IMS
Arquitectura General

Prof. José Luis Pellegrino

CePETel

IMS- MODELO DE CAPAS

Capa de Acceso: ofrece interfaces de conexión para los terminales y es la puerta de acceso a la capa de Control.

Capa de Control: es el centro de la red, es la encargada de gestionar el flujo de mensajes y fijar la dinámica de los servicios.

Capa de Aplicación: Es la residencia de los servicios. Este plano es accedido desde el Core, y puede ofrecer API´s para usuarios externos

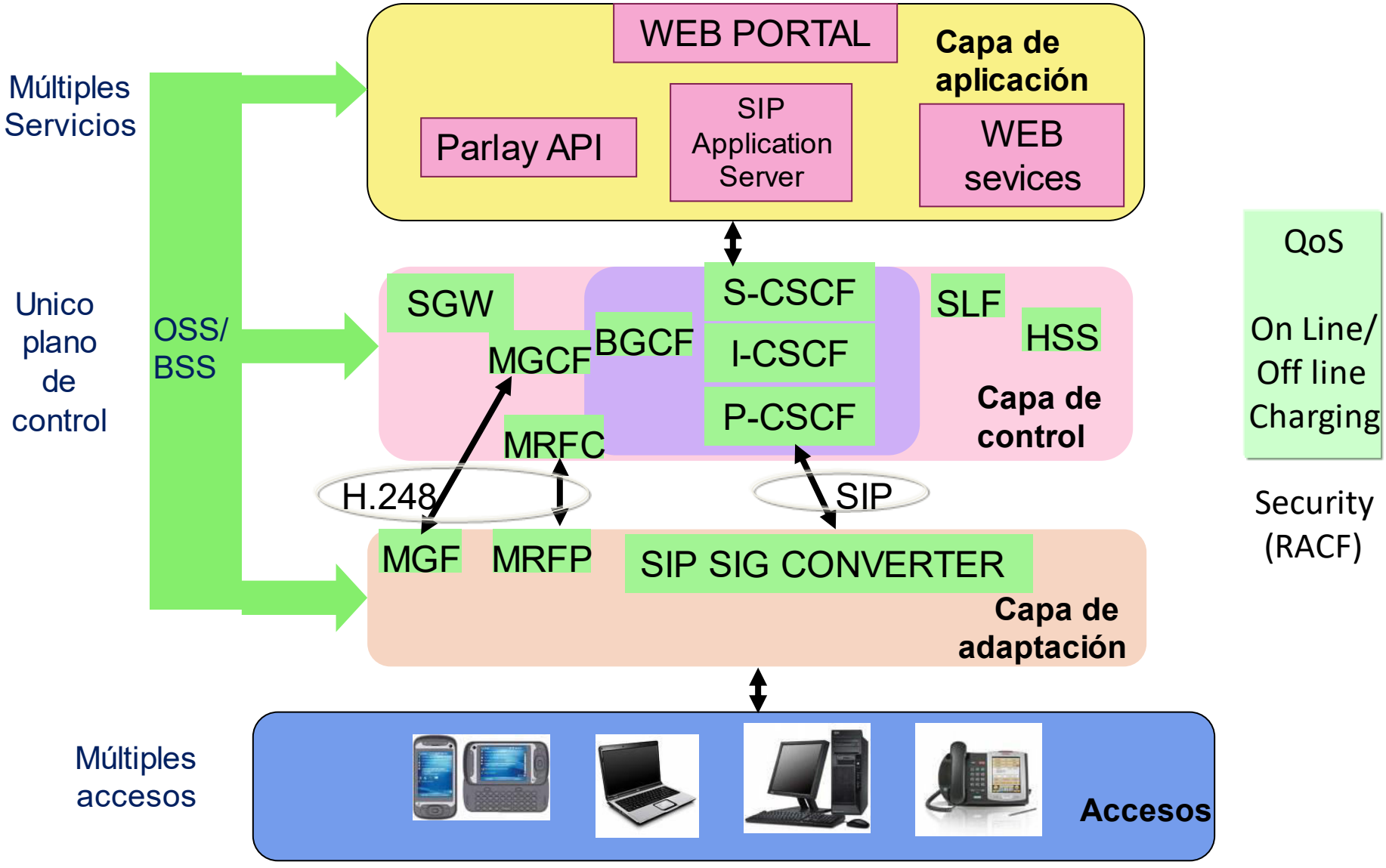
Core de Control ofrece interfaces de interconexión con:

- ✓ PSTN y PLMN
- ✓ Bases de datos (HSS)
- ✓ Sistemas de OSS/BSS. Integración: RETO

Desafío:
Introducir nuevas tecnologías además de IMS; LTE, Femtocells, RCS (cuestiones en algunos casos no transparentes al usuario)

Concepto clave: separación entre Acceso-Core-Aplicación

ANATOMIA DE LA ARQUITECTURA IMS



ENTIDADES, INTERFACES Y FUNCIONES IMS (I)

El Core IMS (núcleo), recibe las peticiones de los UE (User Eqipment) y los enruta a través del CSCF (Call Session Control Function) de acuerdo al perfil del usuario y al contenido de los mensajes, haciendo las consultas a las bases de datos (HSS) y accediendo a los Servidores de Aplicación (AS), donde residen los distintos Servicios.

Por otro lado, el Core IMS se vincula con las redes legadas a través de la funcionalidad conocida como MGCF (Media Gateway Controller Function) que se inserta en los MGC de la NGN.

ENTIDADES, INTERFACES Y FUNCIONES IMS (II)

Proxy-CSCF / P-CSCF

- Punto de entrada para un UE. Funciones de Proxy (RFC3261) ruteando los mensajes hacia el S-CSCF.
- Las sesiones destinadas a otro dominio, deben encaminarse a un I-BGF.
- Compresión de encabezados (radio)
- Puede incluir funciones de SBC (A-BGF y I-BGF)
- Puede implementar autorización de las capacidades portadoras y policía

Discutir en clase NAT y redes trusted/non trusted

ENTIDADES, INTERFACES Y FUNCIONES IMS (II)

Discutir en clase NAT y redes trusted/non trusted

Interrogating-CSCF / I-CSCF

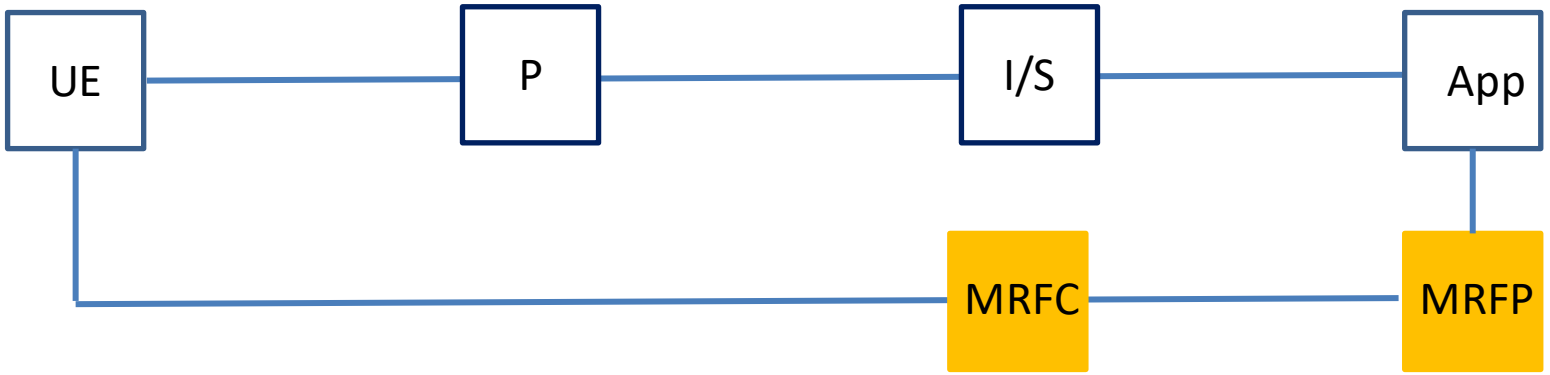
- Punto de contacto, para los usuarios de la red u otros que hacen roamming involucrados en un área de servicio (por ejemplo, se debe consultar al HSS si ese usuario tiene tal o cual perfil de origen para progresar tal llamada). Las sesiones destinadas a otro dominio, deben encaminarse a un I-BGF. Puede haber más de un I-CSCF en la red.
- Identifica y asigna un S-CSCF para el cliente (a través de consulta con el HSS)
- Funciones de Topology Hiding

ENTIDADES, INTERFACES Y FUNCIONES IMS (III)

Serving-CSCF / S-CSCF

- Lleva a cabo el servicio de control de sesión.
- Todo pasa por el S-CSCF. Sus funciones se pueden clasificar en: registración, mensajes relacionados y no relacionados con sesiones, usuarios terminales, usuarios originantes.
- Soporta establecimiento, modificación y liberación de sesiones
- Se vincula con el AS a través de la interfaz ISC
- Determina el AS correcto consultando el HSS

ENTIDADES, INTERFACES Y FUNCIONES IMS (III)



Discutir en clase la relación S-CSCF con TAS en escenarios complejos

Multimedia Resource Function (MRF)

• Es la evolución natural de un Media Server. Se compone de dos partes: controladora (MRFC) y procesadora (MRFP). La primera controla a la segunda a través de la interfaz "Mp" mediante el protocolo H.248 (basado en la Rec. ITU-T H.248-1 y extensiones H.248-x, al cual se suman extensiones definidas por 3GPP en TS 29.333).

ENTIDADES, INTERFACES Y FUNCIONES IMS (IV)

HSS (Home Subscriber Server):

- Base de datos centralizada. Almacena datos y perfiles de servicios
- Es una evolución del HLR de las redes móviles y los servidores AAA
- Es la base de datos maestra que contiene toda la información de usuario
- Registra qué nodo del CORE de red está manejando a cada usuario
- A través de los datos de usuarios brinda servicios al S-CSCF una vez validada la autenticación del usuario
- Almacena los datos temporales con la localización del S-CSCF en el que un usuario ha sido registrado

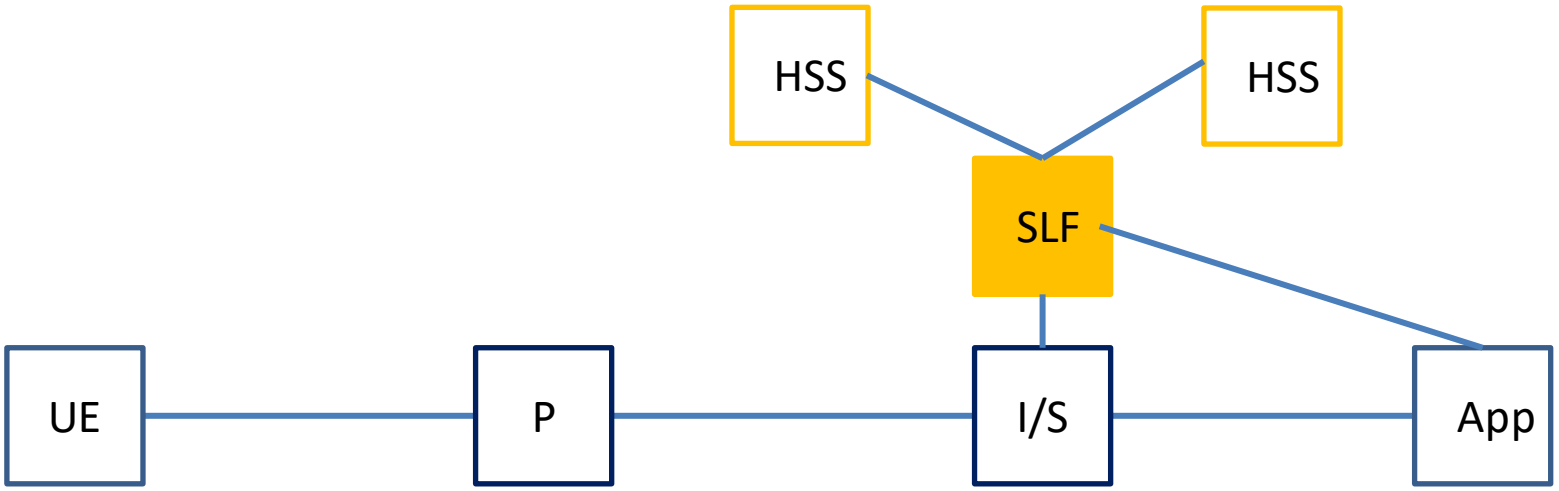
El HSS participa en la registración del cliente y en la gestión de llamadas.
Parte de la provisión de un cliente IMS se hace en el HSS

ENTIDADES, INTERFACES Y FUNCIONES IMS (V)

Subscriber Location Function (SLF):

• En caso de múltiples HSS, actúa recibiendo un pedido de I-CSCF y selecciona el HSS correcto.

Discutir en clase el uso de DRA como sustituto



ENTIDADES, INTERFACES Y FUNCIONES IMS (V)

Policy Decision Function (PDF):

• Gestiona reserva de recursos para brindar QoS. Este es un aspecto diferenciador con redes de VoIP.

ENTIDADES, INTERFACES Y FUNCIONES IMS (V)

Application Server (AS):

- Es la capa de aplicación, son los servidores donde reside la lógica de los servicios
- Se conectan al Core IMS a través de la interfaz ISC. Esta interfaz hoy día es la más desarrollada a nivel multivendor.
- Puede incluir su propia base de datos muy específica relacionada con el servicio en cuestión. Por ej, para VoLTE, el MTAS (AS) incluye una DB conocida como Transparent Data

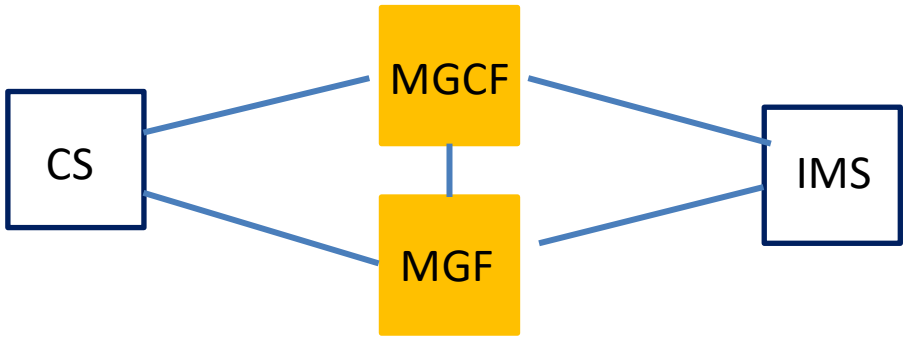
ENTIDADES, INTERFACES Y FUNCIONES IMS (VI)

Media Gatreway Control Function (MGCF):

- Elemento clave en la frontera con la NGN clásica
- Controla los MG (H.248)
- Convive con la función de Softswitch
- Estrecha relación con el SGW (signalling).

Media Gateway Function (MGF):

- Clásico MG.
- Interworking a nivel de media entre dominios IP y TDM (PSTN e PLMN)
- Gestión de audio: cancelación de eco, jitter buffer, supresión de silencio, diversidad de codecs
- Tiene un rol esencial en una NGN clásica (central).



ENTIDADES, INTERFACES Y FUNCIONES IMS (VI)

Media Gatreway Control Function (MGCF):

- Elemento clave en la frontera con la NGN clásica
- Controla los MG (H.248)
- Convive con la función de Softswitch
- Estrecha relación con el SGW (signalling).

Media Gateway Function (MGF):

- Clásico MG.
- Interworking a nivel de media entre dominios IP y TDM (PSTN e PLMN)
- Gestión de audio: cancelación de eco, jitter buffer, supresión de silencio, diversidad de codecs
- Tiene un rol esencial en una NGN clásica (central).

Service Capabilities Interaction Manager (SCIM):

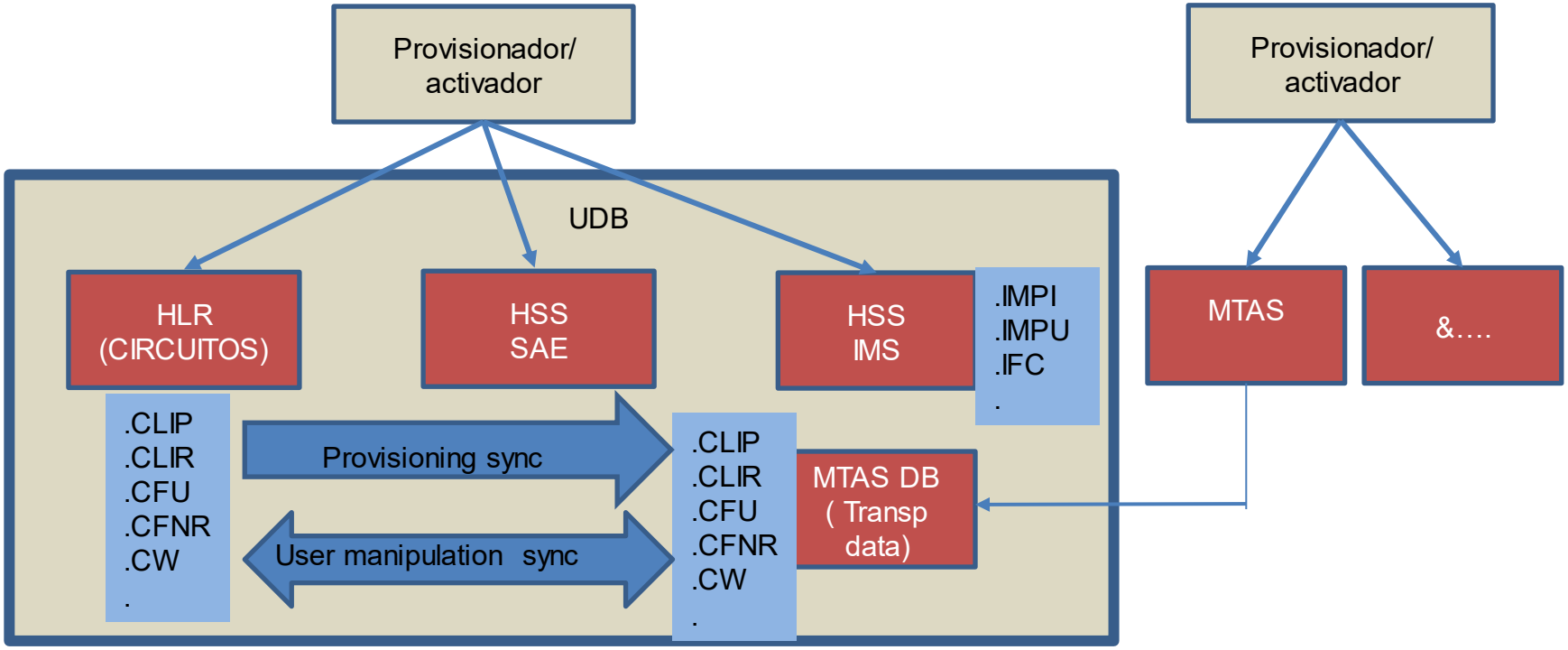
- Es un Service Broker. Es una entidad situada entre S-CSCF y AS que gestiona la interacción entre las capacidades y/o servicios de aplicación

IP Multimedia Service Switching Function (IM-SSF):

- Interconecta con un SCP clásico de la IN. Es parte de la NG IN. Es la entidad que la NG IN le ofrece a IMS para acceder a otras plataformas

ENTIDADES, INTERFACES Y FUNCIONES IMS (VI)

La definición de HSS suele plantear confusiones.
Base de datos centralizada.
La siguiente figura esquematiza algunas clarificaciones



ENTIDADES, INTERFACES Y FUNCIONES IMS (VII)

- ✓ **CSCF** (Call Session Control Function) → Proxy, Interrogating, Serving.
- ✓ **MGCF** (Media Gateway Control Function)
- ✓ **MGW** (Media Gateway Function)
- ✓ **MRF** (Media Resource Function)
- ✓ **HSS** (Home Subscriber Server)
- ✓ **ASF** (Application Server Function)
- ✓ **SGW** (Signalling GateWay Function)

Otros:

- ✓ **SLF** (Subscription Locator Function)
- ✓ **BGCF** (Breakout Gateway Control Function)
- ✓ **ALG** (Application Level Gateway)
- ✓ **ATCF:** Access Transfer Control Function (release 10)
- ✓ **ATGw:** Access Transfer Gateway (release 10)

INTERCONEXIÓN ENTRE IMS y REDES CS - BGCF

• El BGCF es una entidad que interconecta dominios IMS y CS (ejemplos: una red NGN Nokia, Huawei o Ericsson)

• Determina la red en la cual ocurre el cambio de dominios (IMS a CS).

• Define el próximo salto para enrutar los mensajes SIP basándose en información recibida en los mismos u obtenida de su base de datos.

• Para llamadas terminadas en PSTN, determina la red en la cual debe ocurrir el cambio a PSTN /CS.

• Si determina que el breakout debe ocurrir en la misma red donde se encuentra el BGCF, entonces selecciona un MGCF para la interconexión con la PSTN/CS.

• Si el breakout se debe hacer en otra red, el BGCF retransmite la señalización a otro BGCF ubicado en esa red.

• Si la llamada está destinada a otra red IMS, reenvía el mensaje SIP al BGCF de esa red mediante interface Mk.

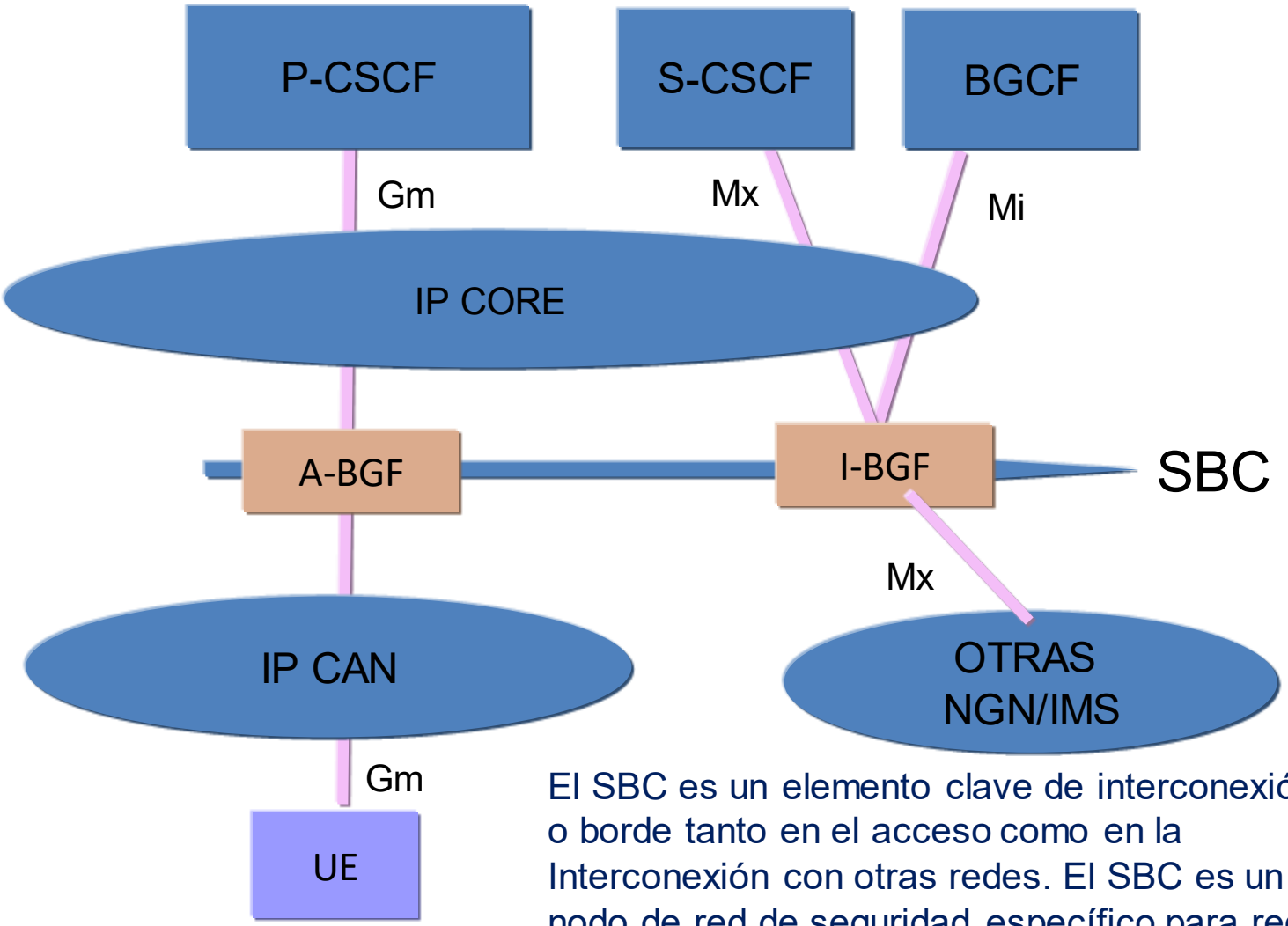
• Si determina que la red destino es otra red IP, entonces se reenvía la señalización al punto de interconexión con esa red.

INTERCONEXIÓN ENTRE IMS y REDES CS - BGCF

Rol del BGCF en la interconexión
Con otras redes no IMS

P-CSCF

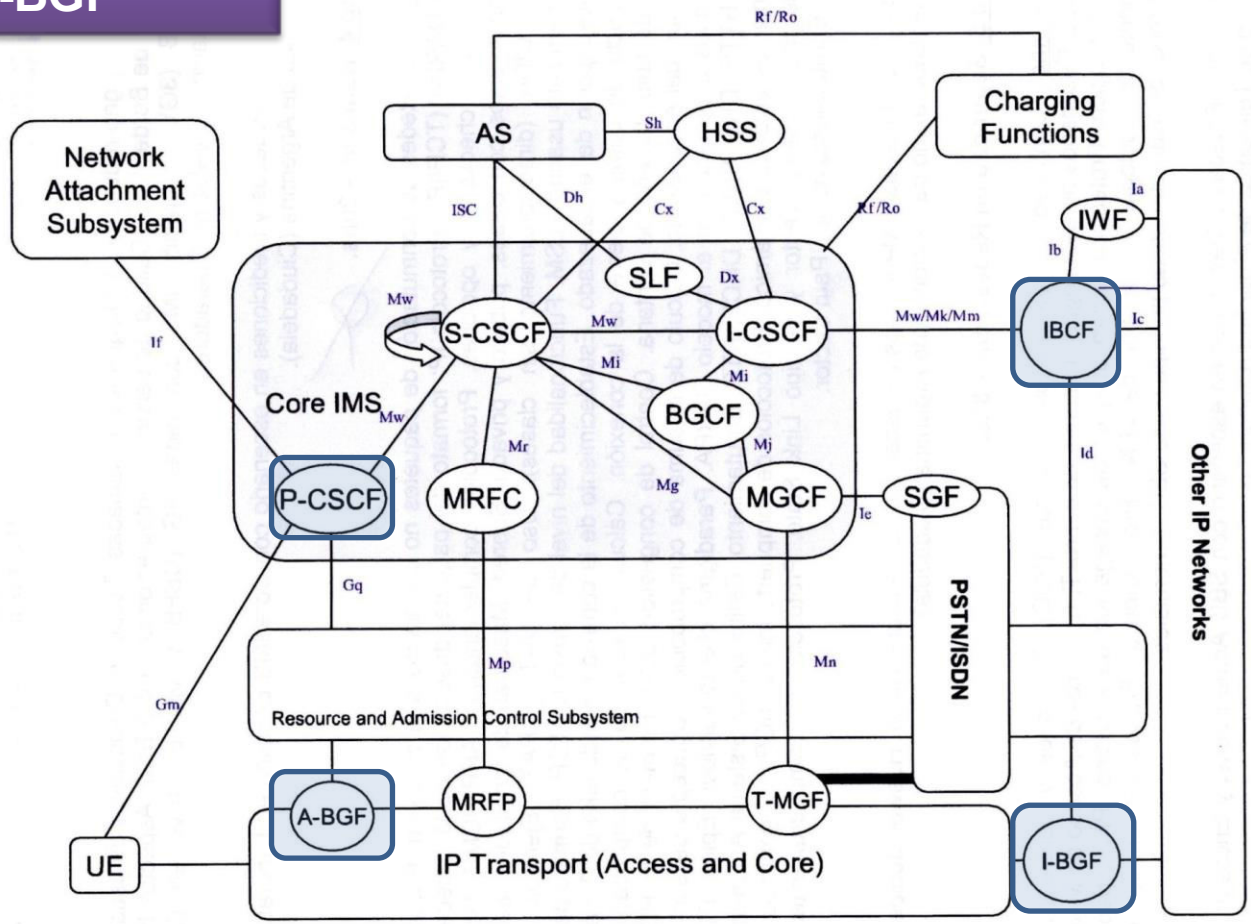
IMS EN EL ACCESO, FUNCIONES DE BORDE



El SBC es un elemento clave de interconexión o borde tanto en el acceso como en la Interconexión con otras redes. El SBC es un nodo de red de seguridad específico para redes de tiempo real.

IMS EN EL ACCESO Y LA INTERCONEXIÓN, FUNCIONES DE BORDE

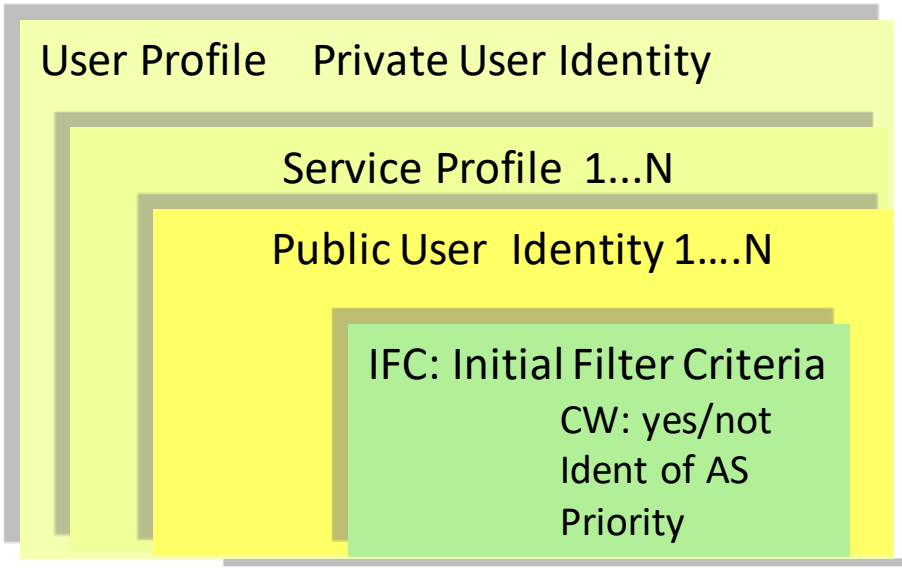
Observar IBCF / I-BGF
P-CSCF / A-BGF



I BCF Interconnection Border Control Function
I BGF Interconnection Border Gateway Function
A BGF Access Border Gateway Function

HSS, MUCHO MAS QUE UNA BASE DE DATOS

- Elemento clave, vincula el mundo IT con red
- Proveedores de CORE. Algunos no integran HSS de terceros (HP, IBM, …)
- Como algunos AS ya disponen de una DB interna, relegan el HSS a un rol secundario:
  - autenticación básica de cliente
  - información de perfil
- Se evalua muy bien las aplicaciones del HSS a fin de determinar si un ambiente multivendor es viable

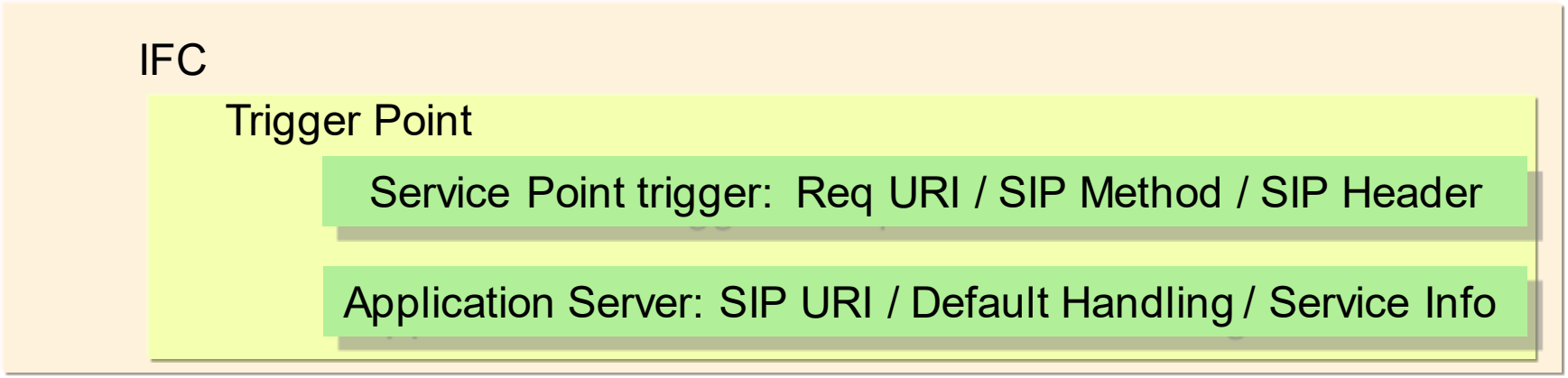


Al registrarse, el S-CSCF levanta los FC desde el HSS

¿Por qué es el S-CSCF?

HSS, FILTER CRITERIA

- A través de los FC, el S-CSCF identifica el AS
- IFC: es evaluado al recibir un pedido inicial de diálogo SIP (estadios iniciales, INVITE, SUSCRIBE)
- No todos los mensajes desencadenan una evaluación de FC, sino aquellos de cuyo enrutamiento se deba alcanzar un AS.
- Los FC forman parte del perfil de usuario
- Cada usuario podrá tener varios FC en el HSS
- Al registrarse, el S-CSCF recibe el perfil de usuario desde el HSS con todos los FC aplicables



HSS, FILTER CRITERIA

Ejemplos

iFC vs SiFC

En el caso *sharediFC*, se creará solamente en el S-CSCF, de modo que en la registración el S-CSCF solo recibe desde el HSS el ID del template en cuestión:

Se debe respetar la coherencia entre los ID de HSS y de CSCF.

HSS: *TPLID:xx*

S-CSCF:*ScscfSharedIfcId:xx*

Sea el ejemplo de creación de un TPLID nuevo para un determinado servicio, como SMSoIP (15 en este caso).

```
ADD                          HHSSSUB:                          SUBID="+54XXXXXXXXXX",
IMPI="72207XXXXXXXXXX@ims.mnc007.mcc722.3gppnetwork.org",      IMPIAUTHTYPE=EAA,
IMSI="72207XXXXXXXXXX",                                        ISDN="54XXXXXXXXXX",
IMPULIST="\"sip:+54XXXXXXXXXX@ims.mnc007.mcc722.3gppnetwork.org\"&\"tel:+54XXXX
XXXXXX\"&\"sip:72207XXXXXXXXXX@ims.mnc007.mcc722.3gppnetwork.org\"",
CHARGTPLID=X, SPTPLID=15, IMPUTPLID=X, IRSID=1, SYSNO=1, CONSFLG=FALSE;
```

HSS, FILTER CRITERIA

Ejemplos

MTAS. ID del iFC

Se tomará como base el *ScscfSharedIfcId=14* y se creará el *ScscfSharedIfcId=15.*

En el *ScscfSharedIfcId=15,* se agregará a los "ScscfIfcNames" existentes, como p ej *ScscfIfcName=342_register*, *ScscfIfcName=346_sccasorigred*, etc, uno nuevo, p ej: *ScscfIfcName=999_ipsmgwreg*.

El index 999 hace referencia a la prioridad del iFC.

Si se utilizaran dos iFC uno para MO y otro para MT, resultaría:

ScscfIfcName=998_ipsmgwmoreg.

ScscfIfcName=999_ipsmgwmtreg.

Triger

Se asignará como Service Point triger, la recepción de un SIP method del tipo "message".

ScscfSptName: Spt0_Method

URL

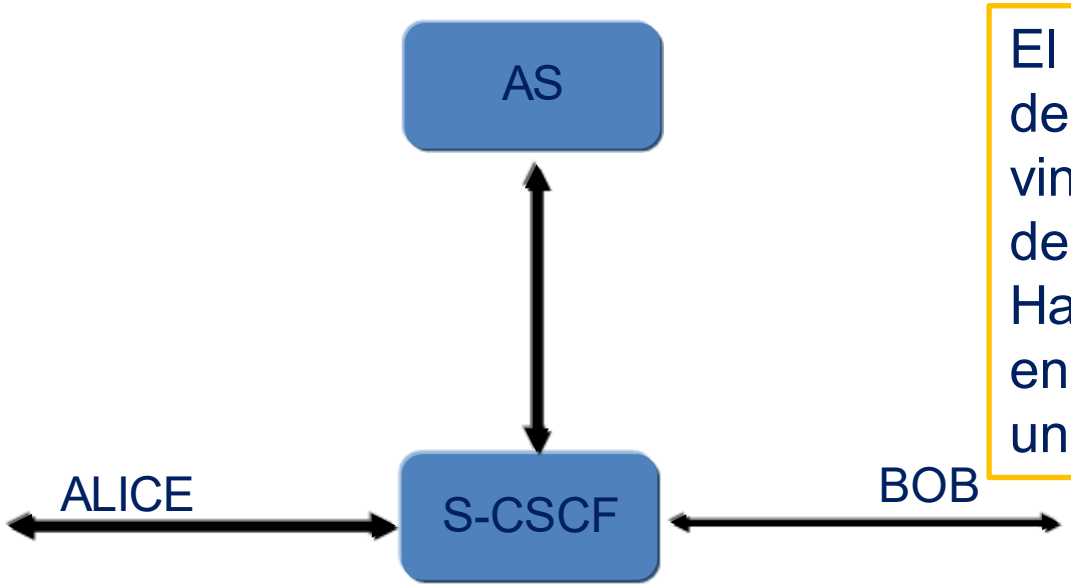
Se deberá asignar la identidad del Servidor IP-SM-Gw.

ScscfIfcAsName: ipsmgwmoreg.ims.mnc007.mcc722.3gppnetwork.org; lr

IMS DNS

Se configurará la resolución de la URI correspondiente a la URI del servidor

AS Y S-CSCF: COMO ES EL VÍNCULO?



El S-CSCF es la entidad del Core IMS que se vincula con los Servidores de Aplicación.
Hay escenarios de llamadas en los que participan mas de un A.S.

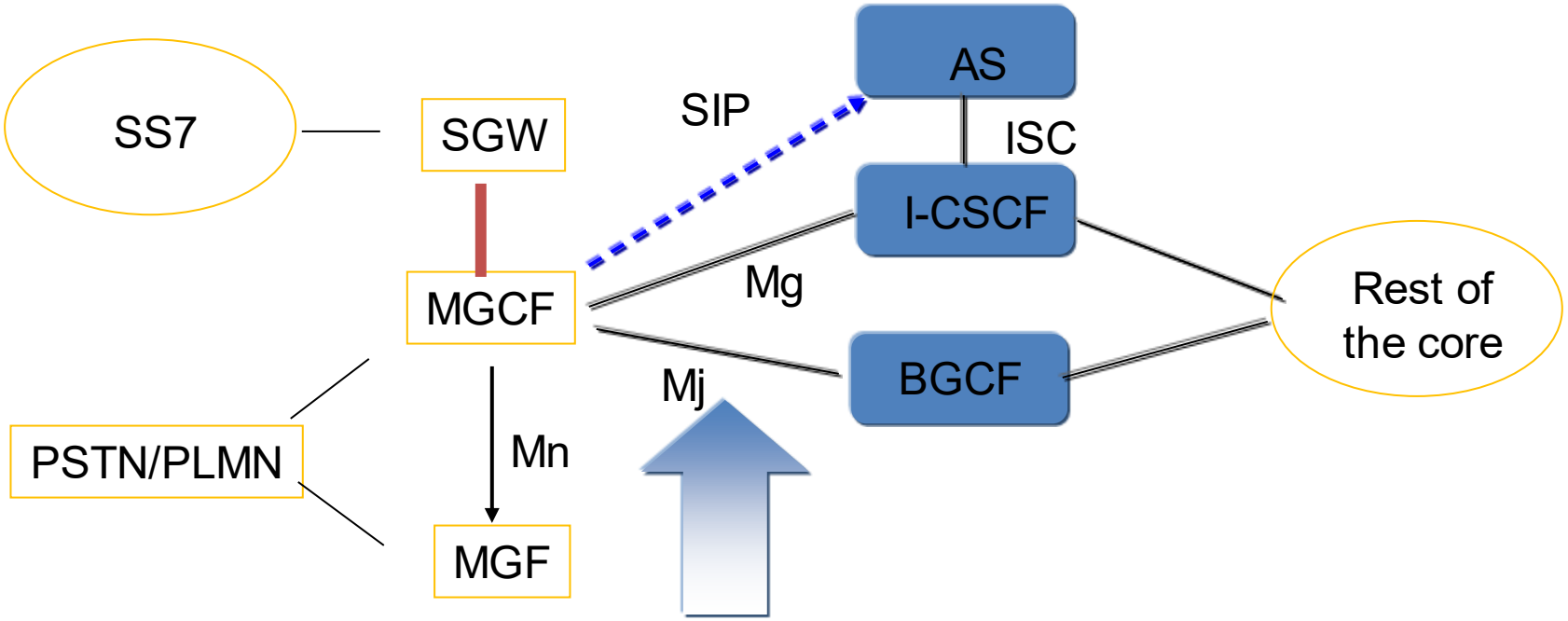
1- AS, es la Plataforma de Servicio propiamente dicha (Ej MMTel)

2 - S-CSCF actúa como originador y terminador

3- AS actúa como Proxy, Redirect o B2BUA Server

4- Hay casos especiales de Servicios sin AS (el S-CSCF resuelve).
P ej: servicios básicos, acceso de clientes no IMS a otros servicios NG IN como RPV, resueltos a través de un mecanismo llamado "Willcard PSI"

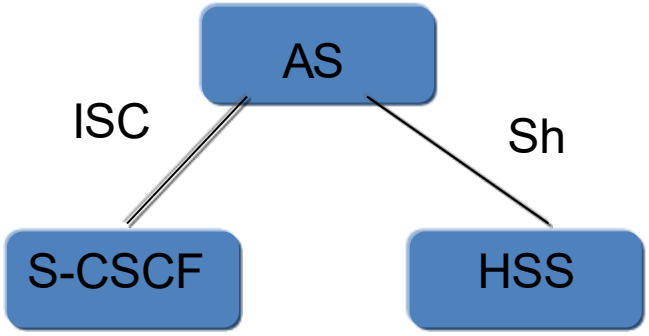
INTERWORKING CON REDES PSTN Y PLMN



- Softswitches clásicos incorporan funcionalidad de **MGCF** (ejemplo: MTs Ericsson en break out para mobileVoLTE, o MGC Huawei para break out de fixed VoLTE
- SIP Application Servers conectados vía ISC (MTAS), pero también casos de AS en modo stand alone conectados a NGN vía SIP (Broadsoft o Prepaid Huawei)

INTERWORKING CON A.S.

La integración de un A.S a un dominio IMS, implica el ajuste de las interfaces ISC (SIP) y la Sh (Diameter).
Ejemplos: MTAS de E/// con HSS de Huawei
SM IP Gw de Xura con S-CSCF de E///



Interfaz Sh hoy dia tan desarrollada como la ISC (no fue así en los inicios).
Endpoints SIP (UE) desplegados sin soporte de interfaz Gm (problemas y ajustes requeridos).
Interfaces Mg y Mj requieren soporte de servicios regulados (911, multicarrier, etc)

SBC: SESSION BORDER CONTROLLER

• Los SBC dieron respuesta a una problemática de SIP en los bordes de las redes: Al haber NAT se planteaba una inconsistencia entre el header ConnectionInformation y la verdadera dirección IP donde reside el UE.

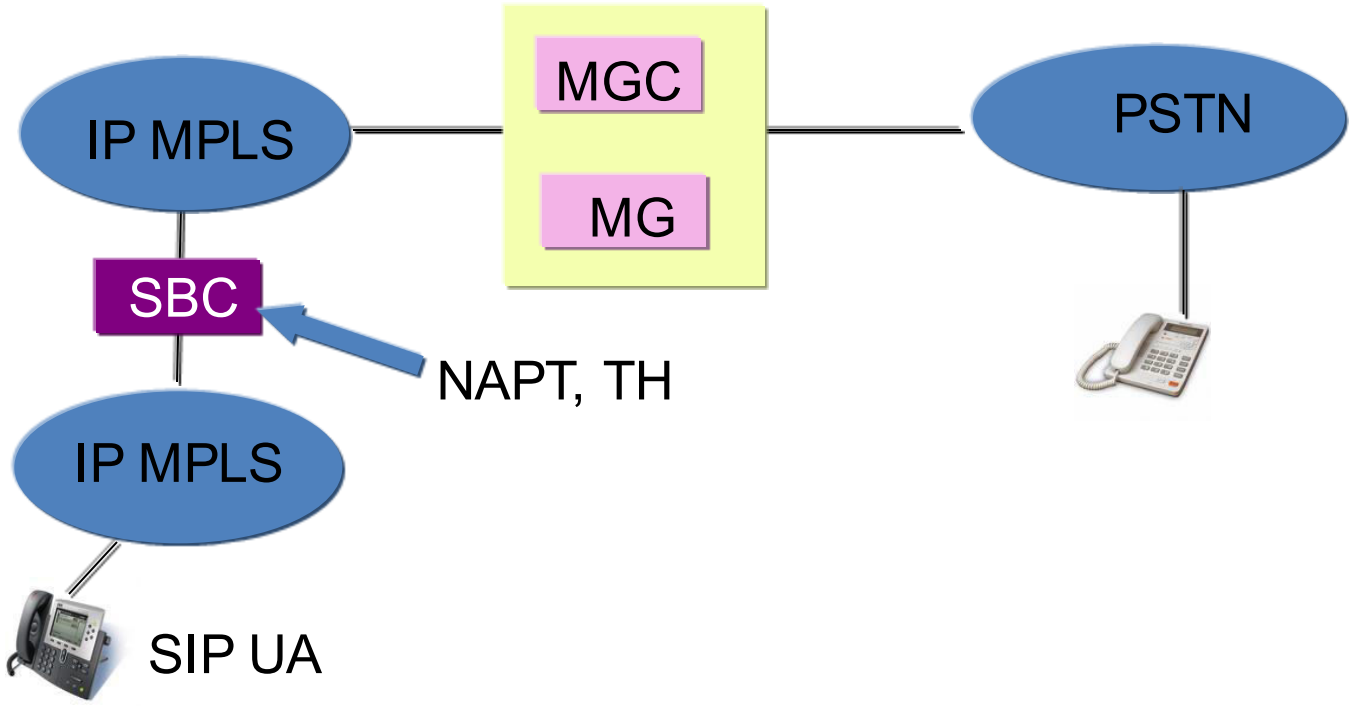
• Un SBC es una especie de Firewall específicamente diseñado para soportar VOIP (de hecho trabaja en la capa de aplicación)

• Los 1ros. SBC eran monolíticos, no cumplían con arquitecturas de 3GPP

• Un SBC es un equipo que provee control de acceso y adaptación en el borde de red, tanto hacia un UE como hacia otras redes, utilizando SIP como protocolo de señalización

• Los SBC se intercalan en el borde de red tanto a nivel Media como Señalización:
  - ✓A nivel Señalización es un B2BUA
  - ✓A nivel Media es un RTP Proxy, Topology Hidding (TH), Media Transcoding, Eco Cancelation, etc

SBC: ESCENARIOS UNI



SBC: ESCENARIOS NNI

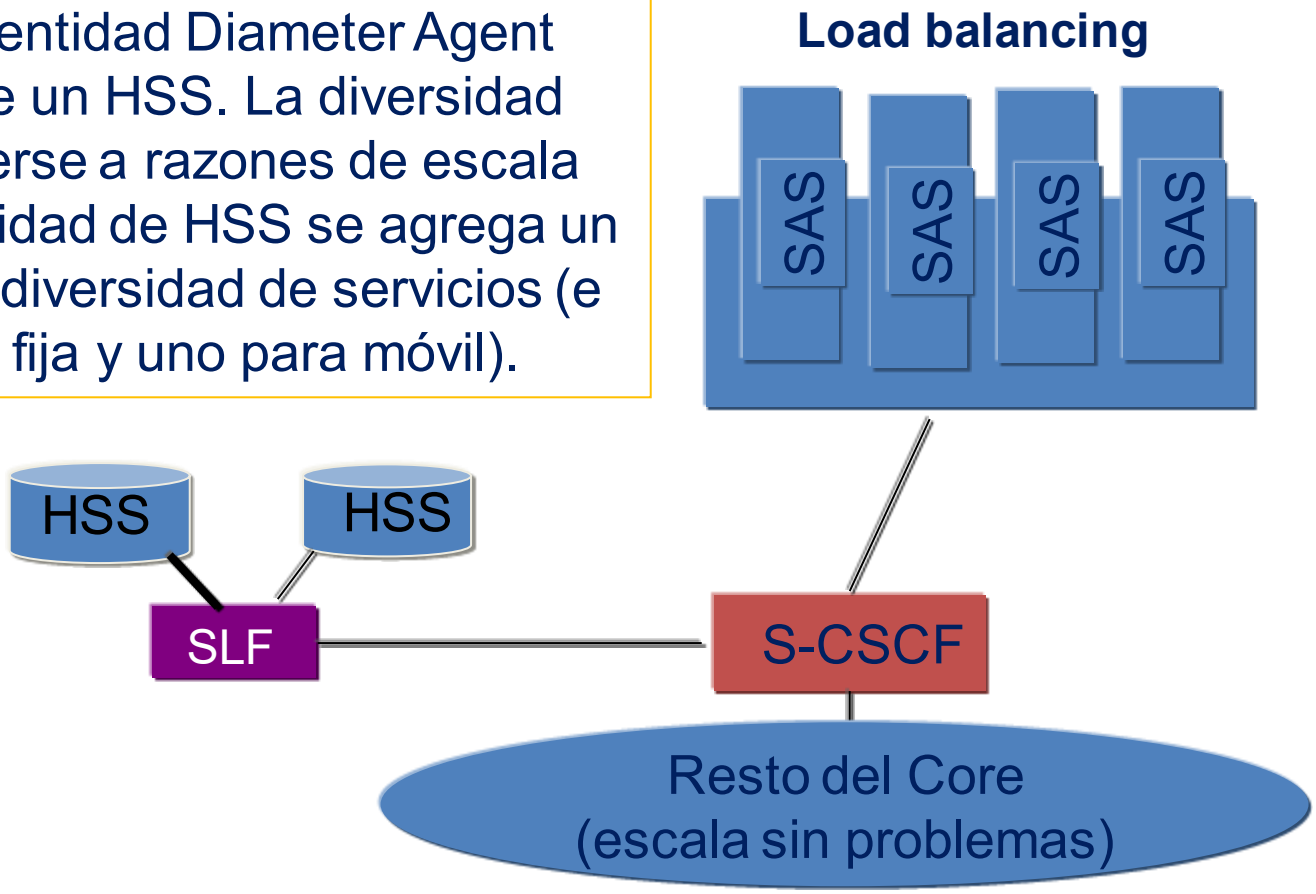
- TH (Topology Hidding)
- ALG (Application Layer Gateway): soporta B2BUA entre redes
- Control de admisión de llamada
- Traffic Policy
- Billing
- Interworking IP V4 / IP V6
- Interworking SIP / H.323

Discutir en clase caso de redes de acceso y múltiples Tipos de IP en el acceso

ASPECTOS CLAVES DE ESCALABILIDAD & ENRUTAMIENTO

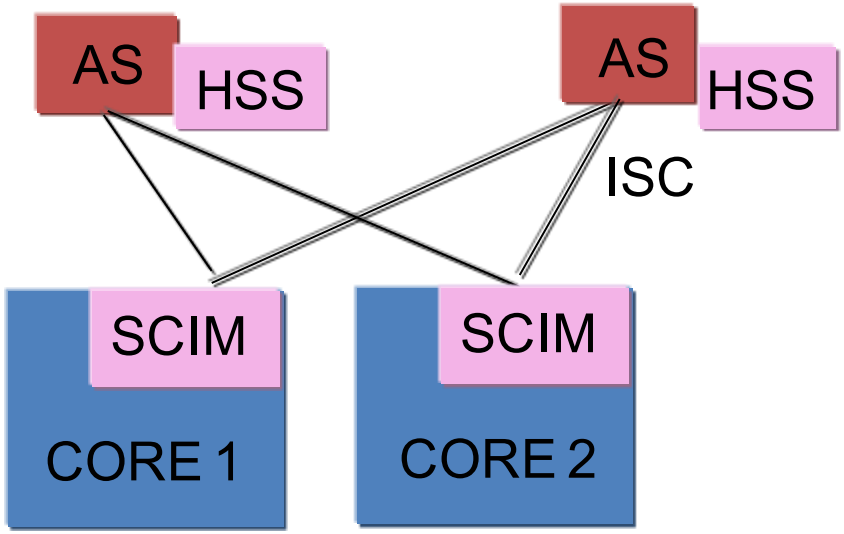
- Escala horizontal de los App Servers (SAS)
- Punto crítico del Core: HSS (500K-1Mill)

El SLF actua como entidad Diameter Agent apuntando a mas de un HSS. La diversidad de HSS puede deberse a razones de escala (si se supera capacidad de HSS se agrega un SLF) o también por diversidad de servicios (e ej: un HSS para red fija y uno para móvil).

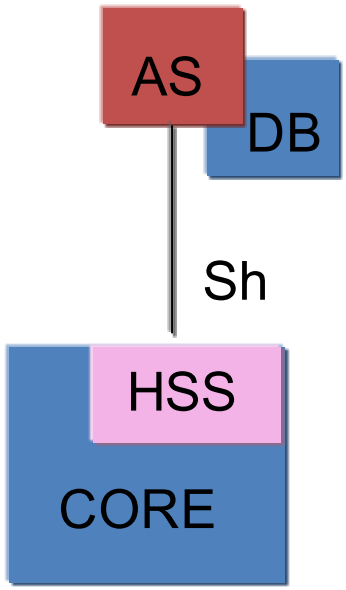


REDUNDANCIA DE BASE DE DATOS REPLICADAS

- **Geo-redundancia**



- **Réplica a través de Sh**

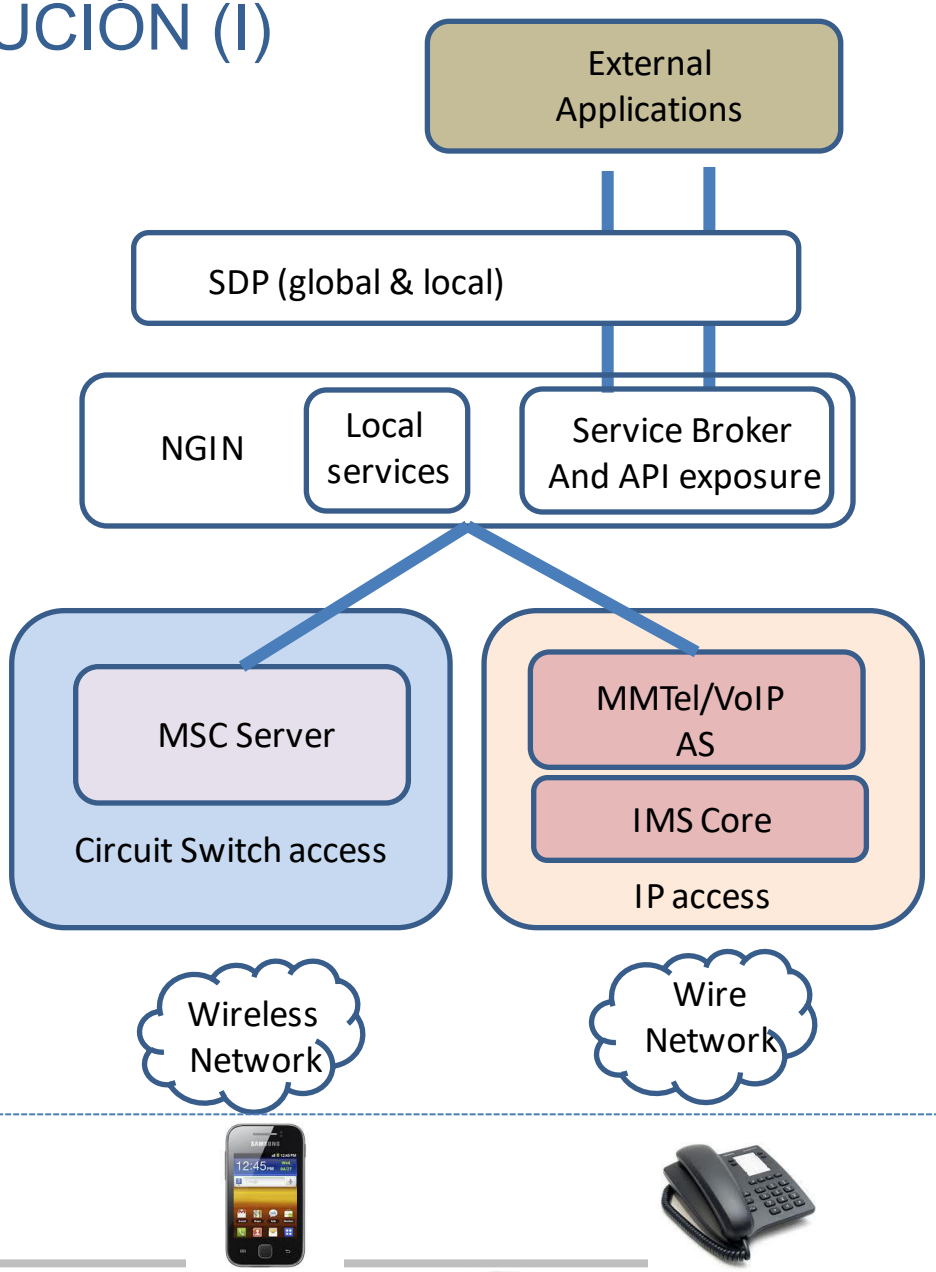


Geo-redundancia requiere sincronismo y réplica en HSS

SCIM (Services Capabilities Interaction Manager) una de las últimas entidades en lograr un nivel de standarización requerido y por lo tanto una de las menos desplegadas

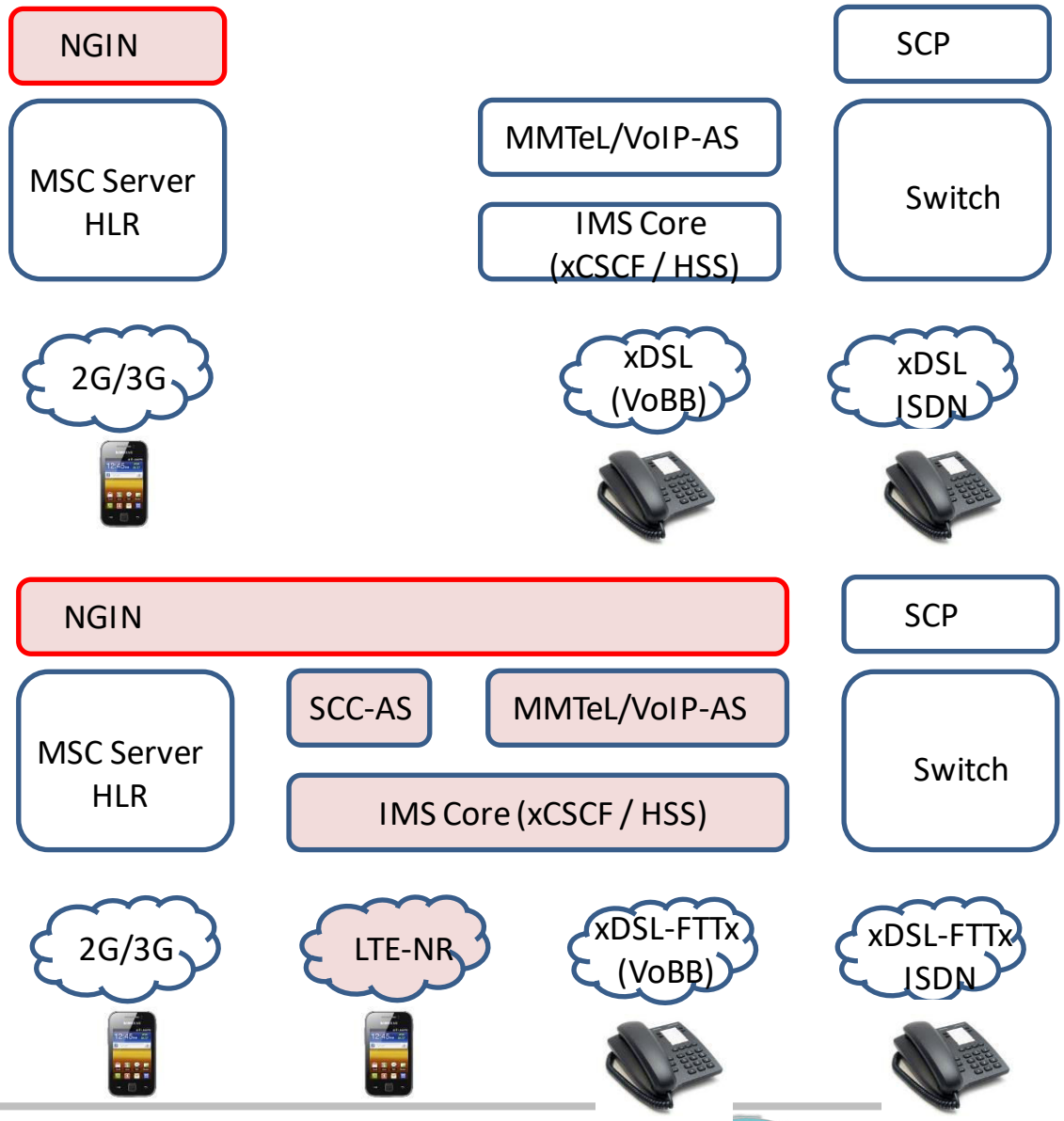
IMS EN CONTEXTO Y LA EVOLUCIÓN (I)

Al inicio, red fija y móvil
con escaso nivel de integración



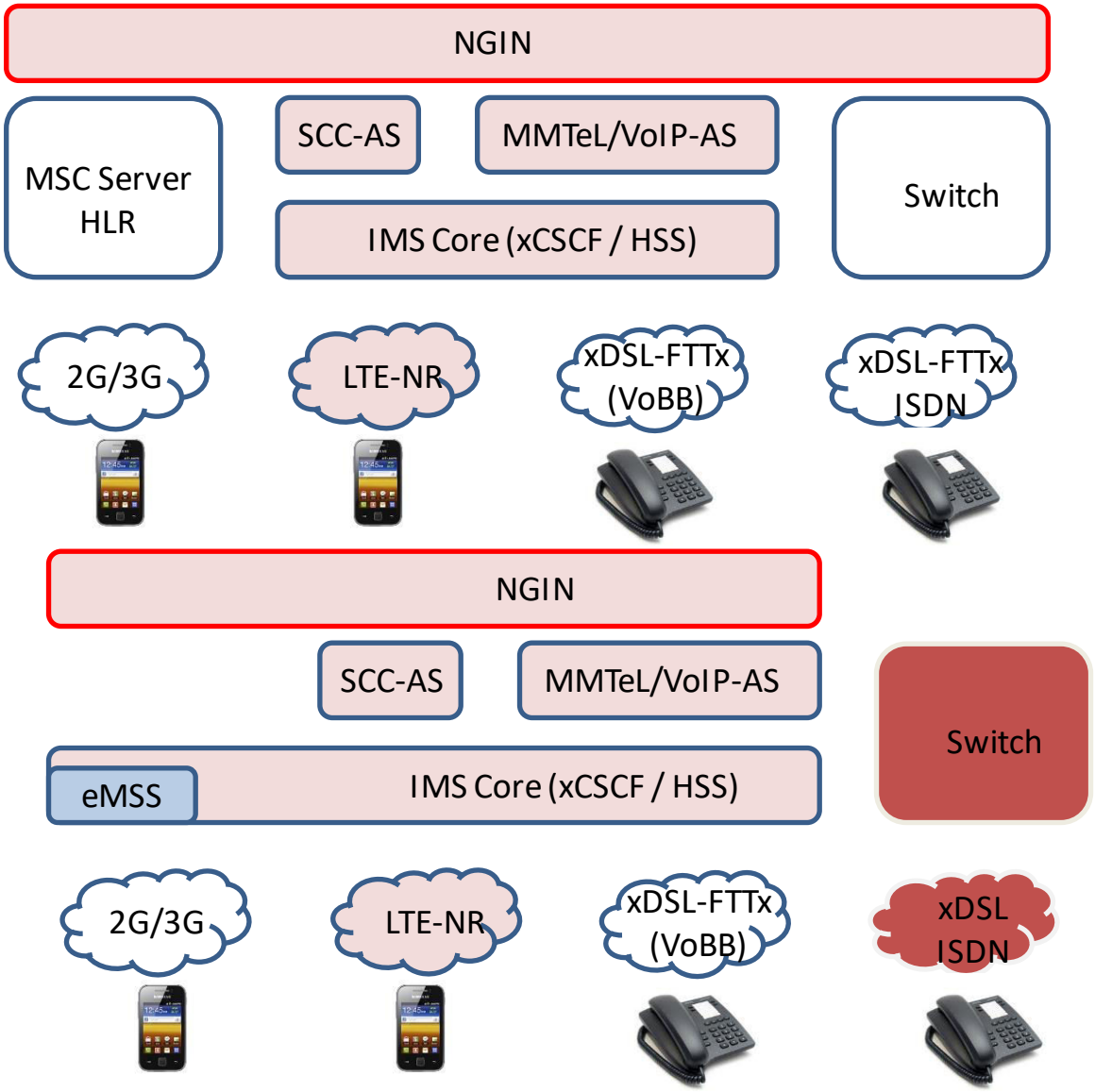
IMS EN CONTEXTO Y LA EVOLUCIÓN (II)

NG IN crece en diversidad de servicios



IMS EN CONTEXTO Y LA EVOLUCIÓN (III)

Al final, la red TDM
Es residual y la NG IN
cubre todos los accesos



Breve discusión en clase:
NG IN Vs IN
DIAM Vs CAMEL

ALGUNOS ACRÓNIMOS

IMS: Internet Multimedia Subsystem
3GPP: 3rd Generation Partnership Project
ABCF: Access Border Control Function.
AGWF: Access Gateway Function
BSS: Business Support System
CSBF: Circuit Switch Fallback
CSCF: Call Session Control Function
EPC/SAE: Evolved Packet Core/System Architecture evolution.
GPRS: General Packet Radio System
HSS: Home Subscriber Subsystem
HLR: Home Location Register
IBCF: Interconection Border Control Fucntion.
IBGF: Interconection Border Gateway Function
ICS: IMS Centralized Services
IDM: Internet download manager
IETF: Internet Engineering Task Force
IM-SSF: IP Multimedia Service Switching Function
IP: Internet Protocol
ISC: IMS Service Control
FWT: Fixed wireless terminal/telephony
LTE: Long Term Evolution

MAP: Mobile Application Part protocol.
MME: Mobility Management Entity
MMTel: Multimedia Telephony
MSC-S: Mobile Switch Center- Server
NAPT: Network Address and Port Traslation
NGN: Next Generation Network.
NGIN: Next Generation Intelligent Network
NMS: Network Manager System
OneVOICE: inciativa de 3 GPP para servicios de VOIP sobre IMS
PDF:Policy Decision Function
RAN: Radio Access Network
RCS: Rich Communication Suite
PES: PSTN/ISDN Emulation Subsystem
PLMN: Public Land Mobile Network
PSS: PSTN/ISDN Simulation Subsystem
SDP: Service Delivery Platform
SDP: Session Description protocol
SCIM: Service Capabilities Interaction Manager
SLF: Subcriber Location Function
SR-VCC: Single Radio Voice Call Continuity
VOCS: Voice over Circuit switch.
VOLTE: Voice Over LTE
VOPS: Voice over Paquet switch.

MECANISMOS DE AUTENTICACIÓN Y CONTROL DE ACCESO

• Hay un único mecanismo especificado en la 3GPP TS 33.203 (Access Security for IP-Based Services) llamado comúnmente **AKA** (Authentication and Key Agreement)
De HECHO EN VoLTE SE USA AKA.

• Pero hay otros mecanismos para cubrir las necesidades de terminales heredados (por ejemplo en VoIP) y permitir un despliegue más rápido como ser:

✓**Early IMS del 3GPP para el acceso móvil.** Como los Early IMS no son totalmente compatibles con los estándares de IMS no son aplicables los mecanismos de seguridad. Ejplo.: implementaciones basadas en IPv4 como los dispositivos 2G.

✓**Digest Authentication de TISPAN y PacketCable (caso de VoIP).**

✓**NASS-IMS.** Autenticación inseparable de TISPAN para redes fijas. Este método que reutiliza la autenticación de la capa de red fija en IMS está orientado a los casos donde el terminal no dispone de una tarjeta **ISIM** (IP Multimedia Services Identity Module). La seguridad es prácticamente la misma que la de la red de acceso.

✓**Digest Authentication con TLS (Transport Layer Security) de PacketCable.**

• Ante la variedad de mecanismos de autenticación utilizados en IMS se definió el estándar 3GPP TR 33.803 para guiar en la selección del método más adecuado.

AKA (AUTHENTICATION AND KEY AGREEMENT)

• La seguridad en IMS se basa en una clave secreta de larga duración compartida entre el **ISIM** y el centro de autenticación de la red local **AUC** (Authentication Center) o el **HSS** .

• **ISIM:** es una aplicación que se ejecuta en una tarjeta inteligente (UICC - Universal Integrated Circuit Card) y que contiene los parámetros de identificación y autenticación del usuario al IMS.

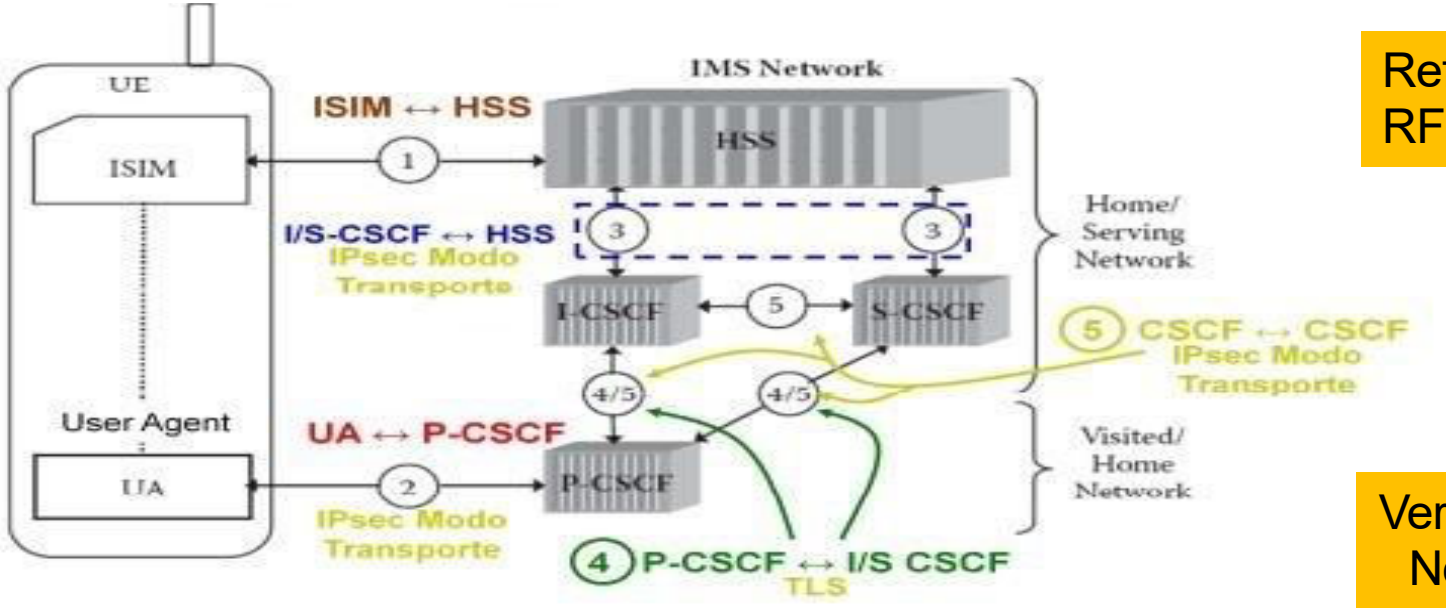
• **AUC:** Asociado en este caso al **HSS.** Contiene la información necesaria para realizar los procesos de autenticación y cifrado de los servicios. Almacena los algoritmos y genera las claves necesarias para cada servicio.

• El AKA se emplea para establecer tanto las claves de cifrado (3DES o AES-CBC) como las claves de integridad (HMAC-MD5 o HMAC-SHA-1).

Buscar en clase en un ejemplo de trazado de SIP Register, los : aes-cbc y aka v1 MD5

Nota: en los despliegues iniciales de IMS y VoLTE se suele usar USIM en lugar de ISIM. En esos casos, la tarjeta no almacena la identidades IMS como **IMPU& IMPI** ya que solo almacena la identidades de Packet Core como IMSI. Analizar “associated URIs”

ARQUITECTURA DE SEGURIDAD CON ISIM



Ref,: TS.33.203
RFC 3310

Ver en clase lado
Non trusted (2)

IMS tiene 5 Asociaciones de Seguridad definidas en 3GPP TS 33.203, Cuando el P-CSCF está en el Home Network aplica la asociación de seguridad #5, sino aplica la #4.

1.- ISIM ↔ HSS: Necesario para la autenticación mutua. Estas entidades tienen almacenada una clave secreta así como la identificación privada (IMPI) asociada a ésta.

2.- UA ↔ P-CSCF: Garantiza un enlace seguro entre el UE y la red (Gm /TS 23.002).

3.- I/S-CSCF ↔ HSS: Establece una asociación de seguridad para la transferencia de información entre esas entidades (Cx /TS 23.002)..

4.- P-CSCF ↔ I/S-CSCF: Esta asociación de seguridad se aplica solo cuando el P-CSCF no se encuentra en el Home Network.

5.- I-CSCF ↔ S-CSCF: Suministra la seguridad entre nodos SIP dentro de una misma red (Home Network).

SEGURIDAD DE ACCESO IMS PARA SIP

• Según estándares de 3GPP, la autenticación del usuario debe basarse en **Digest AKA**, algo análogo a la autenticación de acceso UMTS pero para SIP. Este es el modo que se usa habitualmente en VoLTE.

• La especificación 3GPP TS 33.203 detalla que la señalización entre el agente de usuario y el P-CSCF debe basarse en **IPsec ESP** (Encapsulating Security Payload) en modo transporte (se encripta solo payload a diferencia del modo tunel).

• **Pero el uso de IPSec en este modo no era adecuado para su uso en Redes Fijas (wired VoIP)**

• **El problema de IPsec está en el cruce de NAT,** por lo que TISPAN seleccionó el **modo de encapsulación UDP (User Datagram Protocol) de IPsec.**

VoLTE: Digest AKA & Ipsec
VoIP: Digest & UDP

Breve discusión en clase:
Notas sobre standares 3GPP y la identidad & la autenticación

IDENTIDADES Y REGISTRACIÓN

Algunos Standares

TS.24.229: Technical Specification Group Core Network and Terminals;
IP multimedia call control protocol based on
Session Initiation Protocol (SIP)
and Session Description Protocol (SDP);

TS.33.203: Technical Specification Group Services and System Aspects;
3G security;
Access security for IP-based services

TS.23.228: Technical Specification Group Services and System Aspects;
IP Multimedia Subsystem (IMS);

TS.23.003: Technical Specification Group Core Network and Terminals;
Numbering addressing and Identification;

TS.23.002:Technical Specification Group Services and System Aspects;
Network Architecture

SEGURIDAD DE ACCESO IMS PARA SIP

Authentication in IMS networks

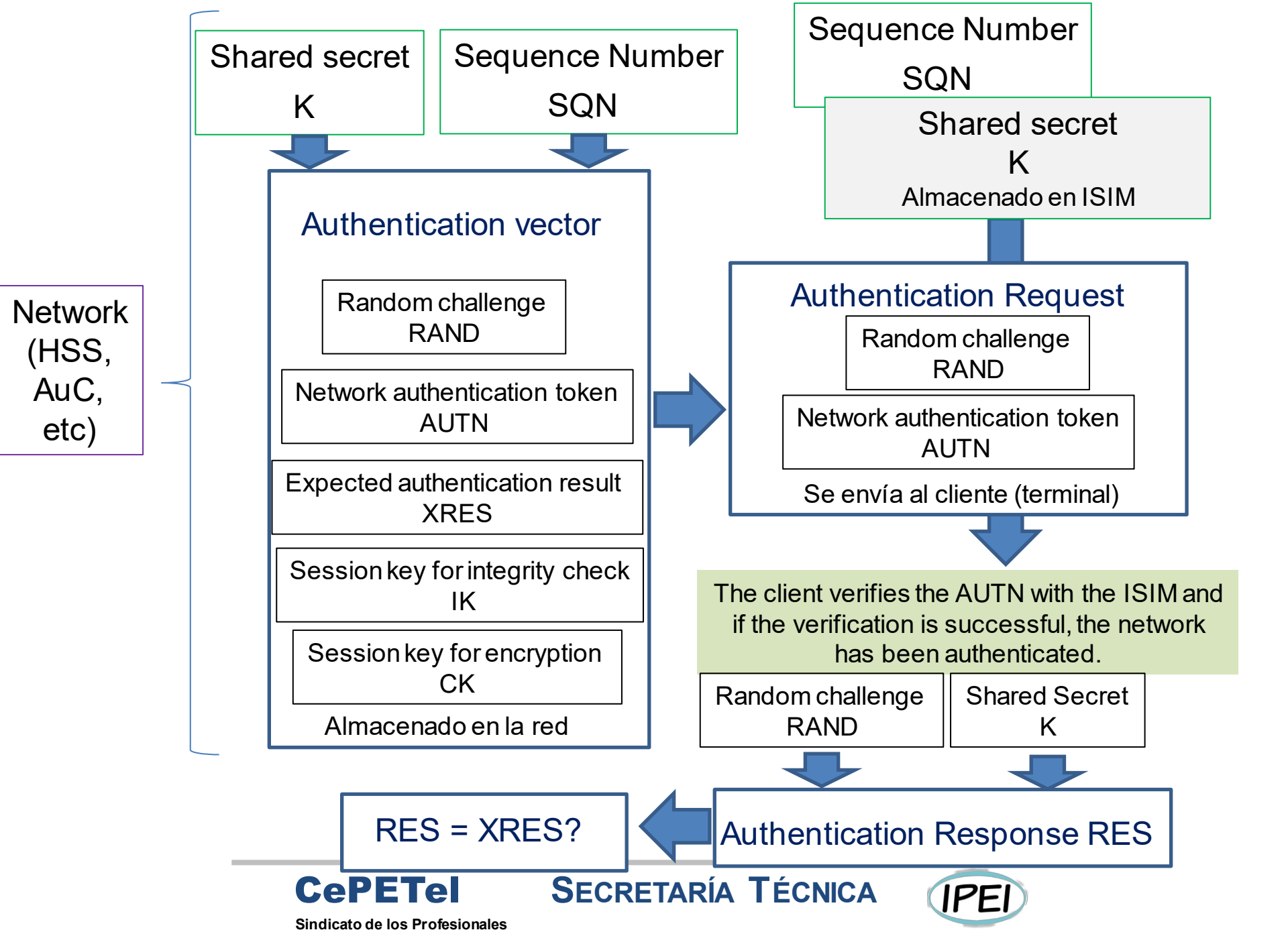
VoLTE Client sends SIP register request to IMS Server. The user is not authenticated at this point. The SIP register request contains IMS related identities (private identity, public identity, URI, etc).

The IMS server (S-CSCF) obtains authentication vector and SQN from HSS that contains a random challenge RAND, authentication token AUTN, expected authentication result XRES, a session key for integrity check IK, and a session key for encryption CK.

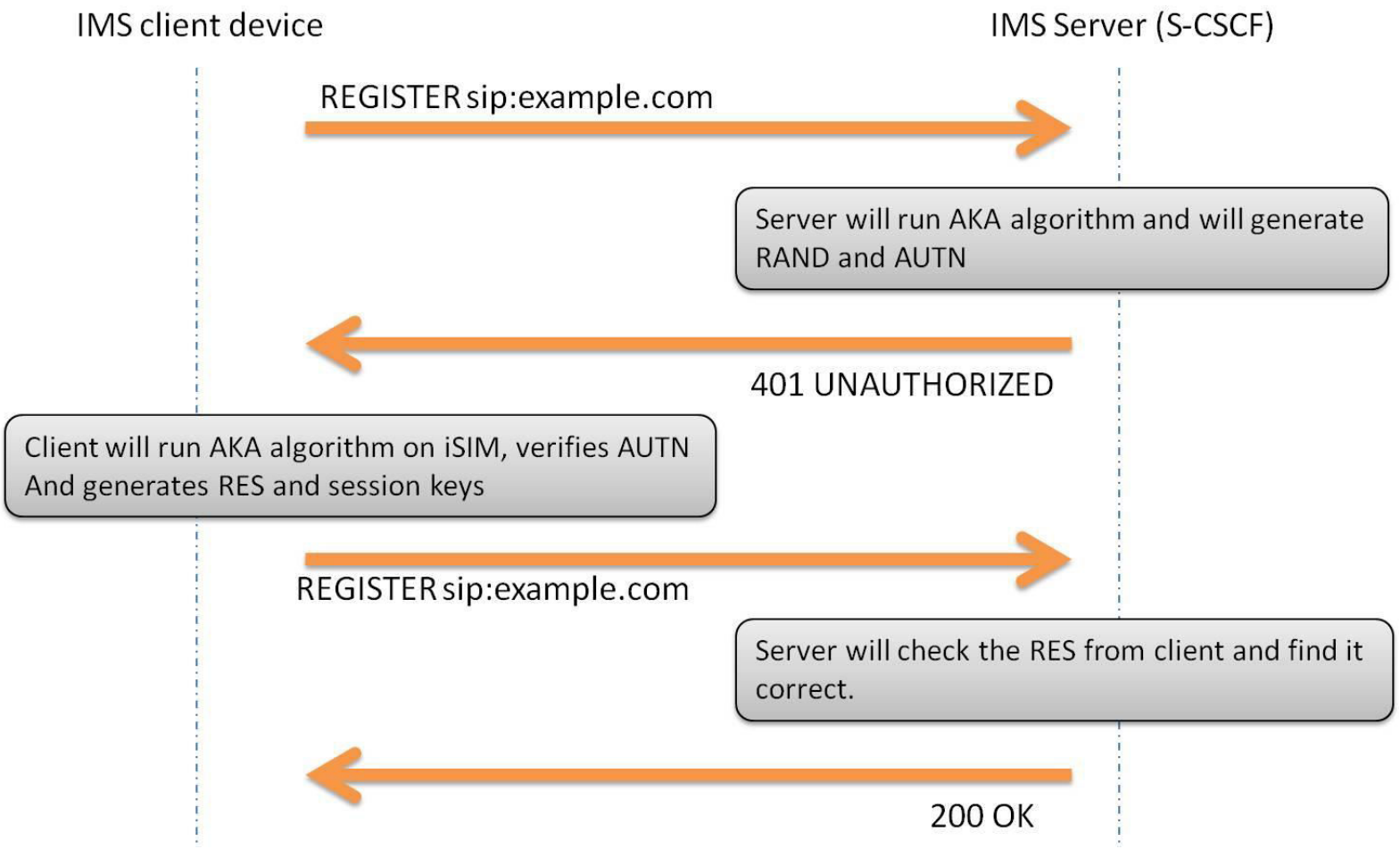
The server creates an authentication request, which contains the random challenge RAND, and the network authenticator token AUTN.

The authentication request is delivered to the client with "401 UNAUTHORIZED" message.

The client verifies the AUTN with the ISIM. If the verification is successful, the network has been authenticated. The client then produces an authentication response RES, using the shared secret K and the random challenge RAND.


Shared secret
K
Sequence Number
SQN
Sequence Number
SQN
Shared secret
K
Almacenado en ISIM
Network
(HSS,
AuC,
etc)
Authentication vector
Random challenge
RAND
Network authentication token
AUTN
Expected authentication result
XRES
Session key for integrity check
IK
Session key for encryption
CK
Almacenado en la red
Authentication Request
Random challenge
RAND
Network authentication token
AUTN
Se envía al cliente (terminal)
The client verifies the AUTN with the ISIM and if the verification is successful, the network has been authenticated.
Random challenge
RAND
Shared Secret
K
Authentication Response RES
RES = XRES?

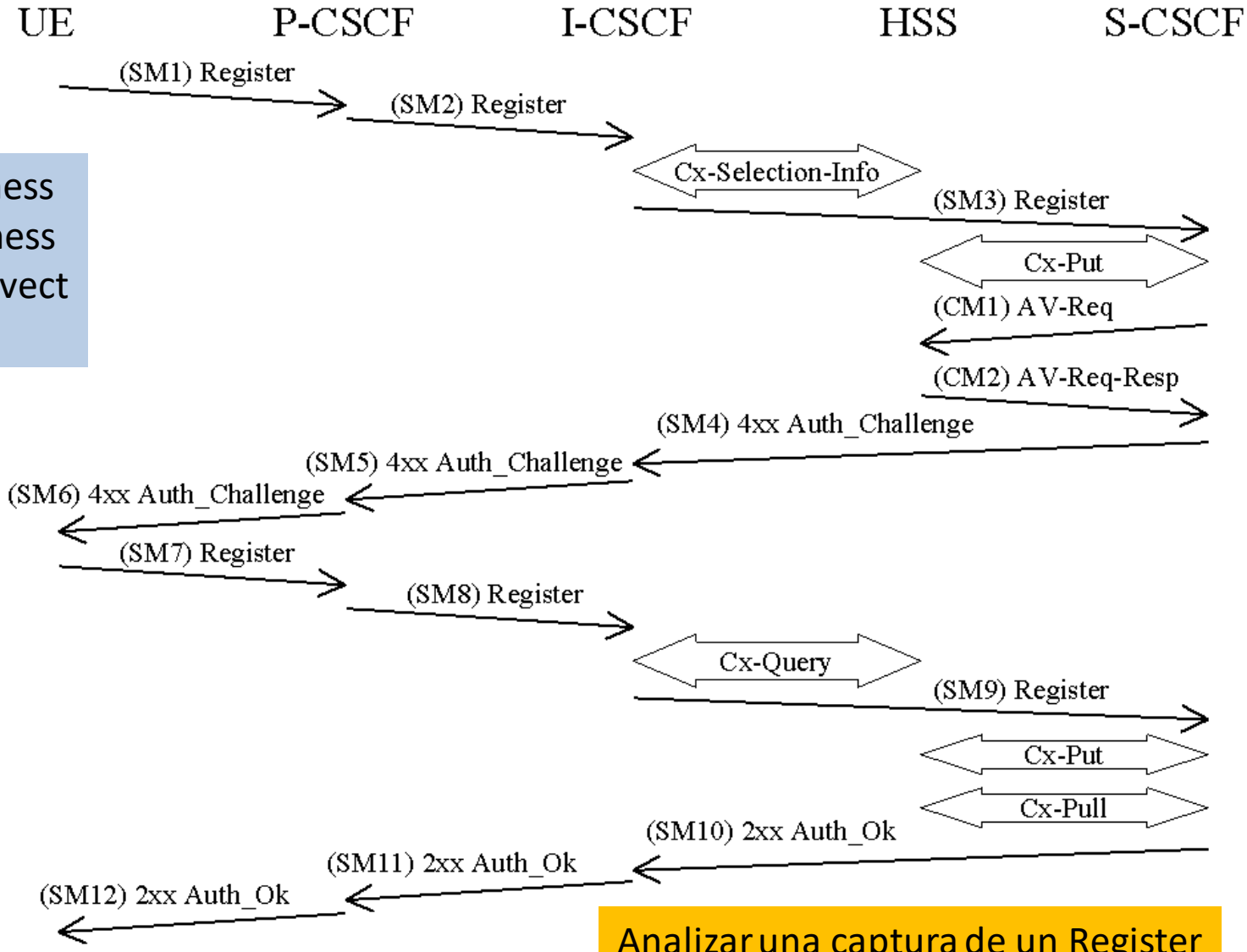
SEGURIDAD DE ACCESO IMS PARA SIP



Analizar una captura de un Register

SEGURIDAD DE ACCESO IMS PARA SIP

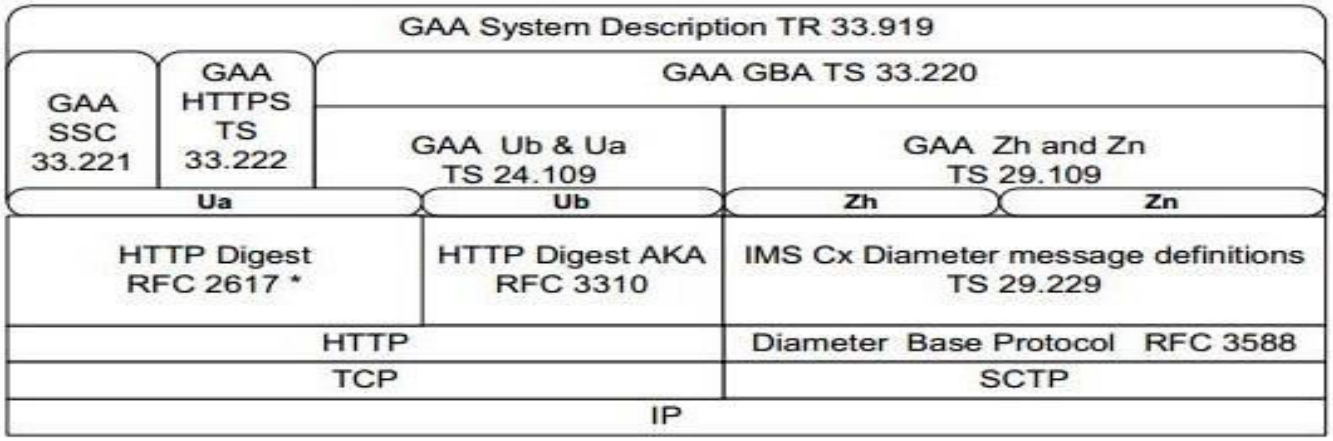
SM:SIP mess
CM: Cx mess
AV: Auth vect



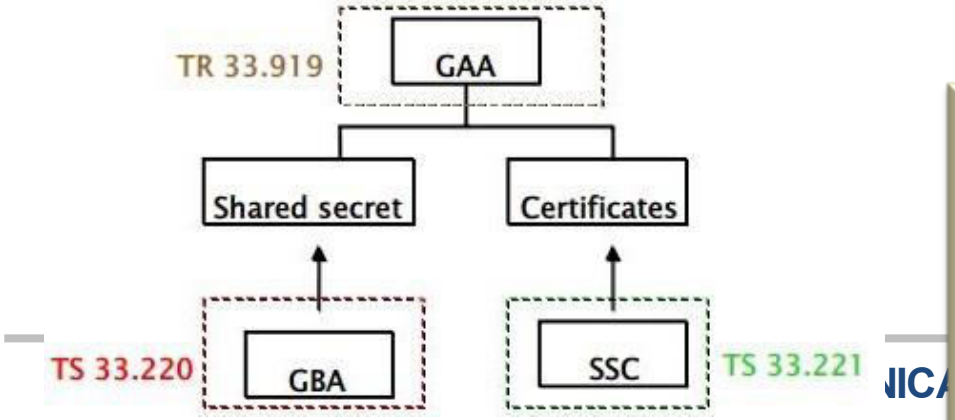
Analizar una captura de un Register

GAA (GENERIC AUTHENTICATION ARCHITECTURE)

todos los mecanismos de seguridad vistos son utilizados en redes de acceso y dominios IMS pero la **GAA** extiende estos mecanismos a nivel de aplicación/servicio.



GAA emplea dos mecanismos: uno basado en la posesión de un secreto compartido entre las entidades comunicantes **(GBA-Generic Bootstrapping Architecture)** derivada de las claves utilizadas en la autenticación AKA, y otro basado en criptografía asimétrica (claves pública y privada) y certificados digitales o **PKI (SSC-Support for Subscriber Certificates).**



Estos mecanismos son utilizados para el acceso remoto desde un UE al MTAS para gestionar Servicios. Se intercala un "Authentication Proxy"

AUTENTICACIÓN USANDO UN SECRETO COMPARTIDO - GBA

• Este es el método más utilizado.

• La gran ventaja de GAA/GBA es que permite la creación de asociaciones de seguridad entre el agente de usuario y las distintas aplicaciones.

• Estas asociaciones consisten en compartir una clave (el secreto compartido), que permite la autenticación posterior del agente de usuario frente a la aplicación, y si son necesarias, otras características de seguridad como la garantía de confidencialidad e integridad de la información (mediante cifrado y firma digital).

• El problema de estos mecanismos es la manera de acordar sobre este secreto compartido.

AUTENTICACIÓN BASADA EN CRIPTOGRAFÍA ASIMÉTRICA Y CERTIFICADOS

• Este método supone que la entidad que quiere ser autenticada debe poseer un par de claves (pública y privada) y un certificado digital que valide ese par de claves.

• Una vez en posesión de dichas claves y del certificado digital, el UE los puede utilizar para producir firmas digitales.

• La principal desventaja de este tipo de autenticación es que se necesita una PKI (Pub Key Infra) y que las operaciones con claves asimétricas requieren un esfuerzo computacional mayor.

• Si un cliente desea hacer uso de la tecnología de cifrado asimétrico, necesita un certificado digital, otorgado por una **CA (Certification Authority)**.

Estos mecanismos pueden Ser utilizados en WiFi Calling donde el UE y el ePDG se autentican

LIBERTY ALLIANCE Y EL SSO (SINGLE SING ON)

• La **Liberty Alliance** es un grupo de empresas que define especificaciones sobre la autenticación, privacidad y gestión de las identidades de usuarios de aplicaciones online.

• Uno de los conceptos manejados es el de **SSO (Inicio Único de Sesión)**, en el que un usuario solo necesita autenticarse una sola vez para acceder a diferentes aplicaciones o servicios.

• **El 3GPP hizo un estándar para la combinación de GAA/GBA y los mecanismos de autenticación y SSO definidos por Liberty Alliance y SAML v2.0.**

• Así se logra una autenticación fuerte, basada en AKA, con los mecanismos definidos por SAML v2.0 y Liberty Alliance para proporcionar SSO.

• No obstante, la mayor desventaja de GAA/GBA es que ha sido diseñada para agentes de usuario que cuenten con soporte de algún tipo de tarjeta.

• **OMA especificó soluciones de autenticación, por ejplo. basadas en HTTP Digest con credenciales de usuario, para terminales que no dispongan de tarjeta ISIM.**

ATAQUES EN IMS (I)

• **NETWORK SNOOP**

Rompe la confidencialidad. Sin la protección con IPSec es fácil capturar la señalización SIP y RTP usando herramientas como Wireshark. Otro ataque contra la confidencialidad puede realizarse mediante el uso de herramientas de análisis para reunir información sobre componentes, SO y topología de la red.

•**SESSION HIJACKING**

•Dirigido hacia la integridad. El atacante puede insertar paquetes maliciosos en una sesión e incluso sustituir una parte del tráfico. Por ejplo, el atacante puede enviar mensajes SIP Re-Invite para modificar los parámetros de la sesión. a esto el UE no puede ser registrado en la red o es registrado en un servidor falso.

• **DOS (DENIAL OF SERVICE)**

•Ataque contra la disponibilidad. El atacante envía un gran número de datagramas en muy poco tiempo, causando una degradación de servicio o llegando incluso a detenerlo por completo. Ejplo: son las inundaciones TCP SYN y UDP.

•**P-CSCF DISCOVERY**

•Orientado a la integridad y disponibilidad. El P-CSCF es el punto de entrada para el UE. DHCP (Dynamic Host Configuration Protocol) y DNS son muy utilizados para descubrir el P-CSCF. Un atacante puede romper el proceso de descubrimiento de P-CSCF envenenando la caché del DNS para que el nombre de un dominio o IP falso sea devuelto al UE.

ATAQUES EN IMS (II)

• **SERVICE ABUSE**

Impacta sobre la disponibilidad e integridad de IMS. Los usuarios autorizados pueden utilizar los servicios más de lo esperado o acceder a servicios que no están permitidos para ellos.

• **TOLL FRAUD**

Ataque contra el accounting. Un atacante puede falsificar un UE y enviar un BYE Request al CSCF. El CSCF, piensa que la sesión finalizó, para de contabilizar al mismo tiempo que los UE no liberan los flujos de medios por lo cual los UE siguen intercambiándose flujos sin ser contabilizados. Se debe a la falta de control de flujos de medios.

• **PERMISSION ACQUISTION**

Ataque contra la autenticación. Un atacante puede obtener la contraseña de autenticación por diferentes métodos. Básicamente, un UE que no dispone de una tarjeta ISIM emplea el método HTTP Digest basado en un nombre de usuario y una contraseña que no es de alto nivel de seguridad. HTTP Digest sólo enumera varios ataques, como un ataque de fuerza bruta o un ataque de repetición.

RICH COMMUNICATION SUITE /SERVICES (RCS)

RCS surgió como una iniciativa de GSMA para ofrecer de manera standard, una serie de servicios de comunicaciones enriquecidas tanto en redes móviles como fijas.
El proyecto pasó por muchas etapas, las que incluyeron el cambio del nombre, sin llegar a tener nunca el éxito deseado

- **Libreta de Direcciones Multimedia:**
  - Actualización automática
  - Foto de perfil
  - Estado on line
  - Información de capacidad de presencia y servicio

- **Llamada enriquecida:**
  - Permite compartir videos ("look at me now", imágenes y archivos durante una llamada de voz
  - Mensajería mejorada, SMS, MMS y Mensajería instantánea uno a uno y uno a muchos

RICH COMMUNICATION SUITE (RCS) SOBRE IMS

- **Potencia servicios de comunicación:**
  - IM/chat: vista del diálogo → uno a uno o uno a muchos
  - SMS/MMS con vista unificada del coordinador y del diálogo
  - Transferencia de archivos MM: intercambio rápido, no es "best effort"

- **Arquitectura basada en IMS:**
- **Backup & sincronización:**
  - Backup y sincronización con PC / Notebook

RICH COMMUNICATION SUITE (RCS) SOBRE IMS

Características

- Para su lanzamiento RCS tuvo varias pruebas de IOT entre Operadores y Proveedores
- IOT entre terminales y redes
- Despliegue de servicios RCS interoperables en un país o entre países
- Basado en el Core IMS para transmitir señalización y media
- Funciona con redes móviles de varias tecnologías (2G, 3G, 4G, …)
- Soporta nuevos servicios de la red del Operador → Usuario con múltiples dispositivos
- Necesita del encabezado “subjet header” en INVITE de SIP para ser cambiado

RCS se apoya en:
- GSMA, OMA y XDM: XML Document Management

RCS presenta ventajas comerciales:
- Aplicable a todos los mercados (fijo y móvil)
- Varios modelos de tasación: pay-per-use, prepago, suscripción
- Mejora velocidades de registro en redes móviles e ingresos por llamada

RICH COMMUNICATION SUITE. TRABAJOS EN GSMA

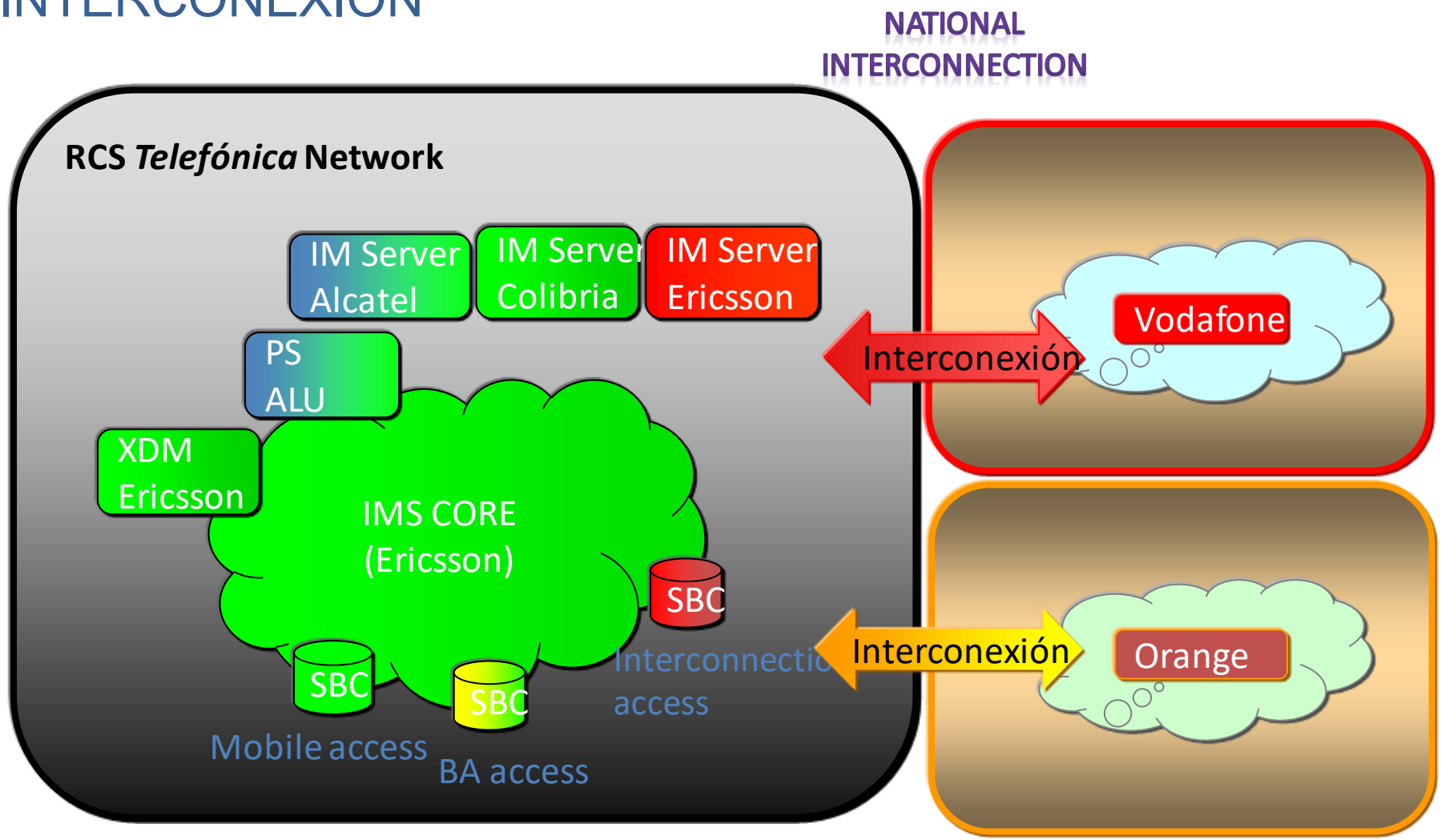
Breve reseña de releases de RCS (inicio hasta 2014 aprox):

- RCS Release 1: Funcionalidades orientadas a móviles (Enhanced Address Book, Enhanced Messaging and Enriched Communications)

- RCS Release 2: Convergencia fijo y móvil de cliente (Broadband Access, Multi-Device Environment, Network Address Book)

- RCS Release 3:
  - "NVAS" (Network Value Added Services). Ejplo: envío de foto a otro usuario y aviso que fue depositada en su recipiente.
  - Retro-compatibilidad con releases R1 y R2
  - Geo-ubicación
  - Inclusión de URL en el estado de los contactos
  - Integración de Servicios mediante API's abiertas

RICH COMMUNICATION SUITE. TRABAJOS DE INTERCONEXIÓN



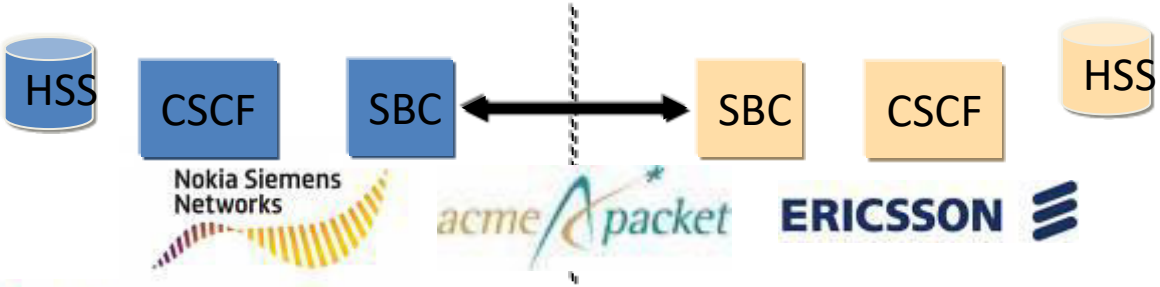
RICH COMMUNICATION SUITE. TRABAJOS DE INTERCONEXIÓN

colibria

Test object interface:
RCS Network – Network Interface (NNI)
Release 1

ERICSSON

XDM
PRESENCE
IM

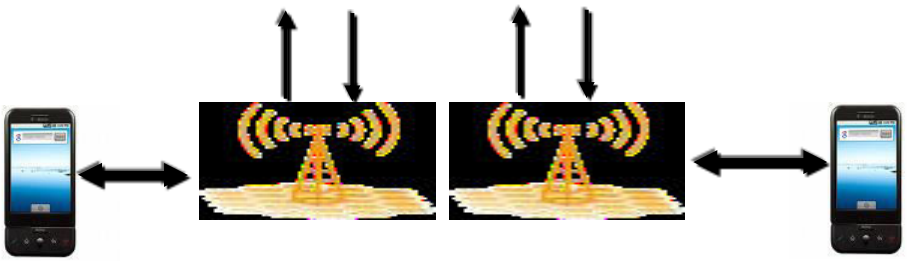


XDM
PRESENCE
IM

WIND

TELECOM ITALIA

Client tested:
Nokia C4
and Movial



Client tested:
Ericsson
and Nokia C4

Local 3G
Radio Access

Local 3G
Radio Access

RICH COMMUNICATION SUITE. TRABAJOS EN GSMA

Si bien se hicieron pruebas de integración exitosas desde 2009/2010, RCS no logró el éxito y la adopción esperada.

La dependencia de un entorno IMS consolidado conspiró contra el TTM

Las complejidades de integración, la necesidad de un despliegue de IMS que perimitiera desarrollo y la instalación de un cliente ralentizaron su adopción

Aun cuando RCS ofreció desde el inicio ventajas competitivas como la calidad de servicio, ell factor TTM, hizo que los clientes adoptaran otros servicios como WhatsApp sin que sus limitaciones “del tipo best Effort” pesaran en su elección

RICH COMMUNICATION SERVICES (RCS)

Segunda Etapa

As a general overview, RCS is part of the new Advanced Messaging standard designed to greatly improve messaging functionality that comes installed on phones by default. Along with text messages, RCS will also allow for higher quality picture messaging up to 10MB in size, group chats, location sharing, and even video calls by default. The service also appears to support read receipts and typing indicators that you're probably already familiar with from other services.

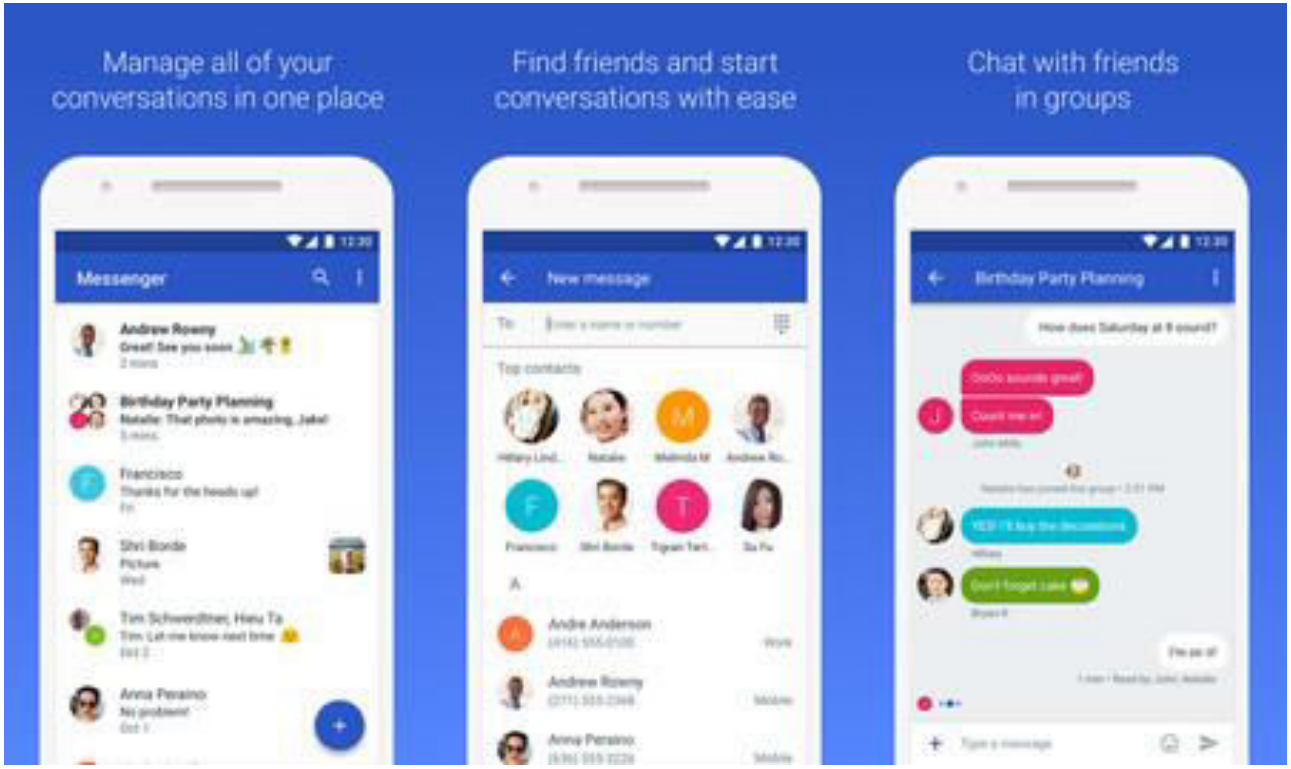
Unlike SMS, the new technology can be integrated with contact apps to see who else supports the service, as well as for sharing contacts and groups. RCS is also looking to go beyond the capabilities seen in many of today's messaging apps. The standard can also be used to share media, location, and other information while you're already in a telephone conversation.

However, to send and receive Rich Communications Services messages, both parties much be using a compatible messaging app and network, and support is not universal, yet. Fortunately, the system is designed to fall back to SMS or MMS when the recipient doesn't support RCS.

RICH COMMUNICATION SERVICES . RELANZAMIENTO

https://www.xataka.com/basics/que-es-el-rcs

Acuerdo con Google Samsung y otros fabricantes, con el propósito de retomar la original idea de mensajería instantánea disponible en el propio terminal (no app)



Discutir otros ejemplos servicios que no se basan en apps. Hay realmente alguno?

RICH COMMUNICATION SERVICES . RELANZAMIENTO

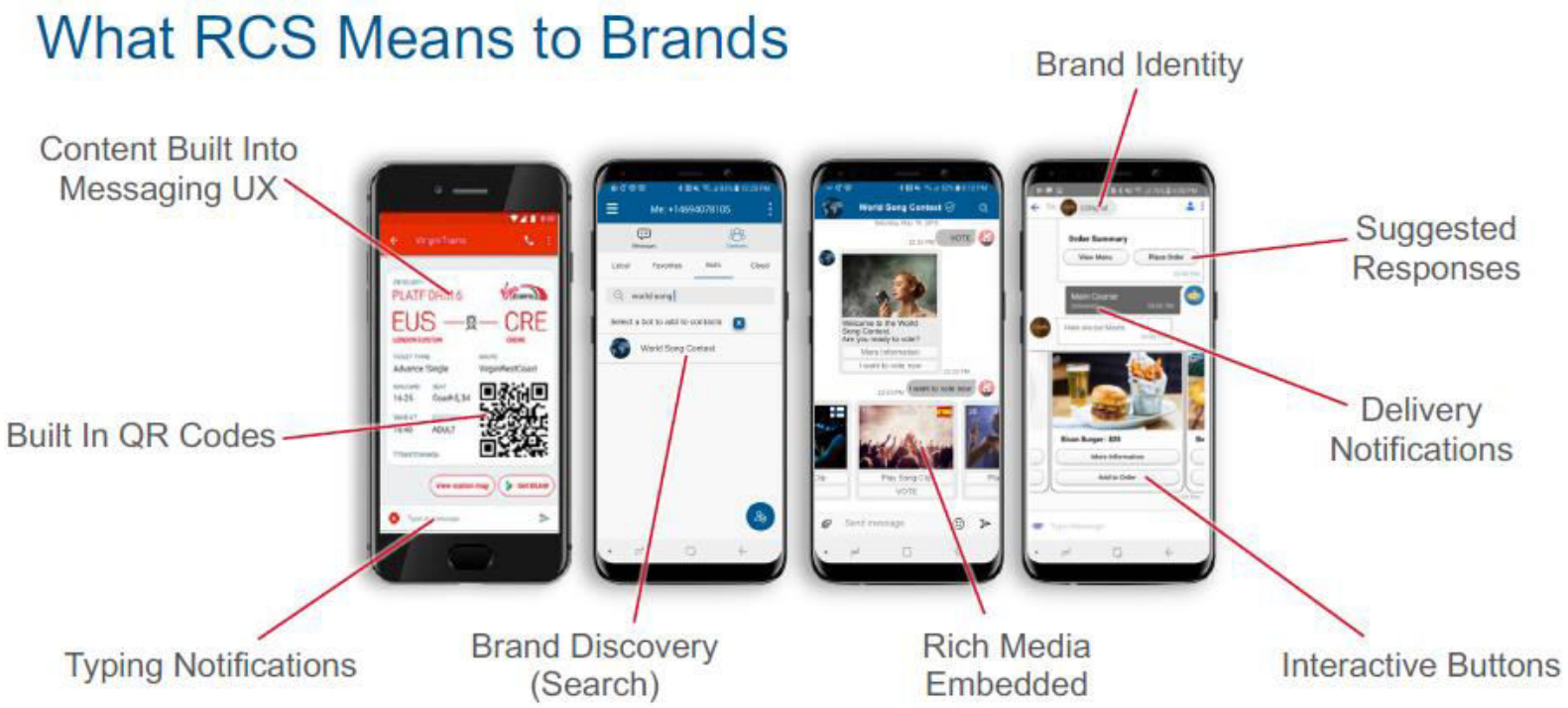
- A mediados de 2007 se impulsa desde la industria, en 2008 surge como estándar de GSMA
- Trata de imponerse como la evolución de SMS y MMS
- No logra trascendencia hasta la irrupción de Google a finales de 2016
- Con el impulso de Google, se aceleran los estándares entre Operadores Móviles y Fabricantes de Terminales
- Busca competir con las mismas prestaciones que otros servicios de mensajería tales como Whatsapp, iMessage, WeChat, Telegram o Line
- Disponible en aplicaciones nativas para terminales Android (Android Messages)
- Retrocompatible con SMS y MMS para terminales viejos
- Al igual SMS, no está cifrado de extremo a extremo

RCS no es SMS

- Competir con Whatsapp
- Potenciar el negocio A2P (app to person) con un nuevo canal
- Ofrecer el nuevo "0800 App" a pequeños comercios
- Recuperar ingresos en mensajería
- Evolucionar la experiencia de usuario en mensajería

https://www.altiria.com/4040/que-es-sms-a2p-ventajas-y-ejemplos-de-uso/

RICH COMMUNICATION SERVICES . RELANZAMIENTO

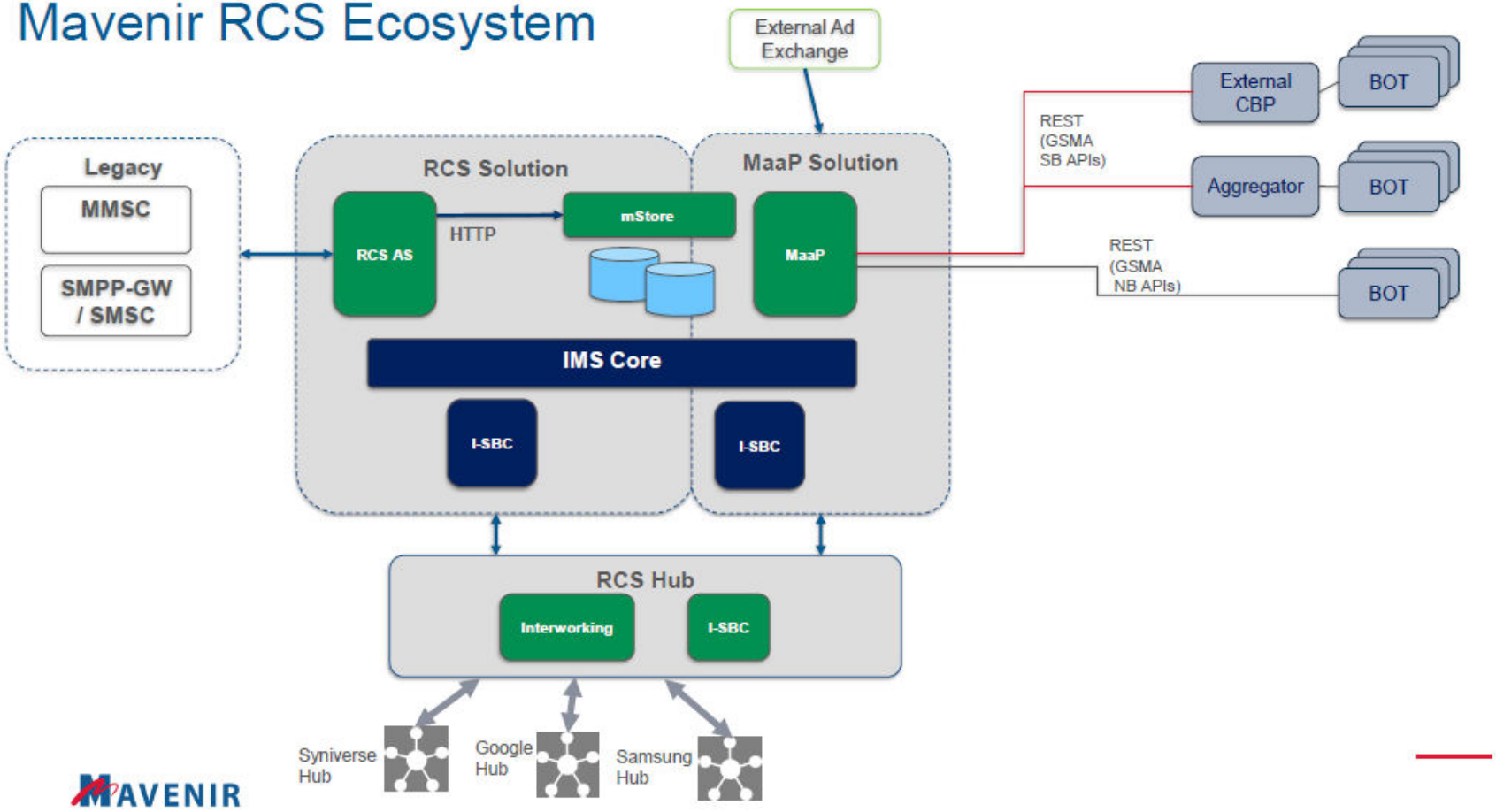


UX design refers to the term “user experience design”, while UI stands for “user interface design”

RICH COMMUNICATION SERVICES

Modelos de Integración

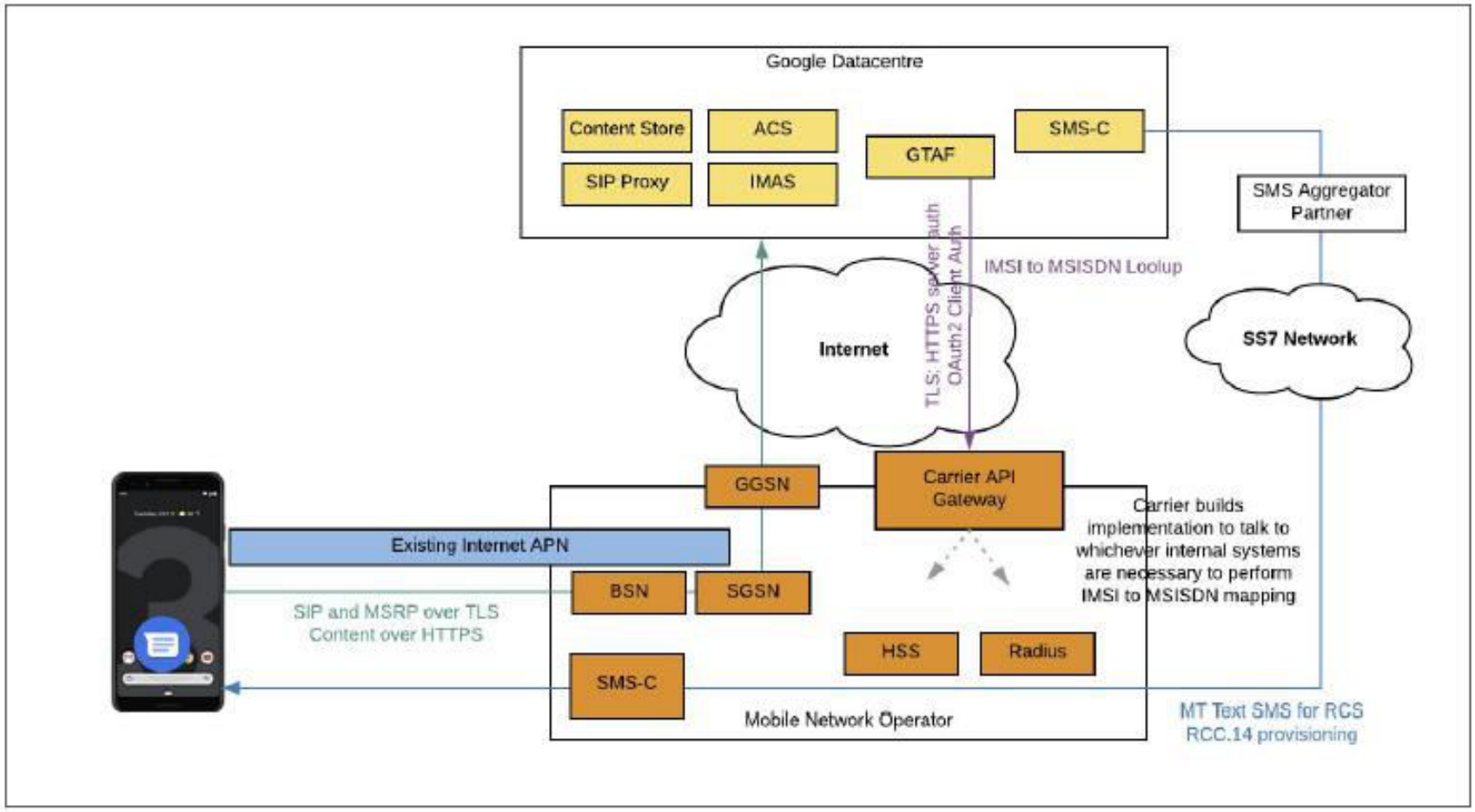
Mavenir RCS Ecosystem



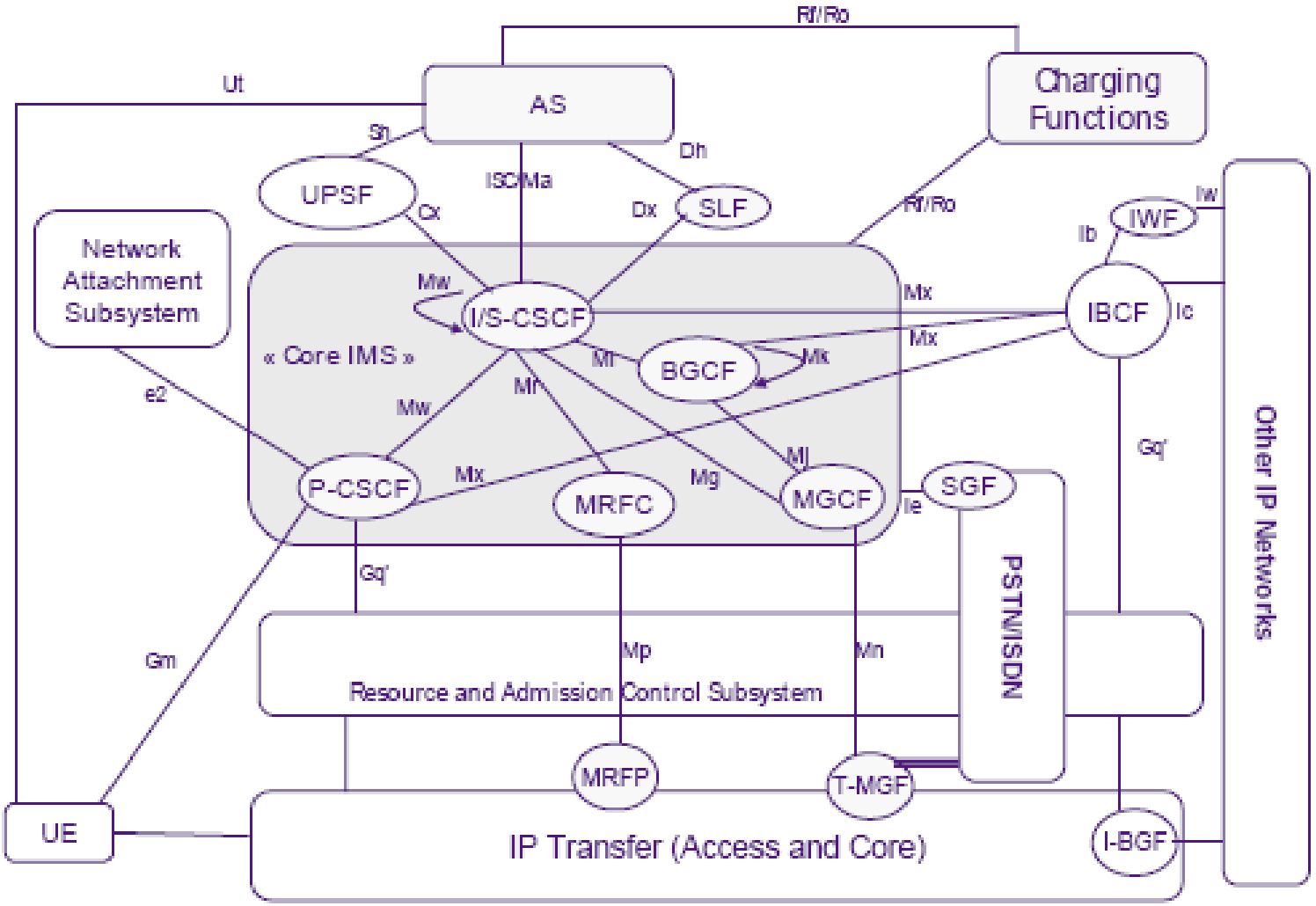
MaaP : Messaging as a Platform
https://www.zte.com.cn/global/about/news/0630ma3.html
Chatbot: programa con el que es posible mantener una conversación

RICH COMMUNICATION SERVICES

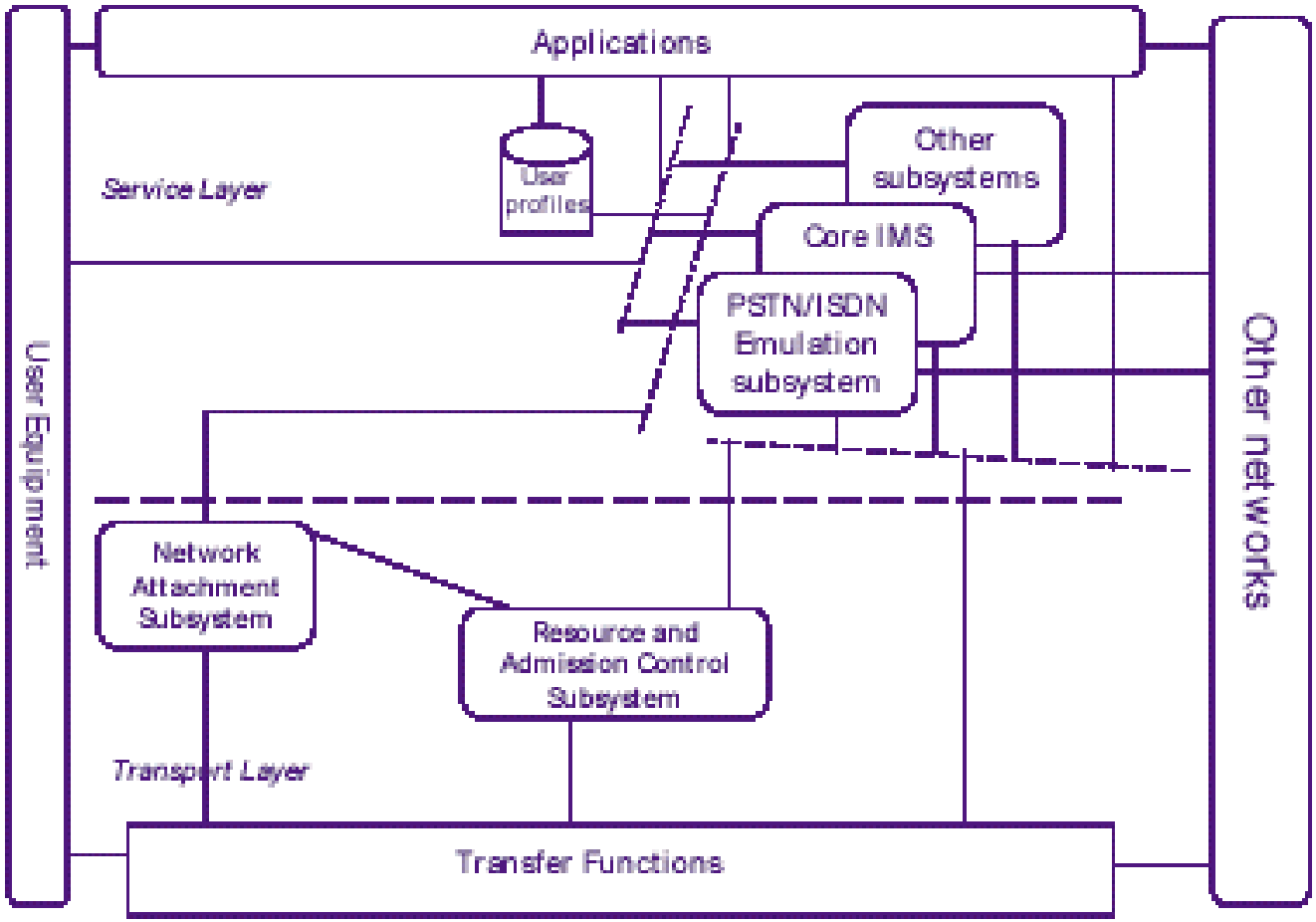
Modelos de Integración



IMS PARA REDES FJAS-ARQUITECTURA GENERAL SEGÚN TISPAN



IMS PARA REDES FJAS-ARQUITECTURA GENERAL SEGÚN TISPAN



SUBSISTEMAS DESTACADOS EN LA ARQUITECTURA TISPAN

- El Core IMS soporta la *provisión* de servicios multimedia (SIP) a los terminales NGN, así como la simulación de servicios PSTN/ISDN (PSS).

- El subsistema PES soporta la emulación de servicios PSTN/ISDN para terminales legacy conectados a la NGN a través de Gateways residenciales o de acceso (detalles de PES en ES 282 002).

- NASS (Network Attachment SubSystem), encargado de funciones como la asignación dinámica de IP, autenticación, autorización al acceso a la red, etc.

- RACS (Resource and Admission Control Subsystem), encargado de las funciones de control tales como NAPT, marcado de prioridades (campo TOS) siguiendo políticas del Operador y recursos disponibles, como por ejplo. anchos de banda suscriptos (detalles en ES 282.003).

ENTIDADES ESPECÍFICAS DE TISPAN

Media Gateway Function (MGF):

• Hay tres variantes:

✓ R-MGF: Residencial, ubicado en casa del cliente

✓ A-MGF: Acceso, reside en la red IP (su acceso o bien al Core)

✓ T-MGF: Trunk, frontera entre la red IP y la PSTN/ISDN/PLMN

• Los tipos A-MGF y R-MGF permiten acceso al subsistema PES; obviamente en el caso del T-MGF, los servicios siguen en el dominio de la PSTN.

• T-MGF, es idéntico a IMS-MGW definido en TS 123.002, aunque podrían haber diferencias particulares sobre algunos recursos.

• Si bien ETSI no lo define, a modo de espejo con lo dicho para los Media Gateway (prefijos A, T y R), algunos suministradores usan esos mismos prefijos para definir roles en sus MGCF.

ENTIDADES ESPECÍFICAS DE TISPAN

Media Gateway Function (MGF):

• Hay tres variantes:
- ✓ R-MGF: Residencial, ubicado en casa del cliente
- ✓ A-MGF: Acceso, reside en la red IP (su acceso o bien al Core)
- ✓ T-MGF: Trunk, frontera entre la red IP y la PSTN/ISDN/PLMN

• Los tipos A-MGF y R-MGF permiten acceso al subsistema PES; obviamente en el caso del T-MGF, los servicios siguen en el dominio de la PSTN.

• T-MGF, es idéntico a IMS-MGW definido en TS 123.002, aunque podrían haber diferencias particulares sobre algunos recursos.

• Si bien ETSI no lo define, a modo de espejo con lo dicho para los Media Gateway (prefijos A, T y R), algunos suministradores usan esos mismos prefijos para definir roles en sus MGCF.

ENTIDADES ESPECÍFICAS DE TISPAN

Border Gateway Function (BGF):

• Conocido como SBC o SBG, puede estar ubicado en la casa del cliente o en la red. Puede ir entre la red de Acceso y el Core o bien entre el Core y el Core de otra Operadora. Los primeros se conocen como C-BGW y los segundos como I-BGW.

• Realiza múltiples tareas, como filtrado de paquetes, análisis según origen/destino, resuelve temas de NAT y NAPT, protege contra ataques, aplica Lawfull Interception, Topology Hidding, Interworking entre IP V4 y IP V6, etc.

Interworking Function (IWF):

• Lleva a cabo el interworking entre protocolos de los subsistemas de control de servicios NGN TISPAN y otros protocolos IP. El caso más relevante puede ser SIP IMS vs. SIP IETF.

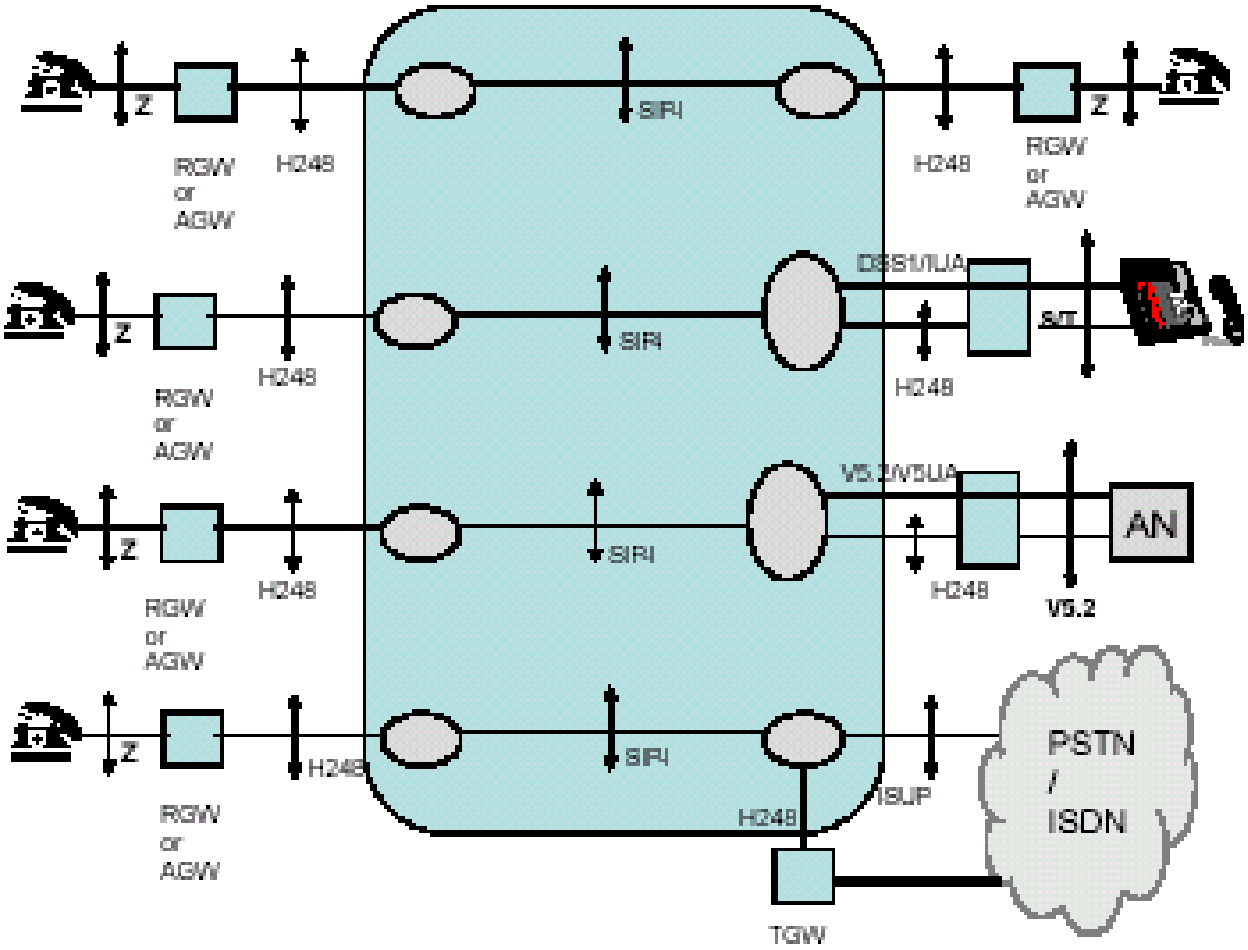
QUE SE REUTILIZA DE LA NGN?

- Mediagateway Controllers (Softswitches): MGCF
- SBCs: NAPT y eventualmente P-CSCF
- Media Gateways: MGF
- Signalling Gateways (integrados en Softswitch)
- Media Servers: MRFC/MRFP
- SIP App Servers (pasan de modo Stand Alone a entorno IMS vía interfaces ISC/Sh)
- IETF SIP Endpoints (si se dispone terminales que no incorporen la interfaz Gm, se hace conversión a interfaz Gm via SBC)
- Interfaces Mg y Mj entre el Core IMS y el MGCF requieren implementaciones especiales dependiendo del país (ejplo.: Presuscripción, 911, etc.)
- Reuso de SIP Endpoints requiere adaptar la aplicación en los SIP AS del Core IMS
- Integración de SIP AS con el Core IMS típicamente vía ISC.
- Interfaz Sh no disponible (dificulta la integración de BdD con el HSS)

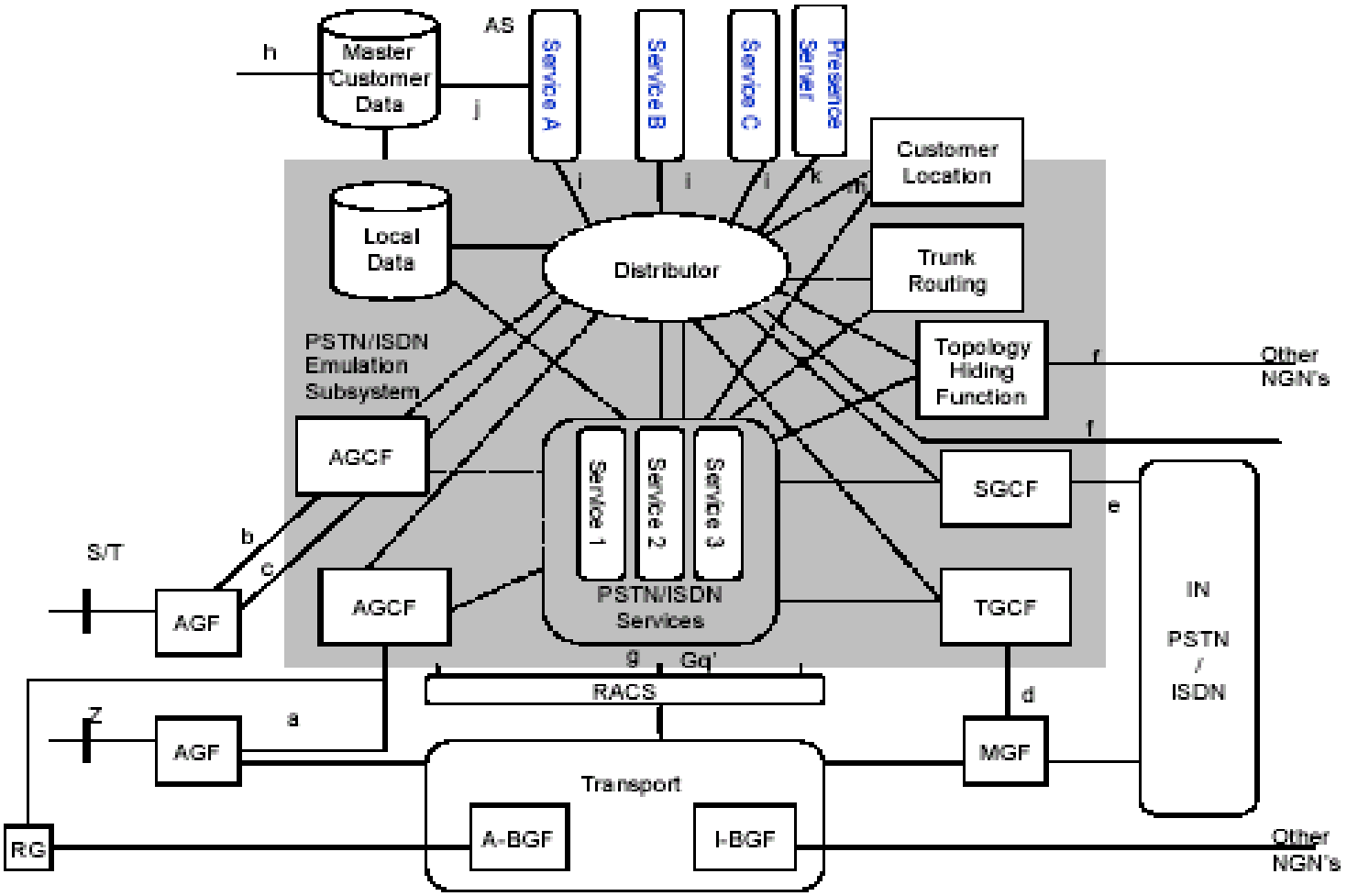
DESAFÍO IMS

- Integración con redes NGN o Pre-IMS preexistentes
- IOT (redes multivendor). Ej.: un CSCF “A” con un Softswitch “B” (interfaz Mg).
- Aspectos de Arquitectura:
  - Escalabilidad
  - Confiabilidad (ser tan confiable como las arquitecturas anteriores)
  - Funciones de borde del IMS: SBC vs P-CSCF. Que hacemos con los SBC existentes monolíticos?
- Independencia del Acceso: hasta que punto?
- QoS/QoE
  - Mitos y verdades sobre QoS
  - RACF/PCRF: que valor agregan frente a mecanismos estáticos de QoS?
- Integración OSS/BSS: el mayor desafío?
- HSS: Lo provee el suministrador del Core?
- IMS UE: No soporte de interfaz Gm. Se pone de manifiesto en RCS.
- “IMS lite” también conocido como “Next Generation Softswitch”...
- Aspectos económicos: una sola aplicación justifica el despliegue?
- Comparación Softswitch vs IMS
- Integración con IPTV y Redes CDN

SUBSISTEMA PES



SUBSISTEMA PES



SUBSISTEMA PES

• En las especificaciones de Entidades Funcionales en la NGN se tiene en cuenta que hay muchas implementaciones completas o en desarrollo.
• Por tanto, es apropiado proceder a estandarizar en una forma más prescriptiva. La intención es sólo estandarizar los flujos de información dentro y fuera del **PES** (PSTN/ISDN Sub-sistema de emulación) y no establecer una implementación particular (detalles en ETSI ES 282 002).

• El punto “a” vincula a AGW con interfaz POTS, los “b” y “c” lo hacen con un AGW con interfaz ISDN (“b” para BRI y “c” para PRI) y los “d” con MGW.
• Se incluyeron los bloques de servicios (1, 2 y 3) al solo efecto de dar cabida a desarrollos preexistentes donde los servicios están distribuidos en varios servidores. Estos son los Servicios Básicos (Dial Tone) y Suplementarios.
• Si bien el TGCF y el AGCF aparecen separados de los bloques funcionales de servicios, el estándar indica que no es mandatorio y de hecho, las funcionalidades podrán estar distribuidas de muchas maneras posibles.
• Si se incluyen los AS A, B, C en un entorno IMS y se desea acceder a ellos, entonces el bloque “distribuidor” será un CSCF. ***Aquí aparece un conflicto de límites ya que por un lado se dice que PES no es una parte de IMS pero por otra ambas partes usan un elemento común.***

SUBSISTEMA PES

• Entre el PES y la Capa de Aplicación del IMS está el punto de referencia “i”.

• Este punto “i” permite al PES invocar servicios de valor agregado tal como son definidos por un perfil de usuario particular.

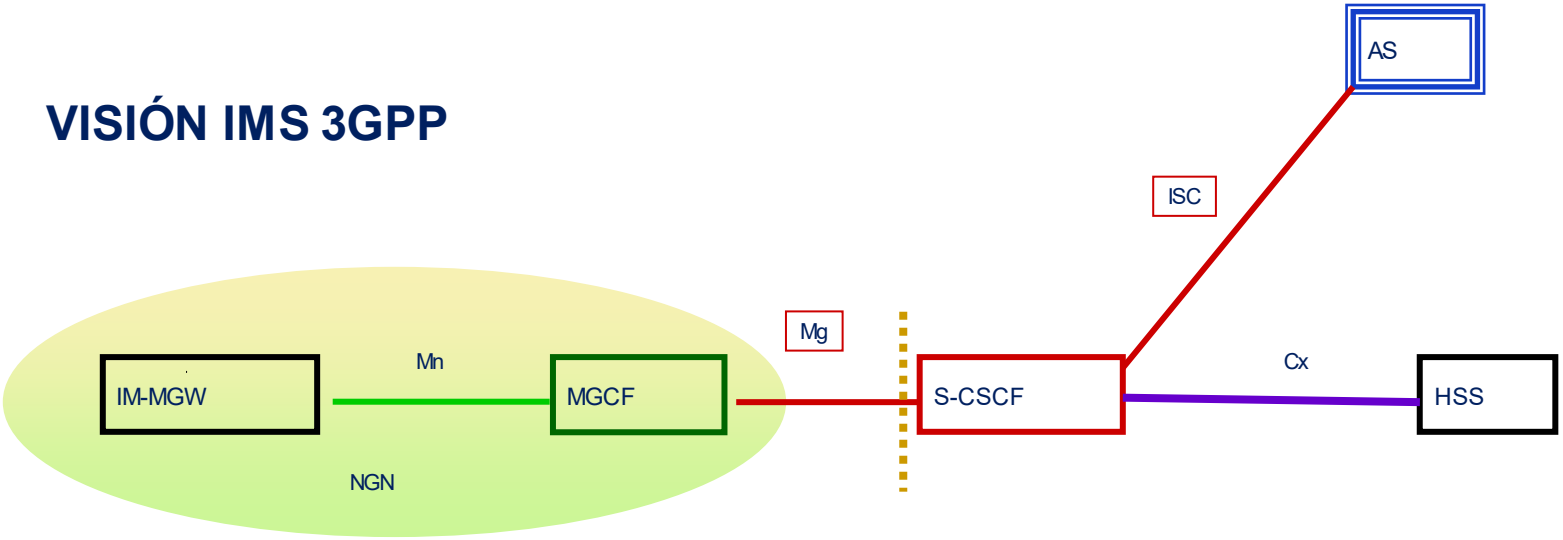
• Para lograr máxima uniformidad y reutilización a través de los Sub-Sistemas en la arquitectura TISPAN NGN, los servicios de valor añadido A, B y C son asumidos para ser desplegados en AS IMS y por lo tanto, la elección del protocolo y flujos de información que fluyen a través del punto “i” son equivalentes a las de la interfaz ISC en el IMS.

• Tb, este punto “i” lleva señalización SIP IMS bajo estándar TS 124 229 a otros componentes IMS y puede ser utilizado para interconectar a IMS usando SIP.

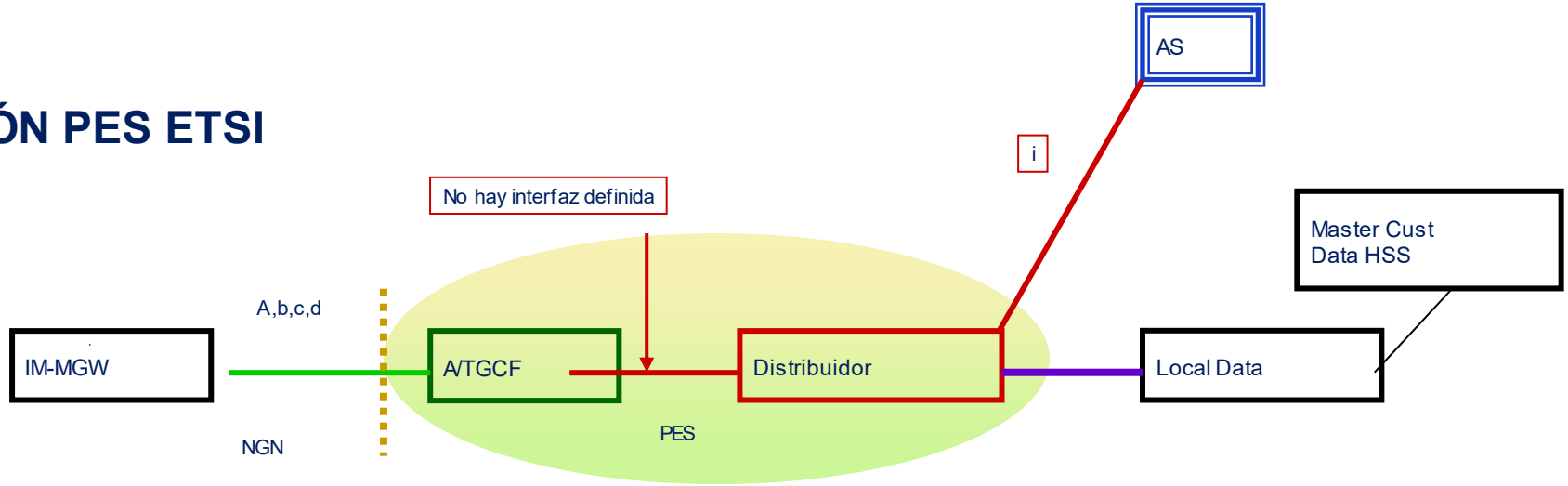
• El punto “k” sirve para habilitar suscripciones relacionadas con Servicio de Presencia, notificaciones y publicaciones entre los AS IMS y el PES.

SUBSISTEMA PES. VÍNCULO IMS (3GPP) / PES NGN (ETSI)

VISIÓN IMS 3GPP



VISIÓN PES ETSI



RACS (RESOURCE AND ADMISSION CONTROL SUBSYSTEM)

¿Cuáles son sus funciones principales?

• **Service Based Local Policy Control:** autorización de pedidos de QoS y definición de las políticas a ser aplicadas por los elementos de red.

• **Soporte de Application Function (AF):** pedidos de reserva de recursos iniciados por la red o por el CPE. Ejplo.: permite QoS sobre redes de accesos diferentes (ADSL / GPRS).

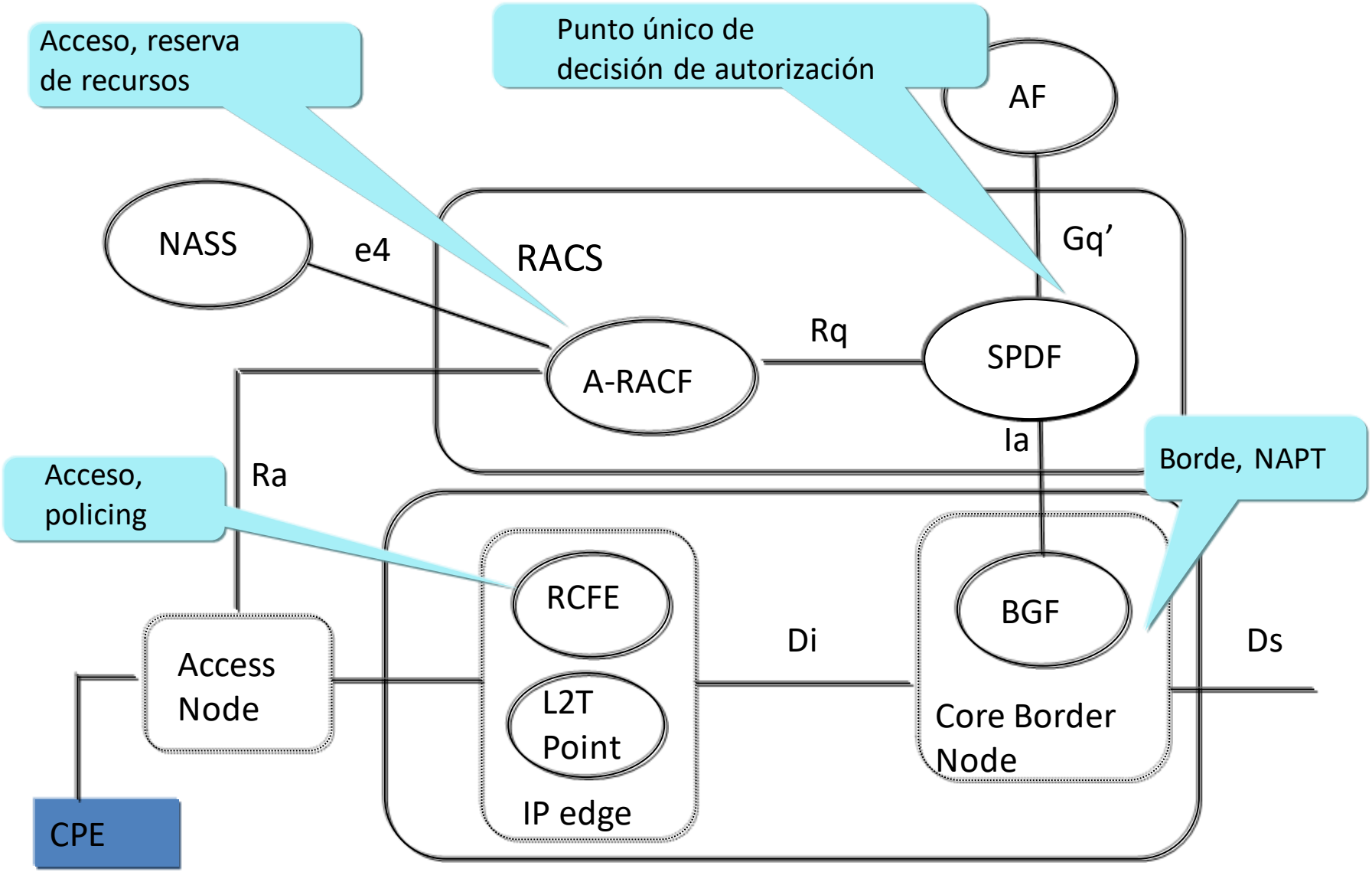
• **Control de Admisión:** aplica el control a los pedidos de reserva, basándose en la disponibilidad de recursos de transporte en el acceso (no cualquiera puede pedir cualquier cosa).

• **NAPT / Gate Control:** controla el near-end y far-end NAPT y funciones de firewall. En casos como:

- Dos redes core NGN TISPAN o
- En el borde entre red de acceso y el core NGN TISPAN

utiliza Topology Hiding, en IBCF/IBGF/SBC sobre NNI.

RACS (BLOQUES FUNCIONALES)



NASS (NETWORK ATTACHMENT SUBSYSTEM)

- NASS provee registración e inicialización del CPE para lo cual soporta las siguientes funcionalidades principales:

✓ Direcciones IP y configuración de parámetros

✓ Autenticación de usuario

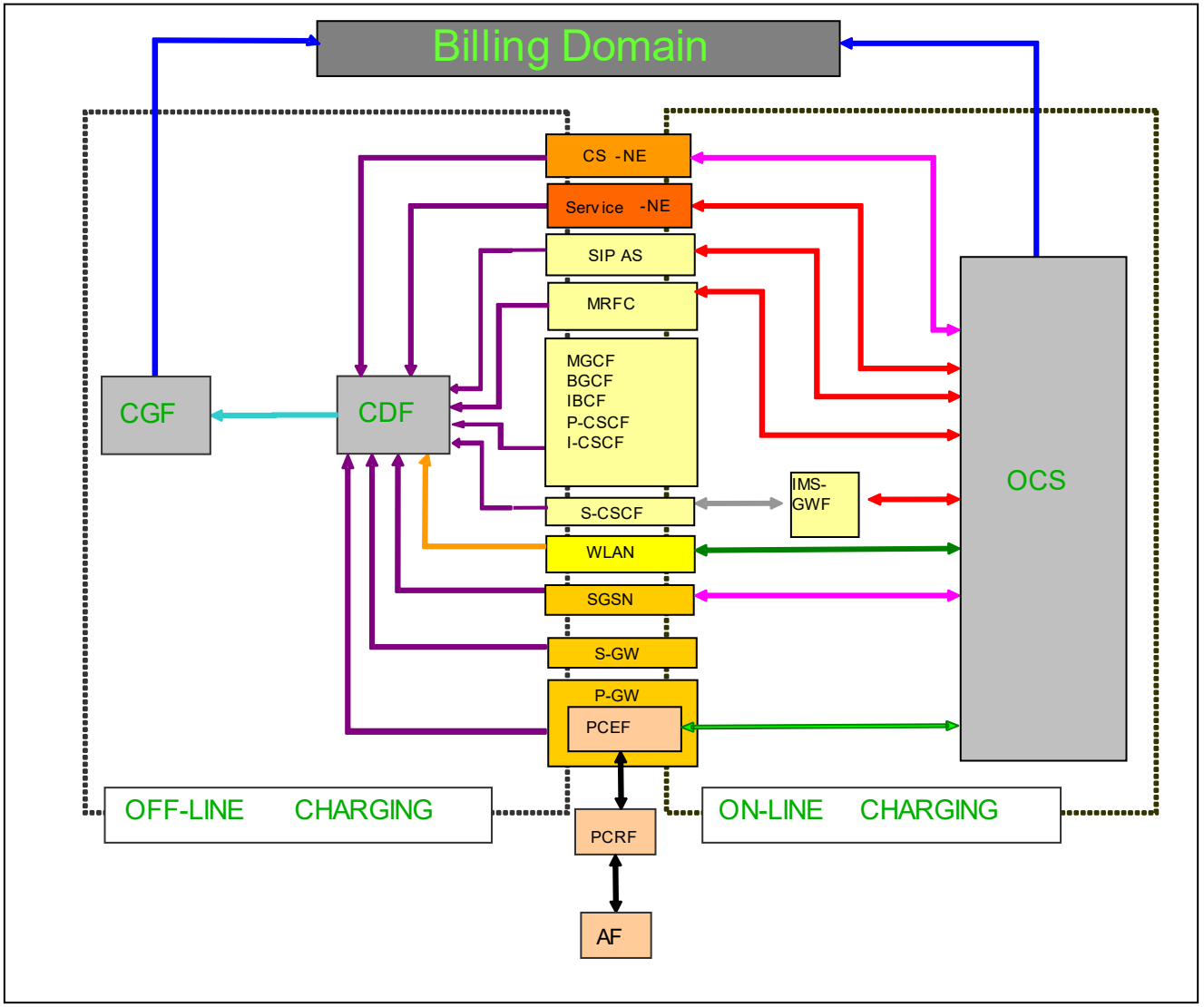
✓ Autorización de red

✓ Configuración del acceso a la red, en función del perfil del usuario.

✓ Gestión de ubicaciones

Discusión sobre VTP

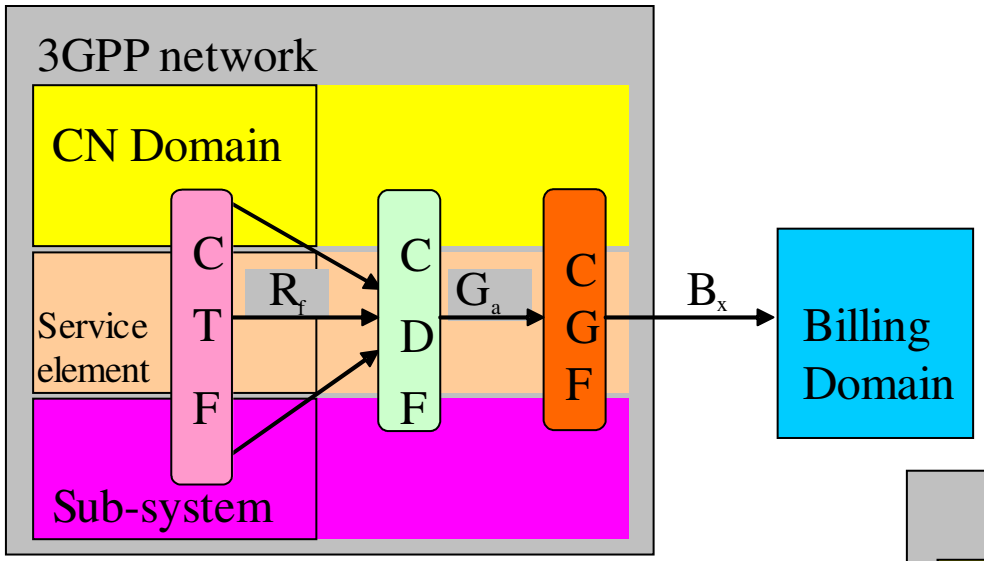
TASACIÓN EN IMS



Tasación Off-line y On-line.

Estándares:
(IMS Charging)
TS 32.240
TS32.260
(CS/PS Domain Charging)
TS 32.270
TS 32.271

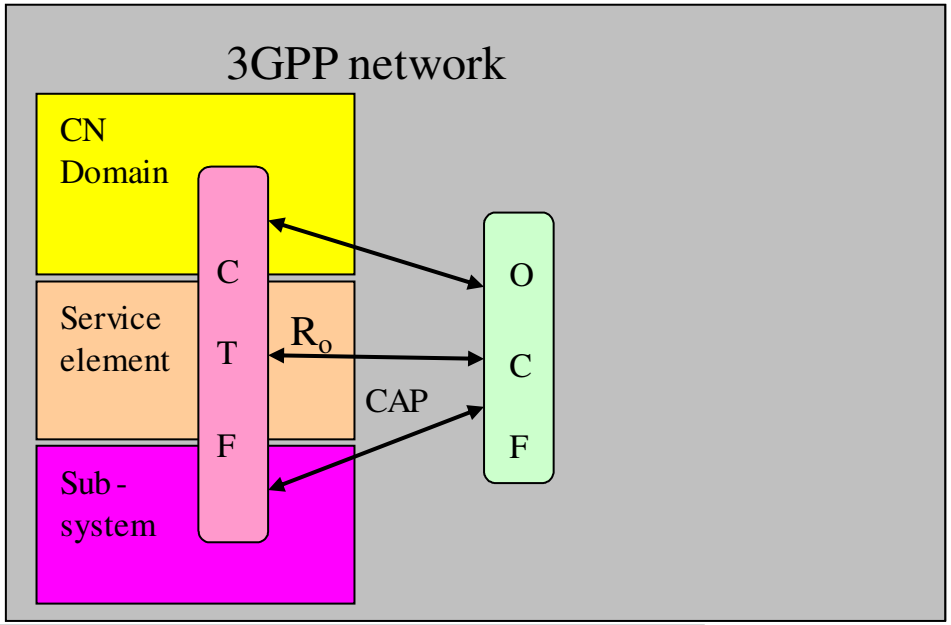
TASACIÓN EN IMS



CTF: Charging Trigger Function
CDF: Charging Data Function
CGF: Charging Gateway Function
OCF: On-Line Charging Function
BD: Billing Domain. Este puede ser un Sistema de Tasación / Sistema de Mediación de Tasación

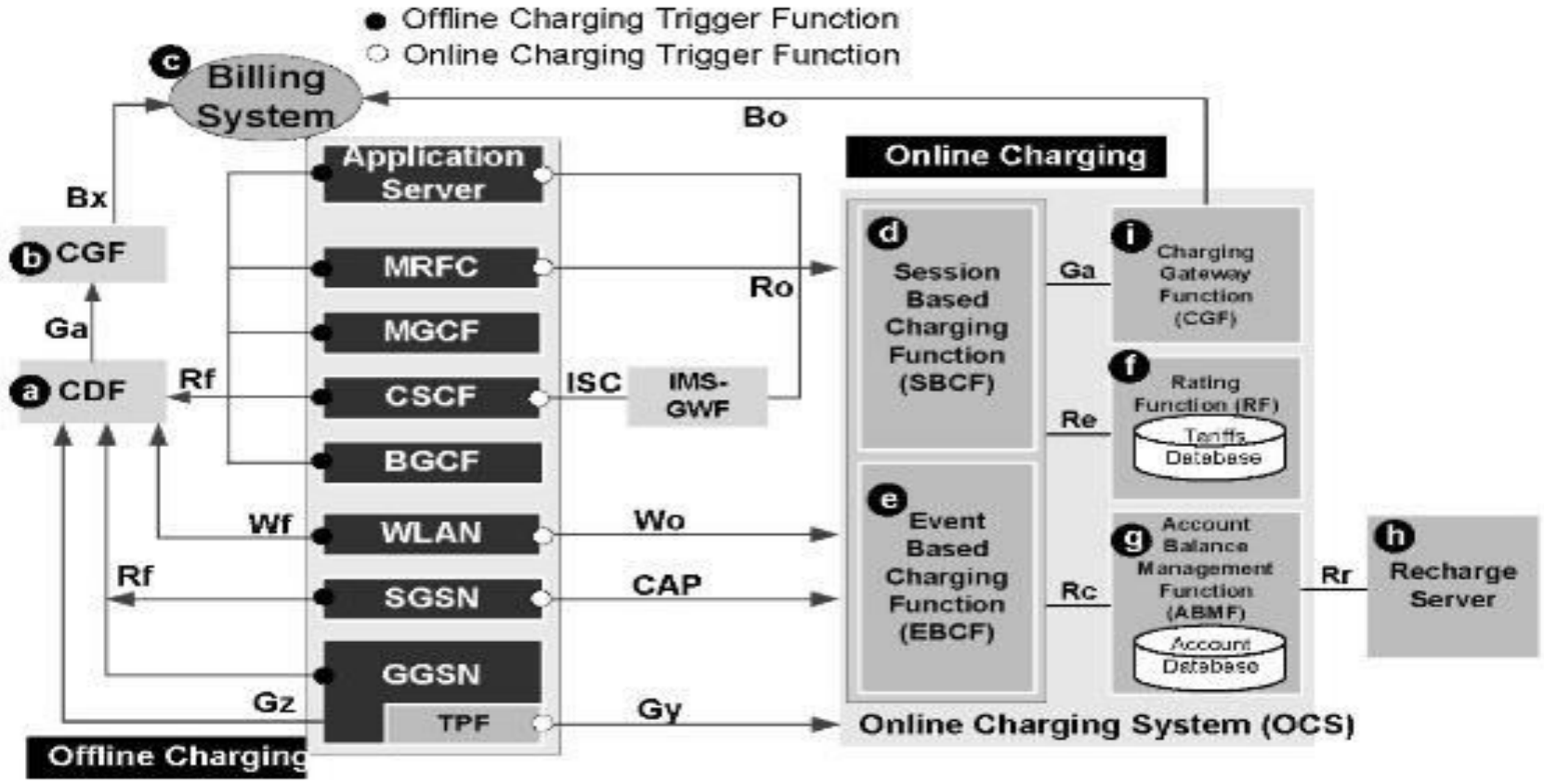
TASACIÓN OFF-LINE

La tasación por eventos permite un perfil de tasación mucho más variado.
El CTF puede formar parte de un dominio, de un servicio o de un sub-sistema (IMS)



TASACIÓN ON-LINE

TASACIÓN EN IMS



BGCF: Breakout Gateway Control Function
CDF: Charging Data Function
CSCF: Call Session Control Function
IMS-GWF: IMS Gateway Function
ISC: IMS Service Control
MRFC: Media Resource Function Controller
TPF: Traffic Plane Function

CAP: CAMEL Application Part
CGF: Charging Gateway Function
GSGN: Gateway GPRS Support Node
IMS: IP Multimedia Subsystem
MGCF: Media Gateway Control Function
SGSN: Serving GPRS Support Node

TASACIÓN EN IMS

OFFLINE CHARGING (Rf)

• En la tasación offline (Rf) se utilizan dos mensajes Diameter:

✓ACR - Solicitud de Contabilidad
✓ACA - Respuesta de Contabilidad

• Cada solicitud puede tener el siguiente Accounting-Record-Type:

✓START_RECORD: utilizado para iniciar una sesión de contabilidad, por lo general cuando la aplicación recibe un SIP 200 OK que reconoce un SIP INVITE inicial.
✓INTERIM_RECORD: utilizado para actualizar una sesión, por ejplo.: en el caso de SIP RE-INVITE y/o UPDATE en el diálogo SIP corriente.
✓STOP_RECORD: utilizado para detener una sesión de contabilidad, por ejplo.: cuando la aplicación recibe un mensaje SIP BYE
✓EVENT_RECORD: utilizado para la contabilidad basada en eventos, por ejplo.: un SMS o similar

TASACIÓN EN IMS

ONLINE CHARGING (Ro)

• En la tasación en línea (Ro), la función de contabilidad realiza el control de crédito antes de permitir el uso de recursos. El cliente prepago debe tener crédito en el OCS y todas sus actividades son supervisadas por ese Sistema.

• Hay dos casos posibles:
✓Débito directo: la cantidad se deduce inmediatamente del crédito del usuario en una sola transacción. Por ejplo.: un SMS o una película (Video-on-Demand).
✓Crédito de unidades: una cantidad se reserva en el OCS porque éste no sabe cuántas unidades se necesitan para prestar el servicio. Durante la sesión, la cantidad utilizada es deducida y más unidades pueden ser pedidas; al final las unidades usadas se reportan al usuario. Por ejplo.: sesiones debido a una llamada VoIP, Videollamada o una sesión de TV (Pay-per-View).

• Hay tres escenarios siguientes:
✓Contabilidad de Eventos Inmediata (IEC): utilizada para contabilidad sencilla basada en eventos
✓Contabilidad de Eventos con Reserva de Unidades (ECUR): del tipo de contabilidad basada en eventos
✓Contabilidad de Sesiones con Reserva de Unidades (SCUR): del tipo de contabilidad basada en sesiones

IMS EN HNB (HOME NODE B – FEMTOCELL 3G)

- Interconexión HNB con IMS, presenta tres alternativas:

✓ Puede tener acceso al CS
✓ Debe tener acceso al PS
✓ Se debe permitir interworking entre UE CS con IMS

- HNB enrutará Request tanto hacia CS como a IMS basado en políticas de Operadora.

- Interworking CS/IMS debe ser transparente para el UE.

- El UE se registra en el HNB y éste se registra en IMS.

- Se debe permitir Servicios CS tales como el FAX que son servicios sin equivalencia en IMS.

- Se debe permitir interworking entre HNB y macro celdas.

- Deberá ser posible constituir un HNB a partir de un NodeB 3G clásico (Interfaz Luh).

ASPECTOS IMS EN HNB (uso de IMS en escenarios pre LTE

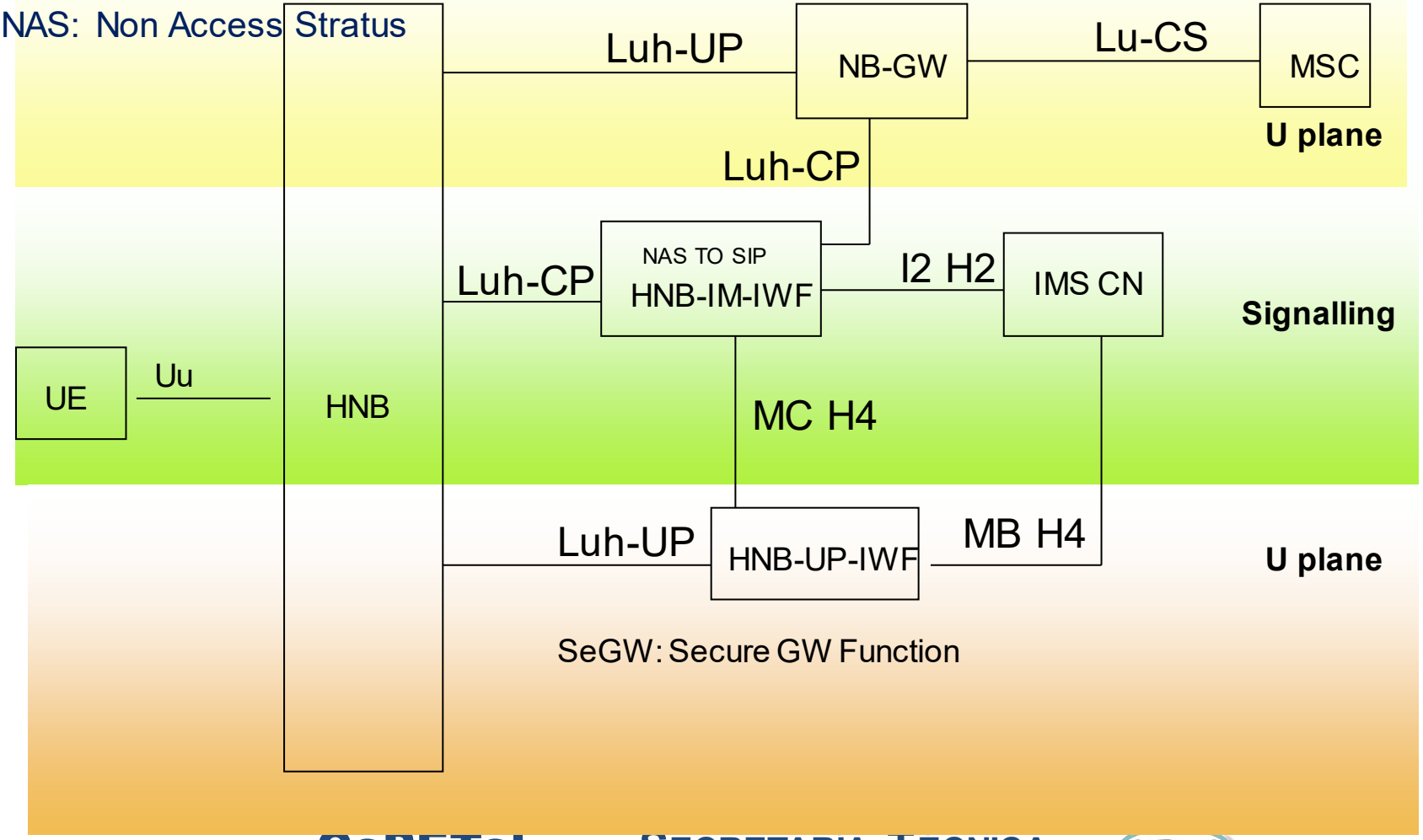
• Se provee interworking entre SIP/IMS y el protocolo de control del HNB. Esto significa que SIP no llega al UE, sino que finaliza en algún bloque de interworking.

• El HNB con esta capacidad debe vincular tanto a CS UE como a IMS UE, y dependiendo del caso utiliza una u otra interfaz para el UP (U Plane).

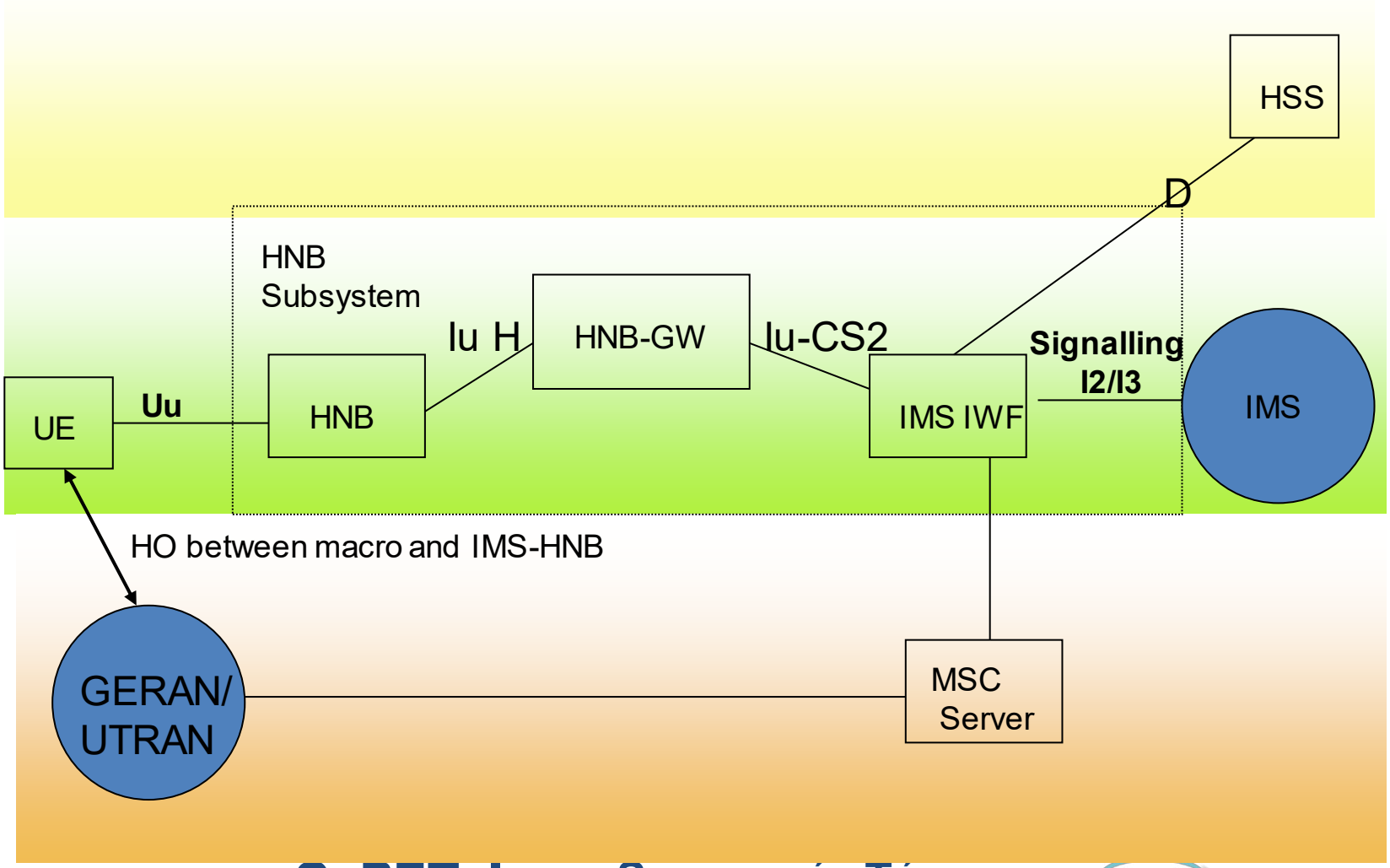
• Es decir que en el caso de HNB, al no tratarse de una arquitectura "All IP", existe una instancia en el HNB para determinar hacia donde encaminar la información (CS o IMS).

EL HNode B PROVEE SERVICIOS A LOS UE CS Y UE IMS

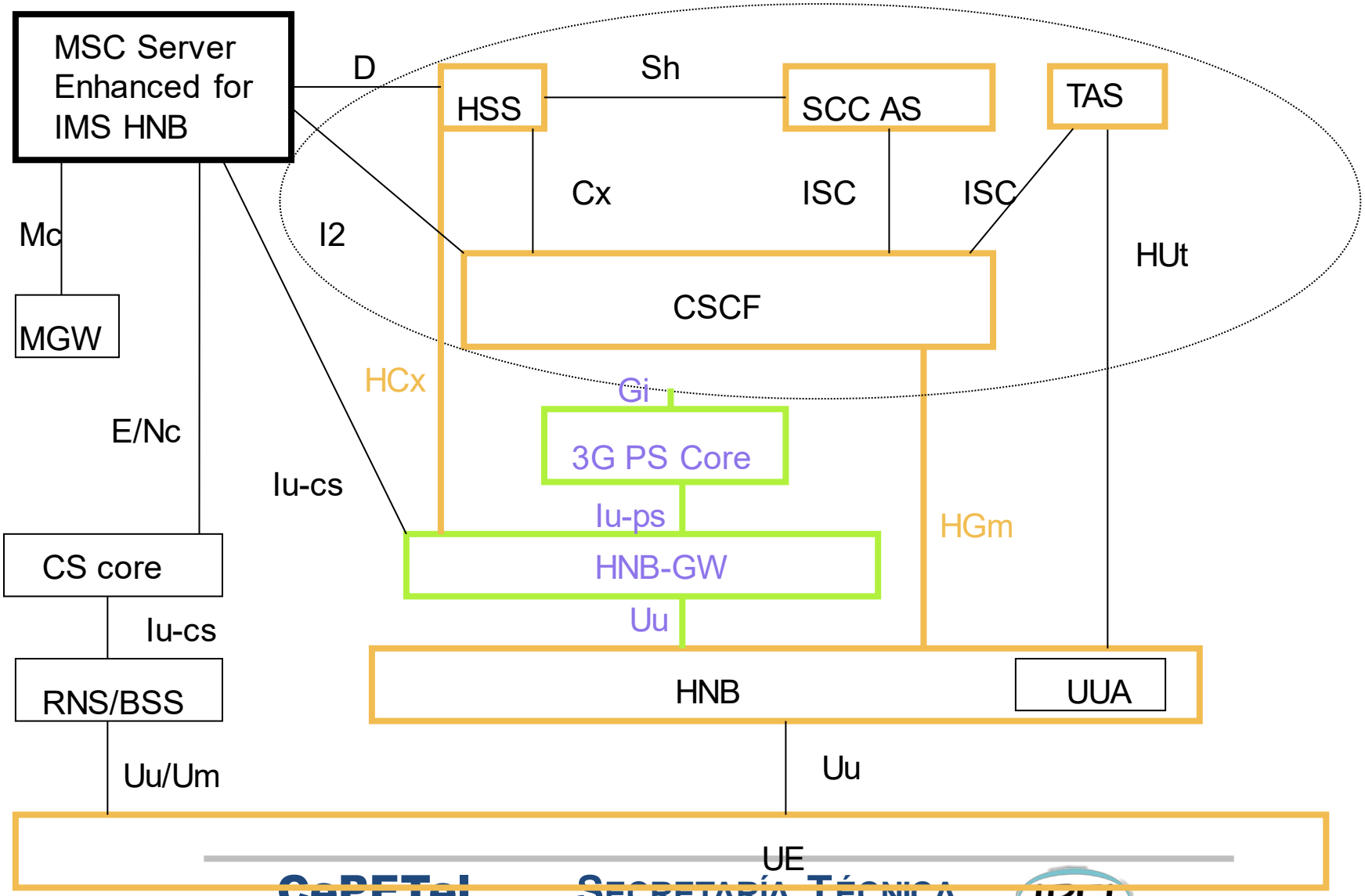
MME: Mobility Managment Entity
SAE PDN GW: Syst Archit Evolut Pack
Dat Netw GW
NAS: Non Access Stratus



EL SUBSISTEMA HNB OFRECE UNA INSTANCIA DE INTERWORKING CON IMS

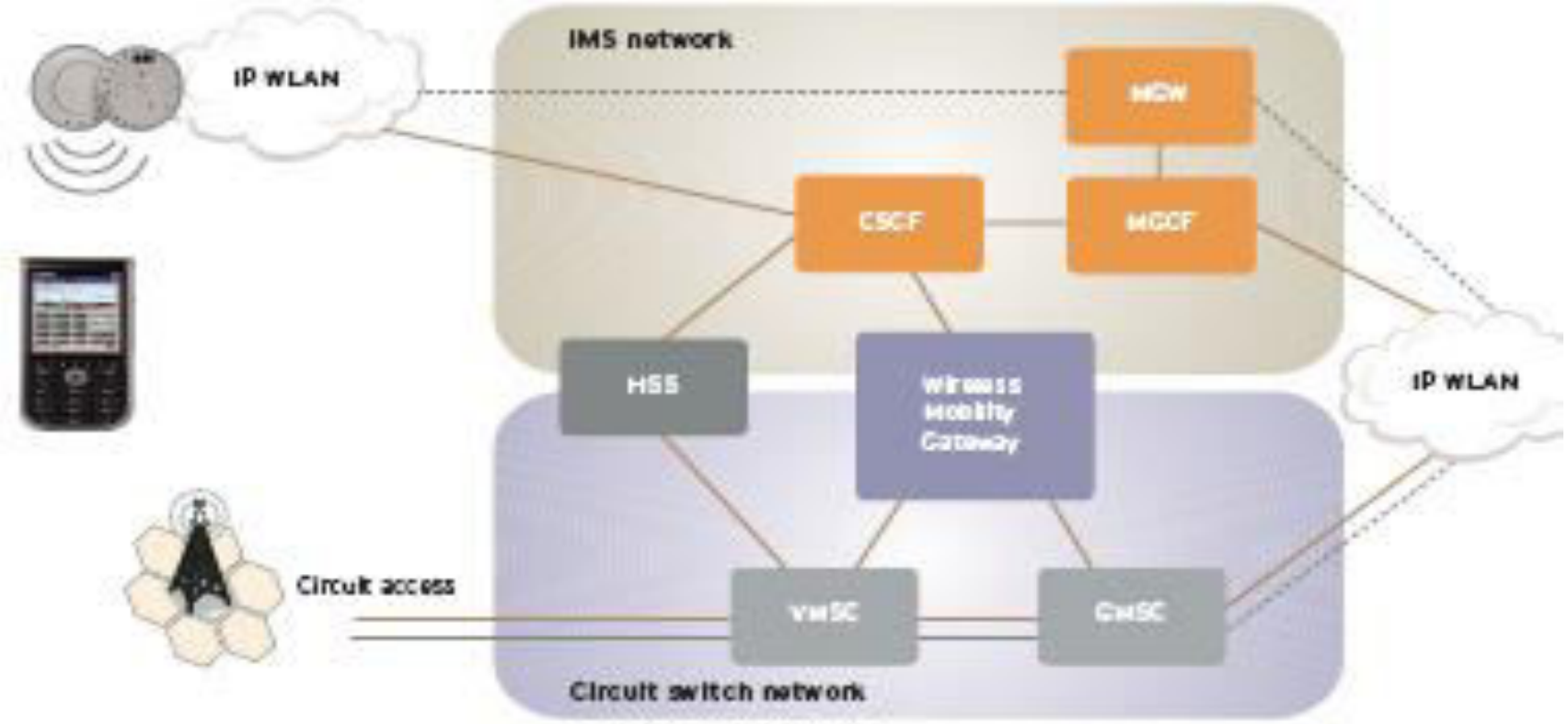


EL PROPIO HNB HACE DE INTERWORKING CON IMS

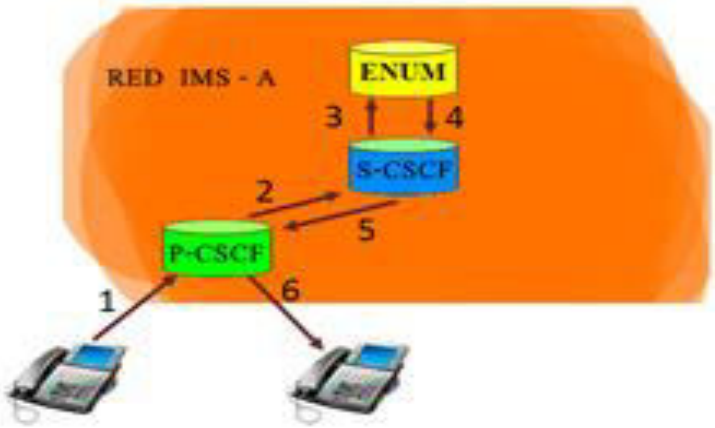


LA CONVERGENCIA DE RED, VCC (mecanismos antecesor de VoLTE y SRVCC

• **GMSC (Gateway MSC):** determina cual es la MSC que "visita" el usuario llamado. Todas las llamadas de Móvil a Móvil y PSTN a Móvil son enrutadas a través del GMSC.
• **VMSC (Visited MSC):** es la MSC donde el usuario esta actualmente ubicado. El VLR asociado a dicha MSC tendrá los datos del usuario en ella.



CONVERGENCIA DE NUMERACIÓN ENUM CON URI EN IMS



Si el destino no es encontrado en ENUM (no es este caso)
la llamada debe enrutarse a la PSTN/ PLMN (break out)

COMUNICACIÓN CON USUARIO DENTRO DE LA MISMA RED IMS

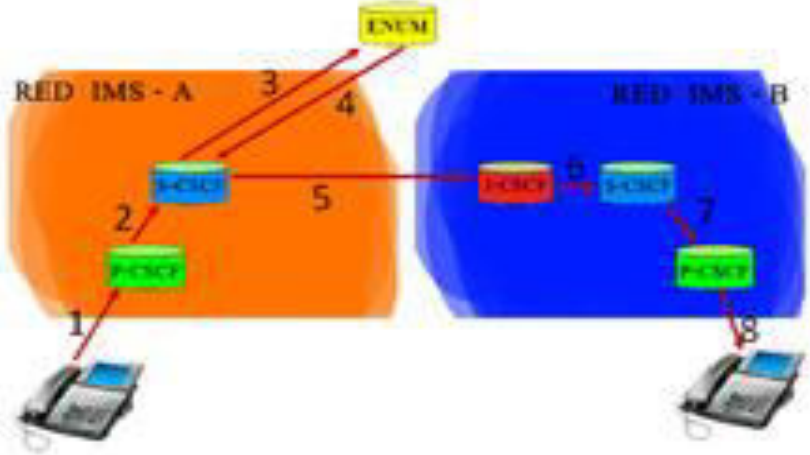
• El usuario A marca el número 123456 y lo transforma ese número a dominio DNS: "6.5.4.3.2.1.e163.arpa" y envía una petición (QUERY) al P-CSCF con dicho dominio para establecer la comunicación.

• El P-CSCF reenvía la petición hacia el S-CSCF que como se trata de una dirección de la que desconoce su URI, realiza una consulta al servidor ENUM/DNS.

• El ENUM recibe la petición del dominio, y consulta en su BdD de entradas NAPTR. Se encontrara una entrada asociada a dicho dominio que se envía al S-CSCF.

• El S-CSCF analiza la respuesta con el registro NAPTR recibido y en ella selecciona la entrada de mayor prioridad del servicio a establecer. En este caso, escogerá la única entrada NAPTR recibida. De ésta, obtiene la dirección URI del servicio del usuario destino. A partir de aquí se sigue como cualquier comunicación en una red IMS. Esta es recibida por el P-CSCF y reenviada al usuario.

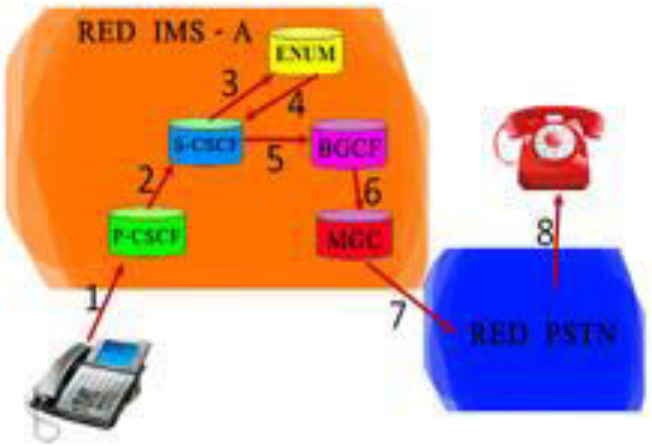
CONVERGENCIA DE NUMERACIÓN ENUM CON URI EN IMS



COMUNICACIÓN CON USUARIO FUERA DE LA RED IMS

- El usuario A marca el número 123456 y lo transforma al dominio DNS: "6.5.4.3.2.1.e163.arpa" enviando una petición al P-CSCF con dicho dominio para establecer la comunicación.
- El P-CSCF reenvía la petición al S-CSCF que como se trata de una dirección de la que desconoce su URI, realiza una consulta al servidor ENUM/DNS.
- El DNS/ENUM, que es privado pero tiene información de otras redes, consulta con el dominio su BdD de entradas NAPTR. Esta entrada es reenviada al S-CSCF que analiza la respuesta con el registro NAPTR recibido. En ella, selecciona la entrada de mayor prioridad del servicio a establecer. La URI obtenida, corresponde al dominio de la red B, por lo que la solicitud se envía al I-CSCF de la red B.
- El I-CSCF verifica que se trata de un usuario de su red y lo reenviará a su S-CSCF que la envía al P-CSCF. Por último, el P-CSCF reenvía la solicitud de conexión al usuario destino para comenzar la sesión.

CONVERGENCIA DE NUMERACIÓN ENUM CON URI EN IMS

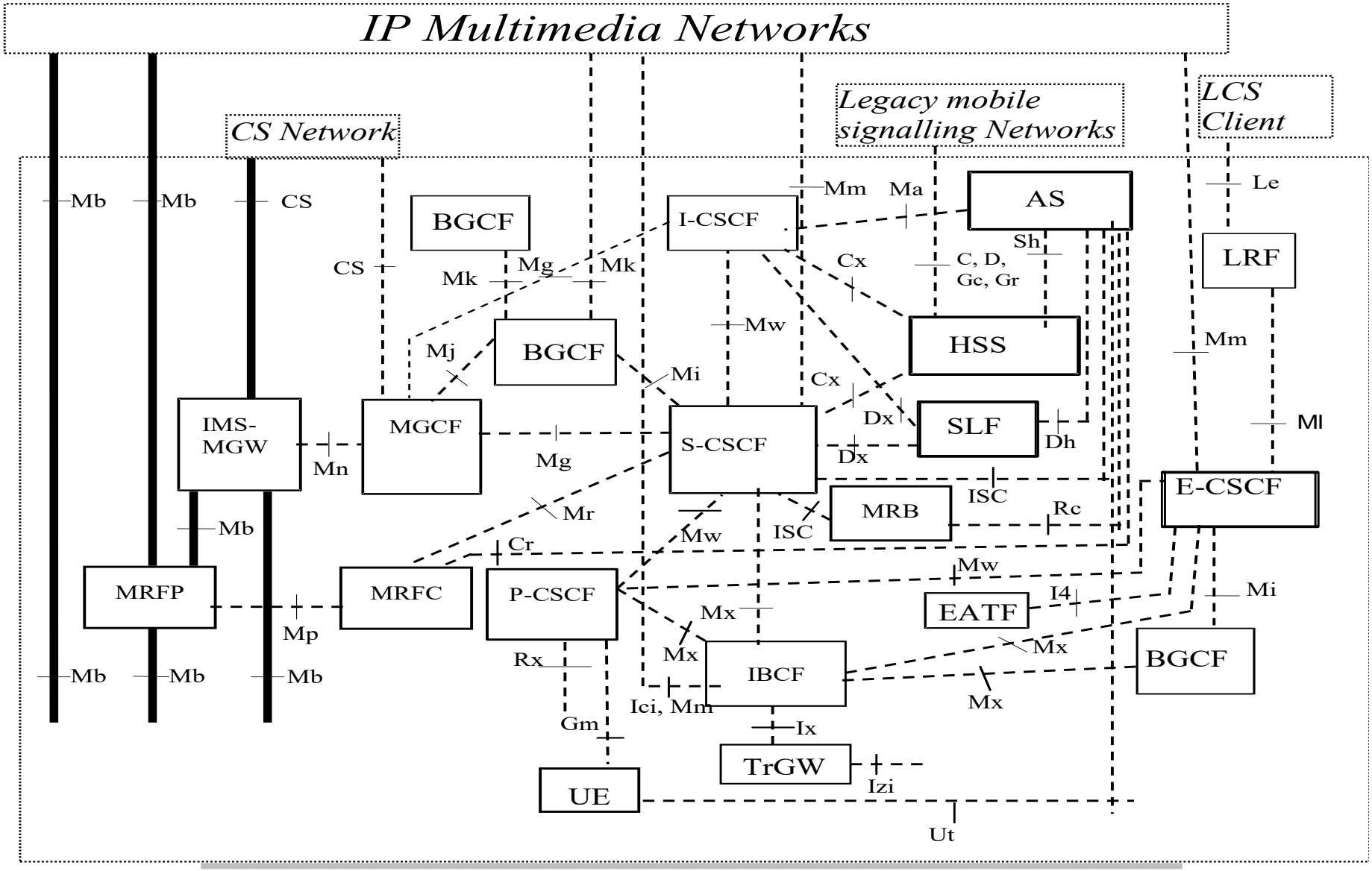


Escenario con enrutamiento a la PSTN/ PLMN (break out)

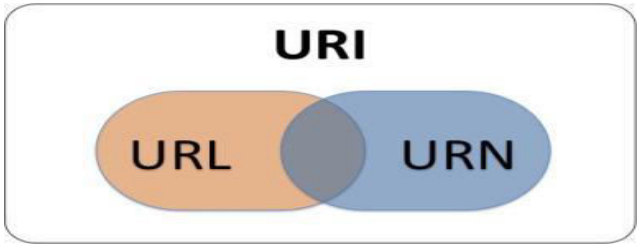
LLAMADA DESDE RED IMS A USUARIO EN PSTN

- El usuario A marca el número +54 1234567 y lo transforma al dominio DNS: "7.6.5.4.3.2.1.4.5.e163.arpa" enviando una petición al P-CSCF con dicho dominio, para establecer la comunicación.
- El P-CSCF reenvía la petición al S-CSCF que como se trata de una dirección de la que desconoce su URI, consulta al servidor ENUM/DNS.
- El ENUM consulta en su BdD de entradas NAPTR pero no hay ninguna entrada asociada a dicho número y envía el resultado de la consulta al S-CSCF.
- El S-CSCF verifica que el usuario no es alcanzable a través de la red IMS y reenvía la petición al BGCF que consulta su BdD para determinar que la llamada debe ser transmitida hacia la PSTN. Por ello, un petición Invite es reenviada al MGCF.
- El MGCF hace de interfaz entre ambas redes realizando la llamada PSTN.
- La llamada es encaminada dentro de la PSTN y llega al usuario destino.

INTERFACES DE LA ARQUITECTURA IMS DEDICADAS AL ACCESO LTE



URI y URL: CONCEPTOS



- **URI (Uniform Resource Identifier):** Identifica recursos en Internet
- **URL (Uniform Resource Localizater):** Localiza recursos en Internet
- **URN (Uniform Resource Name):** Identifica recursos en Internet con el nombre.

• IMS usa URI porque permite la interacción con los servicios ubicados en los AS.

• Un URI puede ser un URL o un URN o ambos (URL y URN). URN no se usa en la práctica.

• Ejplo: El nombre José García, sería un URL pero no dice nada de cómo localizarlo, es más, sirve para identificar a mucha más gente con el mismo nombre. En cambio su dirección física dice exactamente cómo localizarlo (URI) diferenciándolo de los otros José García.

• El formato estándar de URI es: **esquema://máquina/directorio/archivo#fragmento**
Ejplo, ***http://aprenderinternet.about.com/od/buscadores/ss/Como-Crear-Una-Cuenta-En-Google.htm#step2***: el esquema es *http*, la máquina es *aprenderinternet.about.com*, el directorio es /od/buscadores/ss/, el archivo es *Como-Crear-Una-Cuenta-En-Google.htm* y el fragmento es *step2*.

EXTENSIONES SIP

- Al SIP nativo (IETF) se le agregan extensiones o modificaciones (tb ocurre con H.248), a fin de resolver problemáticas adicionales
- Sigue siendo válida la RFC 3261 del SIP pero aparecen nuevas entidades detalladas en TS 24.229
- El UE actúa como UA con algunas excepciones SIP y SDP
- El P-CSCF actúa como Proxy con algunas excepciones SIP y SDP
- El I-CSCF actúa como Proxy
- El S-CSCF actúa como Proxy
- El MGCF actúa como UA
- El BGCF actúa como Proxy
- El AS actúa como UA en llamadas originadas y terminadas. Tb podrá actuar como una alternativa para Call Control.
- El MRCF actúa como AS
- El IBCF actúa como Proxy y eventualmente como UA si posee función de Gateway de Aplicación.
- El E-CSCF (Emergencia) actúa como Proxy.
- El P-CSCF, I-CSCF, S-CSCF, IBCF, BGCF y el E-CSCF, tb podrán actuar como UA.

EXTENSIONES SIP

- ✓ *P-Asserted-Identity*
- ✓ *P-Access-Network-Info*
- ✓ *History-Info*
- ✓ *P-Asserted-Service*
- ✓ *Resource-Priority*
- ✓ *P-Charching-Vector*

IM C-N Subsystem Charging Identifier (ICID):

• Se trata de información intercambiada por las distintas entidades de IM CN a nivel de sesión. Esta información se usa para mensajes no relacionados a una sesión (por ejplo.: SUBSCRIBE/NOTIFY y tb para la correlación con CDR's).

• La primer entidad involucrada en una transacción SIP generará un ICID (incluido en el P-Charching-Vector).

• En el caso particular de la interfaz Mg, el MGCF generará el ICID para llamadas originadas en la PSTN/PLMN.

• El ICID nunca es pasado al UE.

EXTENSIONES SIP

Información de Tasación de Red de Acceso:

✓Esta información relacionada con la media se usa para correlacionar IP-CAN (IP Conectivity Access Network) CDRs' con IM CN CDR's (correlación de información de media con señalización).

✓Esta información es pasada desde IP-CAN hacia el P-CSCF sobre las interfaces Rx y Gx.

Inter Operator Identifier (IOI):

✓Se utiliza en presencia de más de un Operador.

✓El parámetro IOI se inserta en el header del P-Charging-Vector y se utiliza la modalidad orig-ioi.

✓La red de origen inserta el parámetro orig-ioi (P-Ch-V) en el request dejando el term-ioi vacante. La red destino popula el dest-ioi en la respuesta, dejando vacante el orig-ioi.

✓Dependiendo de las entidades participantes, surgen tres tipos de parámetros: utilizándose el tipo 2 en la interfaz "Mg" entre el MGCF y el S-CSCF.

Direcciones de la Función de Tasación:

✓En el P-Charching-Function-Adresses se incluyen los parámetros CDF (Charching Data Function) o el OCF (On line Charching Function).

EXTENSIONES SIP

P-Access-Network-Info Header:

✓Este es un header importante y de contenido variable dependiendo del tipo de acceso que se utilice. En un ambiente de FMC es muy útil para el P-CSCF que todos los UE incluyan este header.

✓Algunos posibles valores son: ADSL, IEEE 802.11a/b/g (wifi), 3 GPP-GERAN.

P-Charging-Vector Header:

✓Este header y su sintaxis se define en la RFC 3455.

✓3GPP define una serie de extensiones para incluir información de correlación que se intercambian las distintas entidades de IM CN.

✓Entre estas extensiones se encuentra el "Access-Network-Charging-Info" que complementa el "P-Access-Network-Info Header", el cual es un parámetro genérico que contiene a otros más específicos como "BRAS Parameter", "Auth-Token-Parameter" y un set de parámetros de información sobre portadoras "DSL-Bearer-Info" aplicables a los accesos del tipo xDSL.

✓Otros no son de aplicación para la red fija como ser el "GPRS-Charging-Info Parameter" (GPRS como IP-CAN).

INTERFACES DE LA ARQUITECTURA IMS DEDICADAS AL ACCESO LTE

• En un acceso LTE, la interfaz “Gm” de acceso al Core IMS debe ser entendida como una interfaz SIP (nivel de aplicación) que se monta sobre la interfaz “SGi” de salida del EPC.