (BCCH-Broadcast Common Control Channel) más intensas de 6 celdas vecinas, junto con la identificación de dichas celdas (BSIC- Base Station Identification Code, de 6 bits).
- ▶ El BSIC se obtiene en la MSC del BCCH. Las BS difunden esta información.

Criterios para el traspaso

- ▶ Se produce un traspaso entre dos celdas cuando el RXLEV y RXQUAL son bajos en la celda servidora y en la celda destinataria RXLEV es mayor.
- ▶ Se produce un traspaso intracelular (entre pares radiocanal/intervalo) cuando, manteniéndose un buen RXLEV, se obtiene una mejora en la RXQUAL.

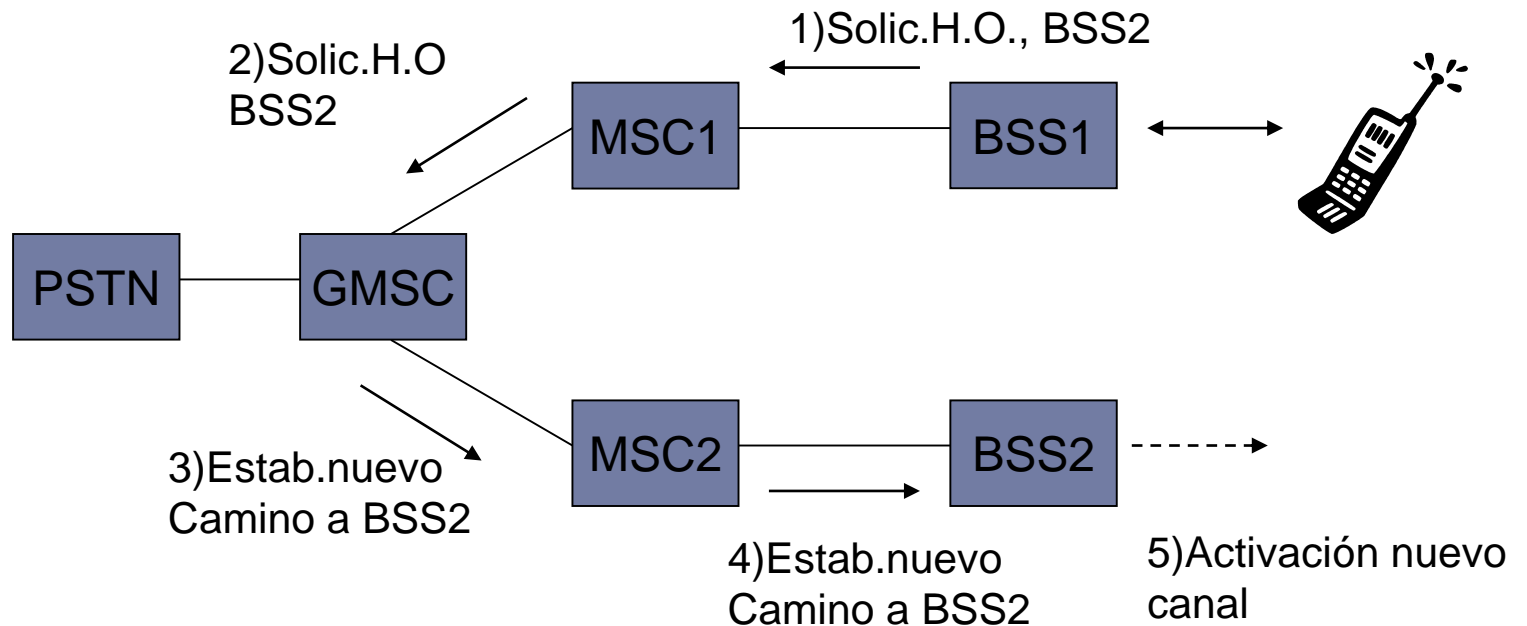


Traspaso entre MSCs: Fases



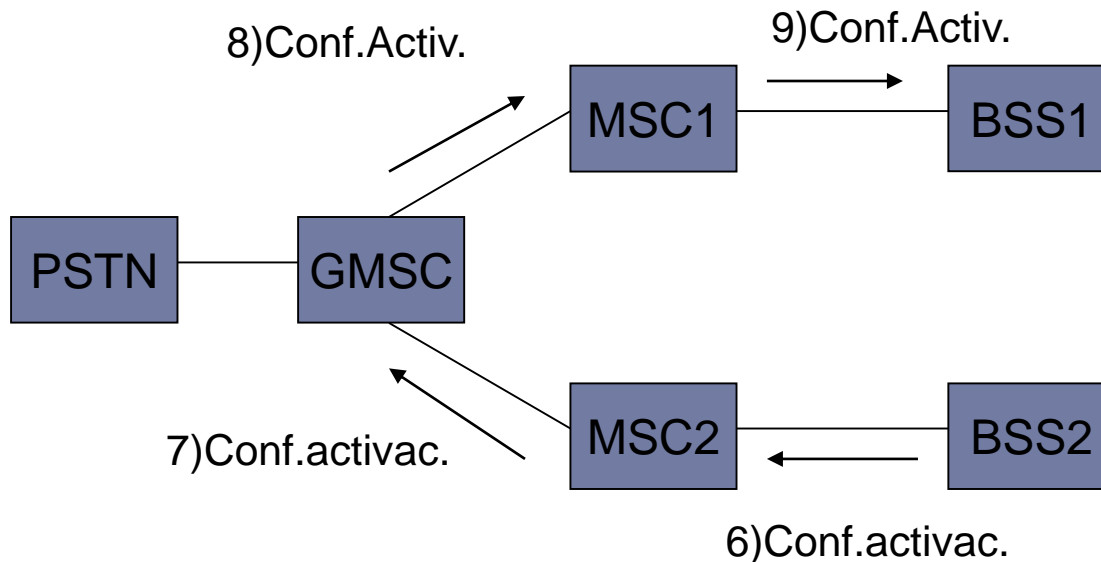
Camino Inicial de la llamada

Traspaso entre MSCs: Fases



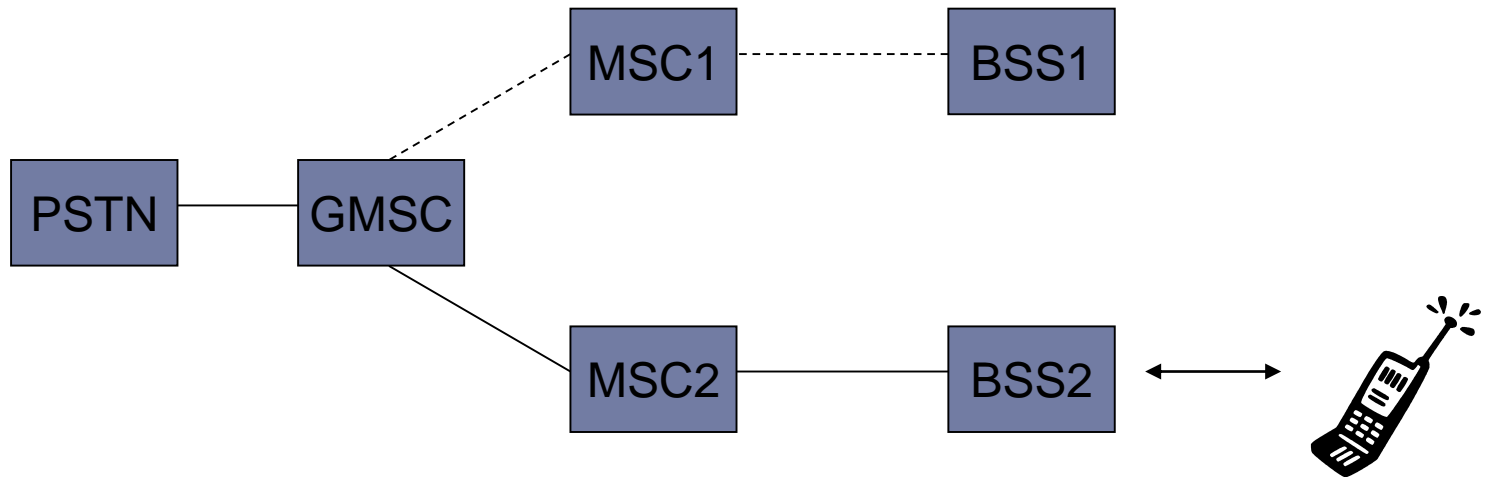
Solicitud de Handover

Traspaso entre MSCs: Fases



Asignación de recursos

Traspaso entre MSCs: Fases



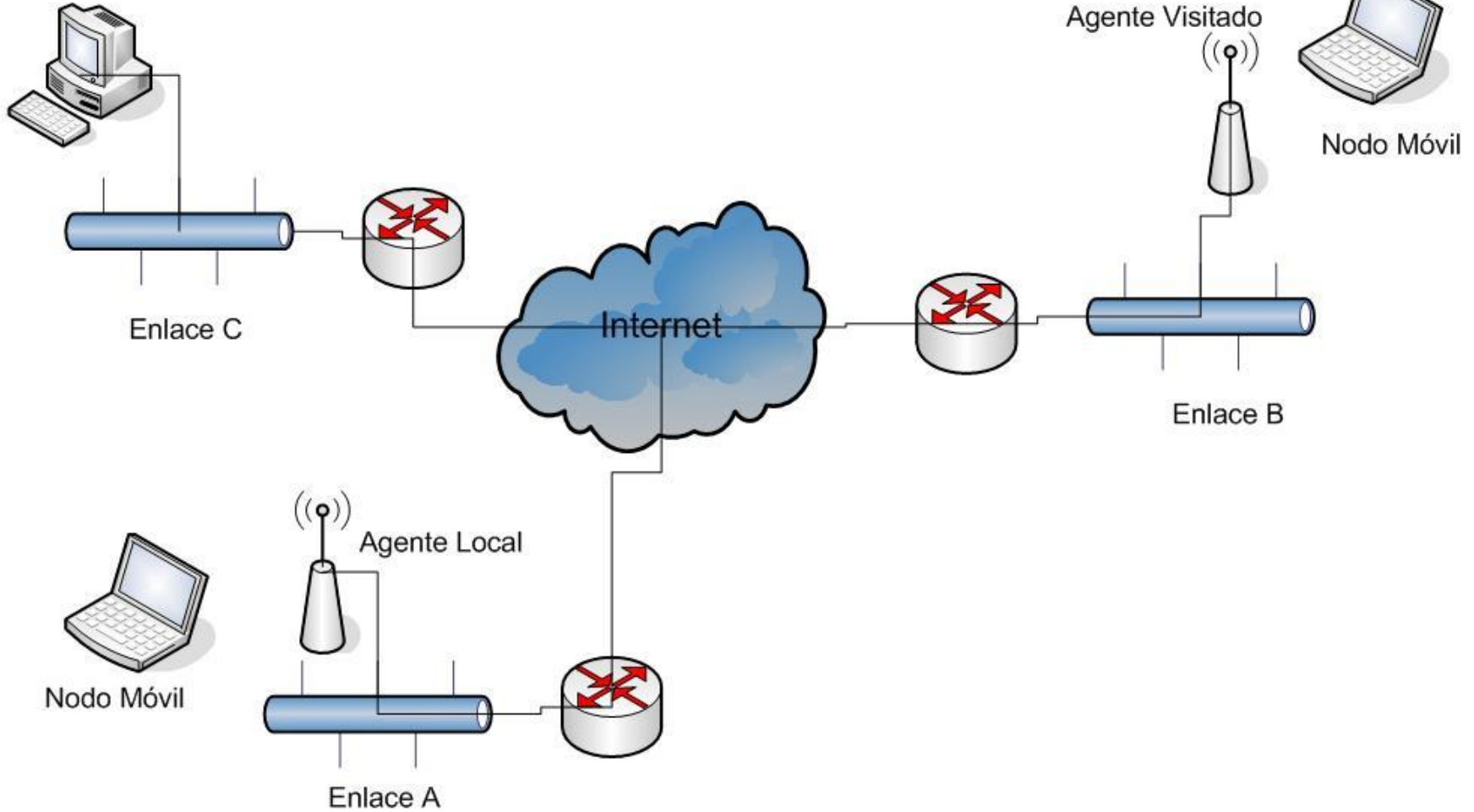
Liberación de los recursos

Traspaso en redes IP

- ▶ Se utilizan soluciones como:
 - ▶ Mobile IP (Macro-movilidad)
 - ▶ Hierarchical Mobile IP (Micro-movilidad)

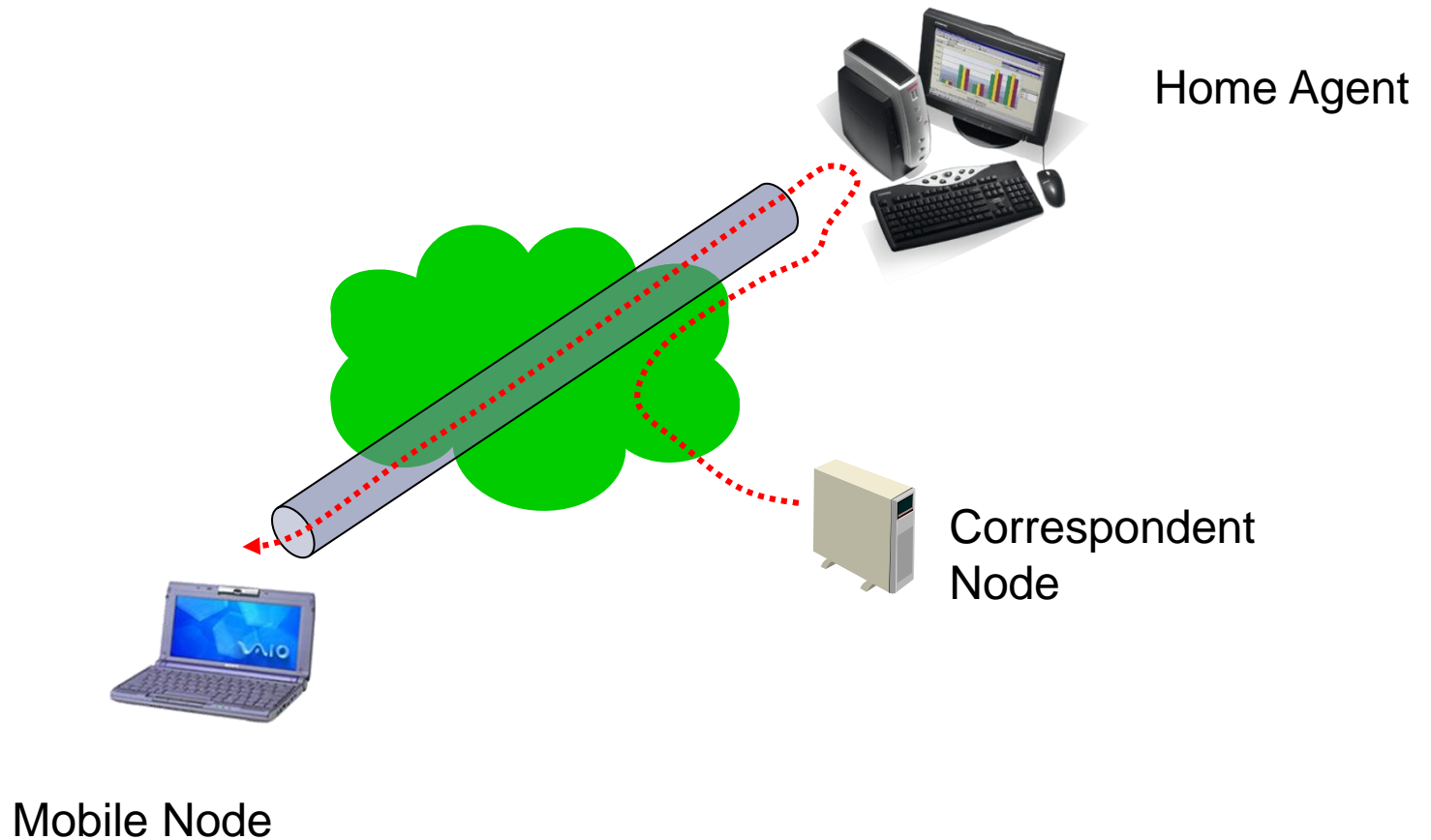
Mobile IP

Nodo Correspondiente

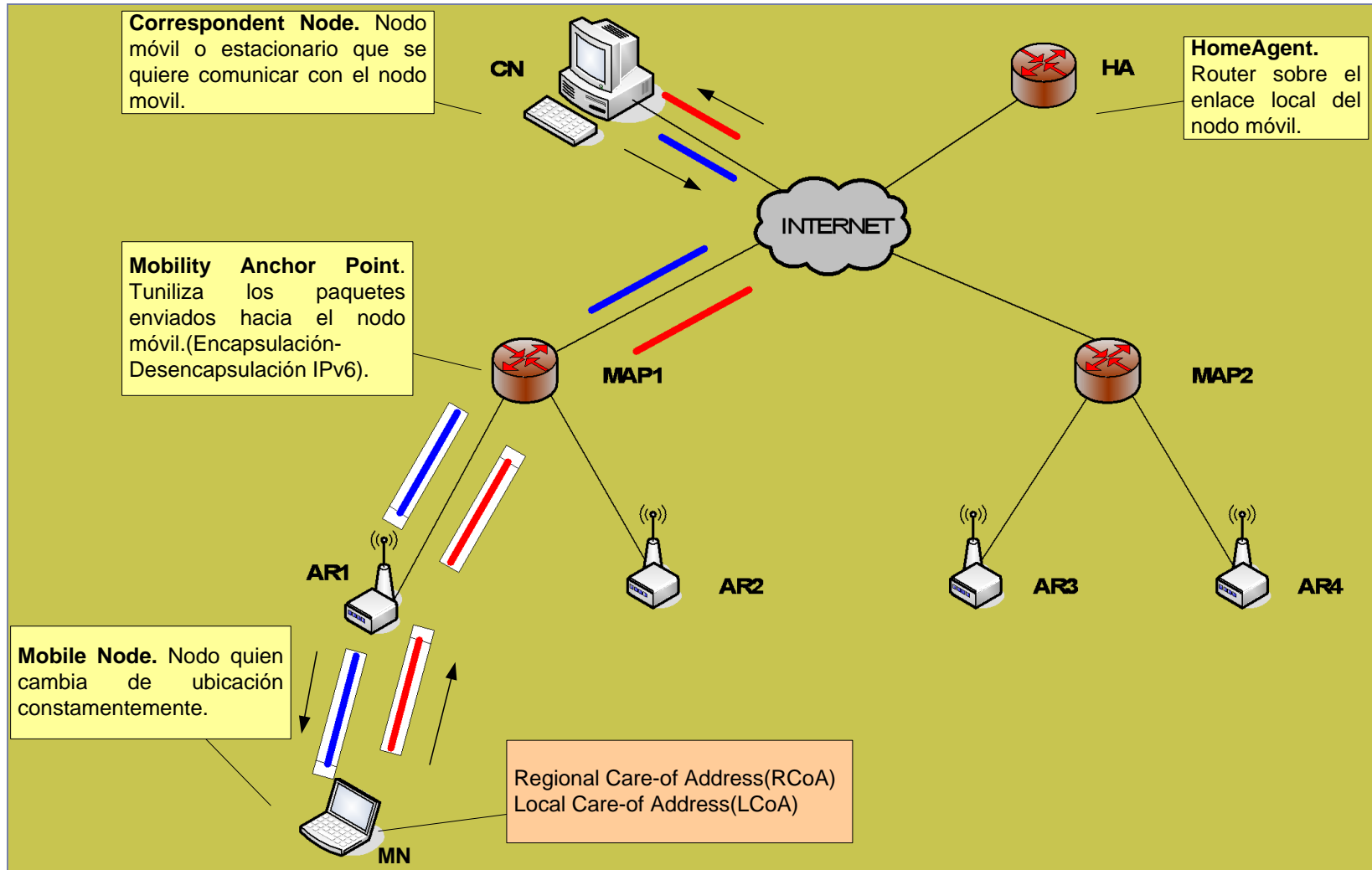


Mobile IP

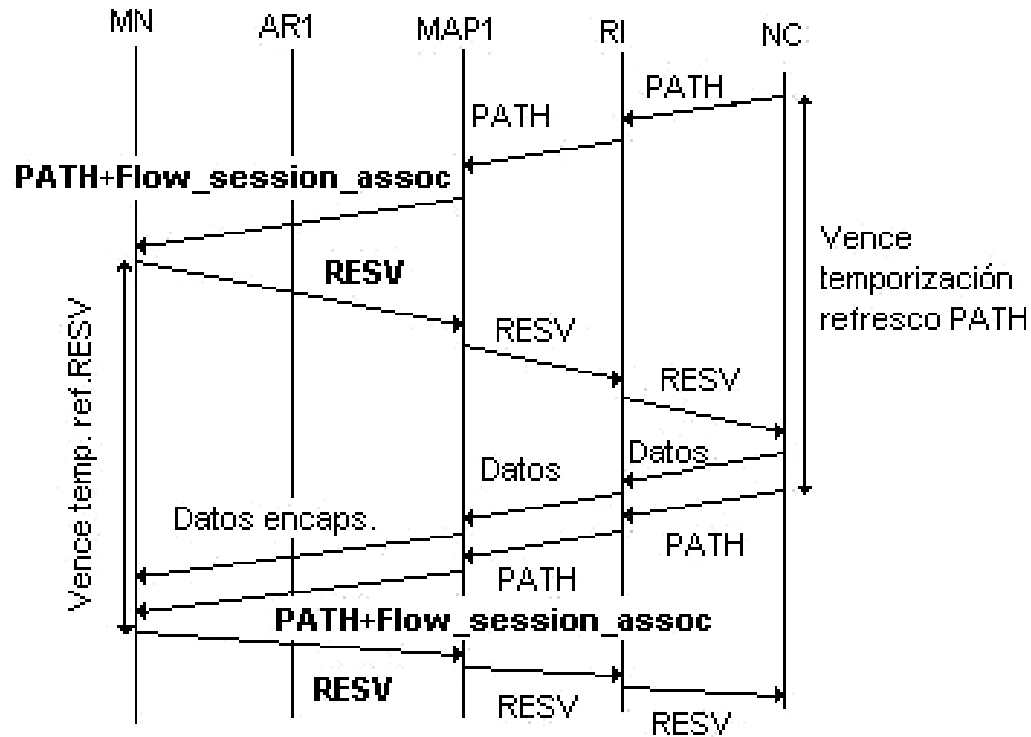
▶ Túneles en Mobile IP



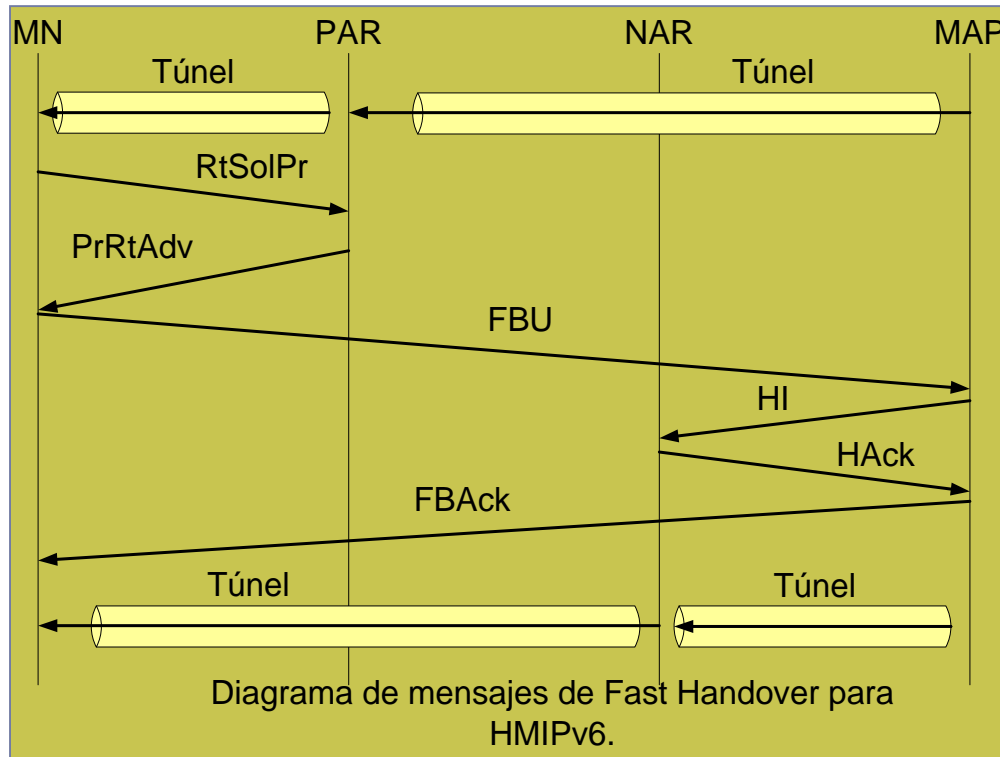
Hierarchical Mobile IP



Establecimiento del camino

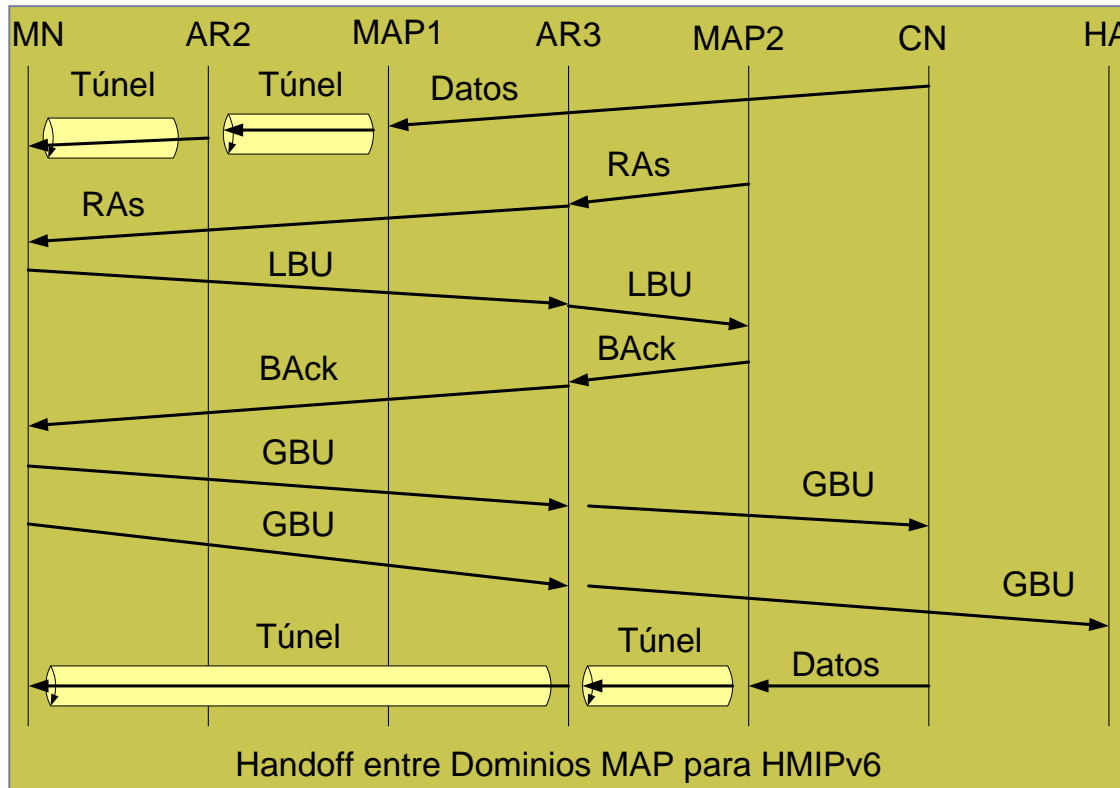


Handoff entre ARs



- RtSolPr:** Router solicitation for Proxy Advertisement
- PrRtAdv:** Proxy Router Advertisement
- FBU:** Fast Binding Update
- HI:** Handover Initiate
- HAck:** Handover Acknowledge
- FBAck:** Fast Binding Acknowledgement

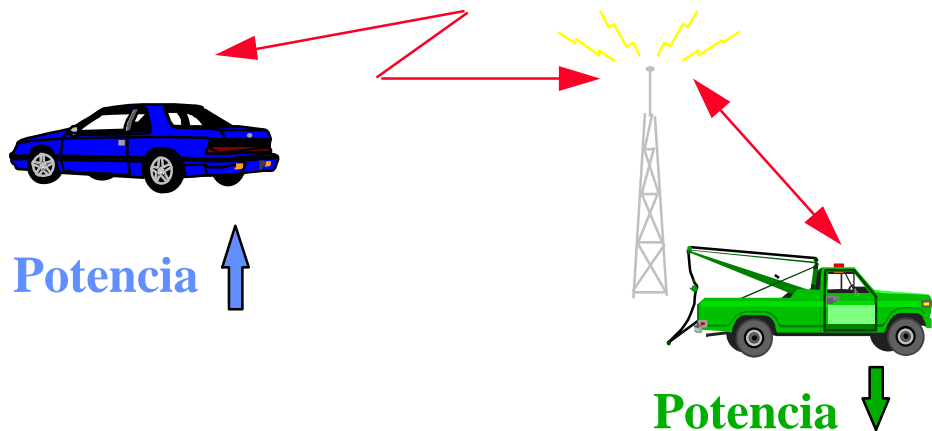
Handoff entre MAPs



RA: Router Advertisement
LBU: Local Binding Update
GBU: Global Binding Update

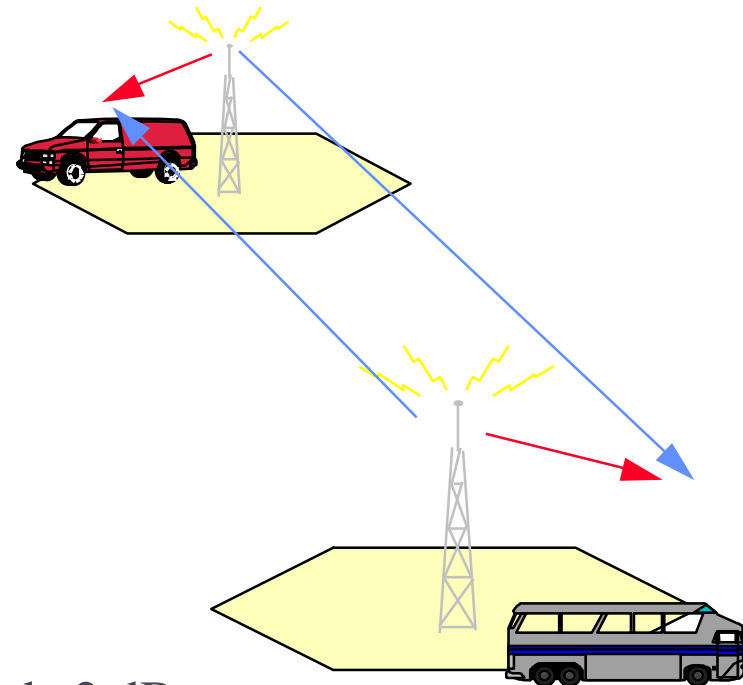
CONTROL DE POTENCIA

- **Ahorro de baterías : los móviles transmiten con la mínima potencia que garantiza S/N óptima.**



Las MS pueden variar su potencia en pasos de 2 dB
(Potencia mínima: 20mW y máxima según categoría MS)

- **Reducción interferencias**



Control de Potencia: Procedimiento

- ▶ Cuando accesa inicialmente a una BTS, la MS utiliza la Potencia menor entre la máxima permitida por su clase y la máxima admitida en la celda (difundida por el BCCH).
- ▶ Una vez realizado el acceso, la BTS calcula la potencia que debe usar la MS.
- ▶ La BTS envía el valor de Potencia de Tx a la MS por el SACCH descendente.
- ▶ La MS efectúa el cambio y lo confirma a la BTS por el SACCH ascendente.
- ▶ La BTS realiza los cálculos de potencia de las MS a partir de las medidas que estas le entregan.
- ▶ Este proceso tarda 60mseg

Alineación temporal adaptativa

- ▶ El acceso TDMA requiere una excelente sincronización temporal.
- ▶ Las MS obtienen su sincronización de las señales recibidas de las BTS (Problema solucionado en el D/L)
- ▶ En el U/L hay un problema:
 - ▶ Las MS envían sus ráfagas aisladas, una por trama.
 - ▶ El tiempo de propagación depende de la distancia MS-BTS
 - ▶ Pueden superponerse dos ráfagas de dos MS (Colisión)
- ▶ Solución: **ALINEACION TEMPORAL (TA- Time Alignment)**

Alineación temporal Adaptiva

- ▶ La BTS ordena a las MS lejanas que inicien la transmisión de sus ráfagas con cierto adelanto con respecto al instante teórico marcado por la temporización.
- ▶ Este parámetro lo transmite la BTS a cada MS y se conoce como TA (tamaño: 6 bits)
- ▶ El adelanto lo calcula la BTS cuando la MS accede por el canal RACH.
- ▶ Máximo retardo compensado: $233\mu\text{seg}$
- ▶ En GSM la distancia máxima que permite compensación está entre 35 y 37 km.
- ▶ La BTS mide periódicamente el TA y lo corrige cuando se produzcan cambios de 1 LSB como mínimo.
- ▶ Los datos de corrección los envía la BTS a través del canal SACCH