NGN/IMS a fons

PID_00265728

Víctor Huertas García

Temps mínim de dedicació recomanat: 7 hores

Universitat Oberta de Catalunya

Víctor Huertas García

Enginyer de Telecomunicacions per la Universitat Politècnica de Catalunya. Actualment treballa com a enginyer de *networking*. És expert en NGN/IMS al Departament d'Equips de Comunicació de la multinacional Indra Sistemas. Ha participat en nombrosos projectes de recerca de l'ESA (Agència Espacial Europea) sobre l'aplicació de la tecnologia IP en xarxes de satèl·lit. Recentment, ha participat en projectes d'integració d'IMS a les xarxes de satèl·lit per a aconseguir la convergència amb xarxes terrestres.

L'encàrrec i la creació d'aquest recurs d'aprenentatge UOC han estat coordinats pel professor: Victor Garcia Font

Segona edició: setembre 2019
Autoria: Víctor Huertas García

Av. Tibidabo, 39-43, 08035 Barcelona
Realització editorial: FUOC

Índex

Introducció

El paradigma introduït per les xarxes NGN fa possible que qualsevol xarxa que pugui transmetre paquets IP es converteixi en una xarxa multiservei amb garantia de qualitat de servei. Es produeix un total desacoblament entre els serveis oferts als usuaris i la tecnologia de les xarxes de transport.

Si hi ha hagut una entitat d'estandardització i especificació que ha portat la veu cantant en l'especificació de NGN i IMS, aquesta és 3GPP, que s'ha focalitzat sobretot les xarxes que més diners mouen en el mercat de les telecomunicacions avui dia: les xarxes de telefonia mòbil. Aquest mòdul es focalitzarà en el model de referència que aquesta entitat proposa tant per a la **capa de transport** (LTE) com per a la **capa de servei** (nucli IMS).

Finalment, abordarem la **capa que afecta les aplicacions**, que és en realitat allò que aporta valor afegit als serveis als quals els usuaris accedeixen des dels seus terminals. Com veurem, en aquesta àrea hi ha més laxitud quant a l'especificació, ja que les seves característiques s'han indicat a un nivell més alt. La indústria mateixa és la que ha emplenat els buits deixats per l'especificació proposant les seves pròpies solucions.

En resum, en aquest mòdul es veuran amb més detalls totes les capes del model de referència proposant exemples de com avui dia s'han implementat (per exemple, en les xarxes LTE) i com la seva arquitectura ha anat evolucionant segons els requeriments que el mateix mercat ha imposat (per exemple, la irrupció de Wi-Fi com a tecnologia d'accés gairebé a escala global).

Objectius

Els continguts d'aquest mòdul han de permetre als estudiants els objectius següents:

1. Conèixer els blocs funcionals que defineixen els models de referència de 3GPP i que afecten les següents capes:

a) Capa de transport de LTE: *Evolved Packet System* i model de referència PCC per a garantia de QoS.
b) Capa de servei: nucli IMS compost primordialment per P-CSCF, I-CSCF i S-CSCF.
c) Capa d'aplicació: integració del nucli IMS amb servidors d'aplicació de xarxes heretades i SIP.

2. Identificar els punts de referència (o interfícies) entre blocs de la capa de transport i de servei (nucli IMS).

3. Identificar i conèixer els punts de referència (o interfícies) entre el nucli IMS i la capa de transport i la seva importància en la garantia de QoS d'extrem a extrem tant en mode *push* com en mode *pull*.

4. Conèixer els principals protocols emprats en un context NGN/IMS per a l'establiment de sessions multimèdia i el control d'admissió i recursos: SIP i Diameter.

5. Comprendre la filosofia d'un servei NGN i el seu paral·lelisme amb el paradigma SOA.

6. Conèixer la interacció en l'àmbit d'interfícies i funcionalitats genèriques en la invocació de serveis en un context d'IMS per als actors següents segons el model de 3GPP:

a) L'usuari i la seva interacció directa amb el nucli IMS i amb el servidor d'aplicació.
b) El nucli IMS amb el servidor d'aplicació.

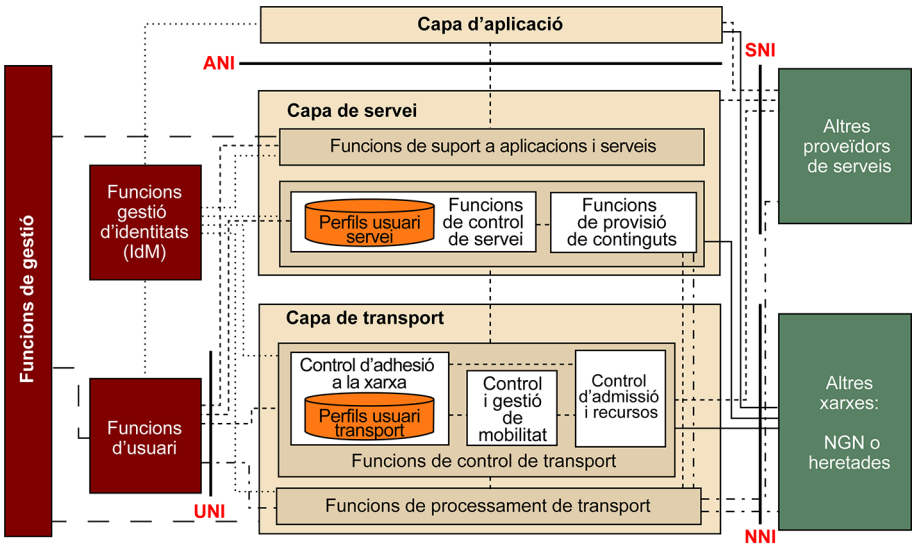
7. Entendre la importància de l'orquestració en la integració de serveis.

8. Comprendre les funcionalitats del *service broker* i la seva arquitectura interna.

1. Arquitectura funcional de NGN/IMS

Les xarxes de propera generació o xarxes NGN es caracteritzen per estar basades íntegrament en paquets IP i per l'accés lliure a serveis multimèdia amb garantia de qualitat de servei (QoS) d'extrem a extrem amb independència de la tecnologia de la xarxa de transport (tant en la xarxa d'accés com en la troncal).

Figura 1. Arquitectura de referència segons la versió 2 de xarxes NGN de l'ITU-T.



La Figura 1 es correspon amb la versió 2 de l'arquitectura, en la qual s'han introduït alguns blocs nous respecte a la versió 1, enfocats bàsicament a serveis com IPTV, gestió d'identitats i mobilitat en la capa de transport.

Malgrat que l'ITU-T ha tingut un paper harmonitzador de totes les especificacions pel que fa a les NGN que han anat sorgint al llarg dels anys, al final la indústria de la telefonia mòbil és la que ha portat la iniciativa en l'evolució futura d'aquestes especificacions. I si hi ha una entitat que ha contribuït i contribueix a definir les xarxes de telefonia mòbil, aquesta és sens dubte 3GPP. I aquesta és l'especificació en la qual ens basarem en les properes seccions.

Així, doncs, a continuació veurem cadascuna de les parts i capes que conformen l'arquitectura 3GPP de referència per a les xarxes LTE, començant per la capa de transport i les seves funcions, pujant a la capa de servei i finalment fins a la capa d'aplicació.

Abans d'abordar la descripció de totes les capes i subcapes de cada model, definirem dos conceptes que us trobareu al llarg de tot el document.

Entitat funcional

L'entitat funcional és el concepte lògic que especifica una sèrie de funcions úniques que no són portades a terme per altres entitats funcionals. Les entitats funcionals es poden agrupar per a descriure'n implementacions físiques i pràctiques.

Les entitats funcionals que defineixen l'arquitectura genèrica de xarxes NGN són entitats abstractes que es defineixen de manera més concisa quan són instanciades en un context concret tecnològicament parlant. És a dir, es podria donar el cas que una instància d'una entitat funcional tingués un comportament lleugerament diferent depenent d'aquest context.

Això condiciona totalment la implementació de la interfície (també anomenada punt de referència) entre dues entitats funcionals i, per tant, la descripció d'aquesta només té sentit quan coneixem les instàncies particulars que s'usen en un context.

Punt de referència

El punt de referència és un punt d'unió entre dues entitats funcionals ben diferenciades. Es pot usar per a identificar el tipus d'informació que s'intercanvia entre aquestes entitats funcionals. En l'àmbit de la implementació física, un punt de referència es pot correspondre amb una o més interfícies físiques entre dos equips i es pot implementar amb protocols que s'adaptin a l'intercanvi d'aquesta informació, com és el cas de Diameter.

2. Capa de transport

3GPP és l'entitat que ha especificat les tecnologies més importants en el món de la telefonia mòbil des de GPRS fins a 5G passant per UMTS i LTE. A continuació descriurem l'especificació de 3GPP pel que fa a la capa de transport.

Podem distingir dues arquitectures de referència, una de les quals en realitat està continguda dins de l'altra:

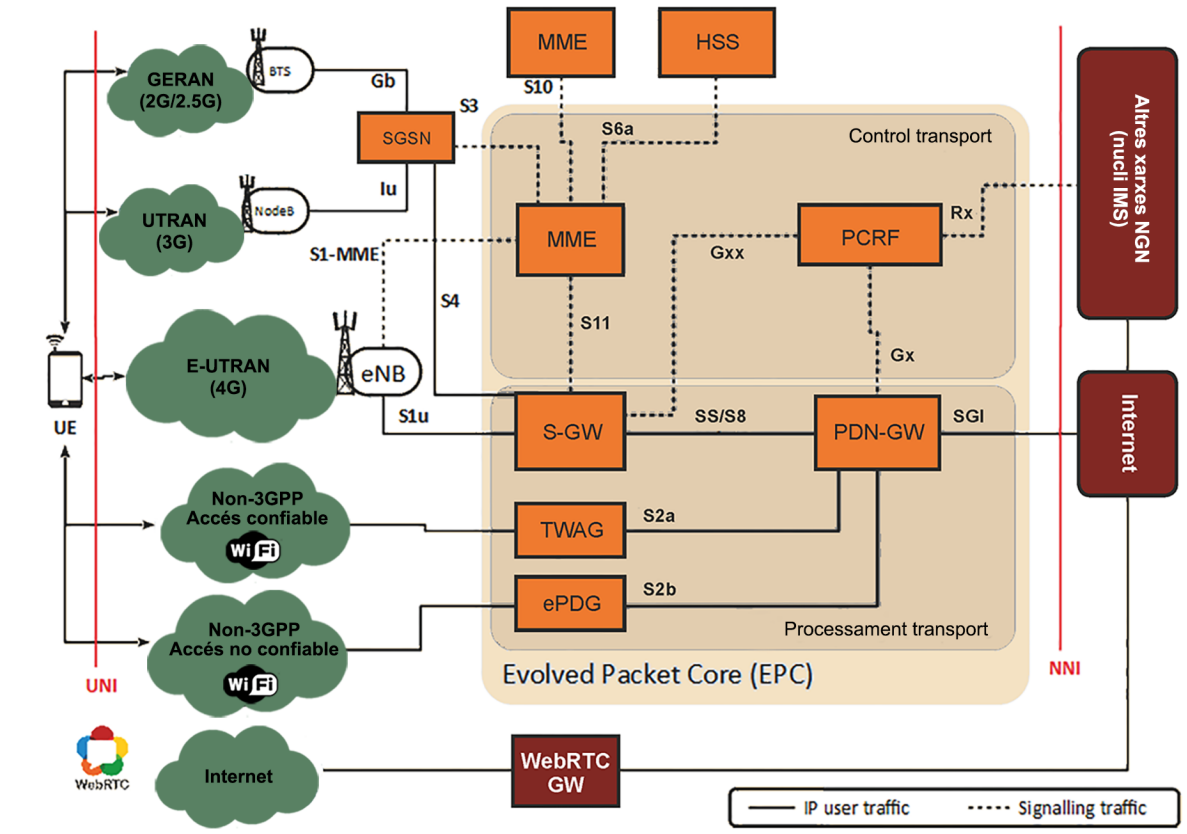
- **EPS (*Evolved Packet System)*.** Inclou totes les entitats funcionals que defineixen tant la xarxa d'accés ràdio LTE com la xarxa troncal. Aquestes entitats ofereixen les funcionalitats de control de recursos ràdio, l'autenticació d'equips d'usuari i l'establiment de connectivitat IP dins de la xarxa de l'operador.
- **PCC (*Policy and Charging Control*).** És un subconjunt de l'EPS que té la funció d'aplicar polítiques de QoS i controls de facturació d'ús de serveis per part dels usuaris.

2.1. *Evolved Packet System*

En la Figura 2 es pot apreciar l'arquitectura funcional de les xarxes d'accés i troncal de LTE que 3GPP proposa, la qual és anomenada *Evolved Packet System*.

L' ***Evolved Packet System*** és la suma de dos subconjunts: **E-UTRAN** (*Evolved UMTS Terrestrial Radio Access Network*) en la part de xarxa d'accés ràdio i **EPC** (*Evolved Packet Core*) en la part de la xarxa troncal.

Figura 2. Arquitectura de referència de l'*Evolved Packet System*.



En la Figura 2 també podem veure que s'integren amb l'EPS altres xarxes definides per 3GPP, com les xarxes d'accés 2G i 3G, i xarxes anomenades de *mobile offload*, que són primordialment xarxes Wi-Fi o femtocel·les en interiors d'edificis.

Mobile offload

Les xarxes Wi-Fi, com que estan integrades en l'EPC, actuen com si fossin una extensió de la cobertura a l'interior d'edificis o fins i tot a manera d'itinerància a l'estranger.

Totes aquestes xarxes sense fil tan diverses s'han d'integrar en una xarxa troncal de LTE perquè l'equip d'usuari (UE) també les té integrades, i es poden usar en tot moment segons la seva ubicació i el nivell de cobertura que tingui de cadascuna. Conseqüentment, a vegades s'haurà de fer una transferència transparent (sense talls en la sessió de servei) d'una xarxa a una altra i hi haurà d'haver una certa coordinació de traspàs de sessió entre aquestes xarxes d'accés, i aquí l'EPC té un paper molt important.

Així, doncs, primer veurem els elements principals que formen l'arquitectura EPS i posteriorment, en la secció 2.2, el model de referència PCC (*Policy and Charging Control*).

Introducció a l' *Evolved Packet System*

La Figura 2 mostra l'arquitectura de l'EPS o SAE (*System Architecture Evolution*), les entitats funcionals del qual veurem a continuació.

Comencem amb l'**equip d'usuari** (UE). L'equip d'usuari en una xarxa de comunicacions mòbils LTE equival a un terminal únic portàtil que, com hem esmentat, és compatible amb moltes generacions de xarxes de telefonia mòbil i Wi-Fi.

A continuació hi ha la xarxa d'accés ràdio de LTE, que es diu **E-UTRAN**. Aquesta xarxa d'accés ràdio (basat en OFDMA) acaba en l'eNodeB (*Evolved Node B*), que, perquè ens entenguem, és l'estació base de LTE. Aquest element estableix una sèrie de canals virtuals ràdio amb cada equip d'usuari i aquests canals tenen particularitats que afecten la garantia de QoS. Els paquets IP es mapegen en aquests canals virtuals, anomenats en anglès *radio bearers*.

OFDMA

OFDMA és un mètode d'accés que permet assignar un nombre diferent de subportadores a cadascun dels usuaris i garanteix així una qualitat de servei (QoS) diferent en funció de l'amplada de banda assignada.

L'element següent, ja dins de l'EPC, és l'**SGW** (*service gateway*) i està relacionat exclusivament amb el mecanisme de mobilitat. Si un equip d'usuari es desplaça d'una cel·la a una altra (dins de LTE), l'eNodeB associat canvia, però no l'SGW, el qual és considerat com una passarel·la d'ancoratge en el servei de mobilitat.

Interfície S4

La interfície entre l'SGSN i l'SGW es denomina interfície S4. Proporciona suport de pla d'usuari per a servei de mobilitat entre el nucli GPRS i l'SGW. També habilita l'SGW per a ancorar el traspàs intra-3GPP (TS 23.401).

Si, per exemple, l'usuari es desplaça a una zona on hi ha exclusivament cobertura de 2G, l'SGW es coordinarà amb el (*Service GPRS Support Node*), pel qual farà arribar el trànsit d'usuari (via la interfície S4).

SGSN

L'SGSN és un node que encamina sessions de dades, com connectivitat a internet via GPRS. Aquestes sessions o trucades de dades són referides generalment com d'àmbit *packet switched* o de commutació de paquets, ja que transporten paquets IP.

En aquest servei de mobilitat cal destacar un altre element molt important: l'**MME (Mobility Management Entity)**. Aquest element no processa paquets d'usuari, sinó que fa tasques de control de mobilitat dins de les xarxes 3GPP, incloses xarxes d'accés d'altres generacions com UTRAN (3G) o GERAN (2G). Per a això, es coordina amb l'SGSN via una interfície de control anomenada S3. Un MME també pot coordinar-se amb altres MME que controlen altres clústers d'eNodeBs adjacents i facilitar així la transferència dins de la xarxa d'accés ràdio LTE. Per a això, s'usa la interfície de control S10.

L'MME fa altres funcions. Per exemple, assigna a l'UE l'SGW en el qual ancorar-se en el moment en què aquest s'adhereix a la xarxa d'accés ràdio (en encendre's).

Interfície S3

La connexió SGSN/MME és proporcionada per la interfície S3. Permet intercanviar informació per a la mobilitat entre les xarxes d'accés 3GPP (TS 23.401).

L'MME també aglutina informació actualitzada de localització de cada equip d'usuari, com a quin eNodeB està associat. Això és important quan es produeix una trucada entrant cap a un usuari i cal localitzar-lo en l'àmbit de cel·la (el servei de localització s'anomena *paging*). L'MME també fa tasques d'autenticació

de l'equip d'usuari en el moment en què es produeix l'adhesió a la xarxa. Per això l'MME té un punt de referència dedicat (S6a) d'interconnexió a l'HSS (*Home Subscriber Server*), on s'emmagatzema la informació de credencials de l'usuari i perfil de subscripció en l'àmbit de transport (l'HSS també emmagatzema informació de perfil en l'àmbit de control de servei). La descripció detallada d'aquest servei es farà en la secció 3, on es descriu el nucli IMS).

Les xarxes 3GPP

Les xarxes 3GPP no solament es consideren les cel·les d'un sistema LTE, sinó que també inclouen xarxes GPRS i UMTS, les tasques de mobilitat de les quals també les assumeix l'MME mitjançant punts de referència dedicats que l'uneixen amb els nodes d'aquestes xarxes d'accés ràdio (GERAN per a GPRS i UTRAN per a UMTS).

Finalment, l'MME també participa en tasques de gestió de *radio bearers* (com en l'activació i desactivació d'aquestes).

L'últim l'element de l'EPC és el **PDN GW**.

Interfície S6a

La interfície entre MME i HSS és l'S6a. S'utilitza per a transferir informació de subscripció, autenticació i autorització d'usuaris (TS 23.401).

El **PDN GW (*Packet Data Network Gateway*)** és l'element fronterer del sistema EPS amb altres xarxes externes com internet o IMS. De fet, la configuració típica en un EPC és tenir un PDN GW per cada APN (*access point name*), i normalment hi ha un APN per a la interconnexió a internet i un altre per a la interconnexió amb el nucli IMS (dos PDN GW en total).

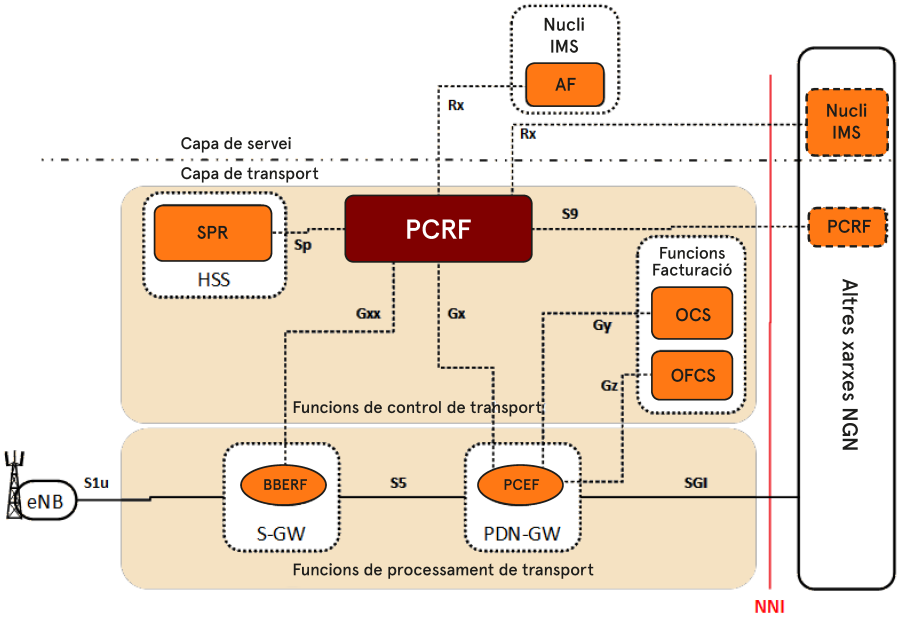
Aquest element té un paper molt important en la garantia de QoS, tal com veurem, i també s'encarrega d'assignar les adreces IP als equips d'usuari.

S'assigna una IP per PDN GW, així que si un usuari és subscriptor d'un servei de dades (internet) i també de serveis d'IMS (VoLTE), com que està connectat a dos PDN GWs diferents alhora, tindrà assignades dues adreces IP: una la usarà per al servei d'internet i l'altra per a serveis multimèdia IMS (senyalització IMS i trànsit de veu o vídeo).

2.2. QoS en LTE: el model de referència de PCC

Ara que hem vist l'estructura bàsica del sistema EPS que 3GPP defineix per a LTE, definirem diversos conceptes clau per a entendre com es gestiona la QoS en l'arquitectura de referència de PCC (vegeu la Figura 3).

Figura 3. Arquitectura de referència del PCC.



El PCC treballa en l'àmbit de fluxos de dades de serveis o SDF (*service data flows*) i proporciona funcions per al control de polítiques i de facturació (càrrecs monetaris associats), i també reporta esdeveniments pe als SDF.

La funcionalitat del PCC es resumeix en dos punts principals:

1) Control de facturació sobre la base de fluxos, que inclou el control de càrrecs monetaris associats i el control de crèdit en línia.

2) Control de polítiques, que inclou principalment el control d'accés a la xarxa i el control de la QoS dels serveis invocats (per exemple, connectivitat a internet i VoLTE, entre d'altres).

Cada SDF és associat a una **regla de PCC** i pot estar subjecte a control de polítiques, a control de facturació o tots dos alhora.

Una **regla PCC** és definida pel PCRF després de prendre la decisió de control d'admissió de la sol·licitud de recursos de servei rebuda tant des de la interfície Rx (anomenada mode *push* quan es rep des de l'AF o *application function*) com des de la interfície Gx (anomenada mode *pull* quan es rep des de la PDN-GW). Aquesta **regla PCC** està composta pels paràmetres següents:

- **Nom de regla** (identificador únic).
- **Identificador de servei o SDF.** És un valor sencer que identifica un servei o component de servei.
- **Filtres IP associats als SDF.** Cada filtre fixa paràmetres de la capçalera del paquet TCP/IP per mapar el trànsit real a un SDF.
- **Precedència.** És l'ordre d'aplicació del filtre o filtres.
- **Estatus d'accés.** És obert o tancat, deixa passar o no el trànsit associat.
- **Paràmetres QoS.** Conté QCI, ARP i velocitat de bit per a pujada i baixada.
- **Clau de facturació** (en anglès, *rating group*) i **altres paràmetres de facturació**. Són usats per a facturació en línia i fora de línia.
- **Clau de monitoratge**

Interfície Rx

La interfície entre PCRF i AF (*application function*) és l'Rx. És utilitzada per l'AF per a sol·licitar recursos de QoS i reportar esdeveniments de capa de transport. 3GPP recomana el protocol Diameter per a implementar-la (TS 29.214).

Interfície Gx

La interfície entre PCRF i PCEF és el Gx. És utilitzada pel PCRF per a instal·lar les regles PCC (establiment d'IP-CAN *bearer* i assignació de fluxos de dades de servei). També és usada per a reportar esdeveniments de capa de transport. 3GPP recomana el protocol Diameter per a implementar-la (TS 29.212).

IP-CAN

Aquesta sigla correspon a *IP-Connectivity Access Network*.

El PCC associa la informació de servei i la de transport de tal manera que la facturació i les polítiques queden lligades totalment amb vista a integrar xarxes de transport heterogènies. De fet, relaciona una sessió en l'àmbit de servei (associada a la interfície Rx) amb una sessió IP-CAN en l'àmbit de transport (associada a la interfície Gx/Gxx).

3GPP defineix una **sessió IP-CAN** (també anomenada **sessió EPS** si la xarxa d'accés és LTE) com l'associació entre l'equip d'usuari (UE) i una xarxa d'accés IP qualsevol. Una sessió IP-CAN pot incorporar una agrupació d'un o més túnels IP-CAN, anomenats també IP-CAN *bearers* (EPS *bearers* si la xarxa és LTE). Una sessió IP-CAN és present sempre que hi hagi una adreça IP assignada a l'UE i notificada a la xarxa d'accés IP. Així que si un UE és associat a dues APN en una xarxa LTE, tindrà dues adreces IP assignades i, per tant, tindrà dues sessions EPS actives simultàniament amb els respectius túnels establerts.

Interfície Gxx

La interfície entre PCRF i BBERF és el Gxx. És utilitzada pel PCRF per a instal·lar les regles PCC (establiment d'IP-CAN *bearer* i assignació de fluxos de dades de servei). També és usada per a reportar esdeveniments de capa de transport. 3GPP recomana el protocol Diameter per a implementar-la (TS 29.212).

A continuació descriurem les entitats funcionals que conformen el model arquitectural PCC, i ho farem abordant primer la subcapa de processament de transport i finalment la subcapa de control de transport.

1) Subcapa de processament de transport

La Figura 3 mostra dos elements que conformen les entitats funcionals en la part de la subcapa de processament de transport de la xarxa d'accés, el PCEF i el BBERF, les quals definirem a continuació.

a) Funció d'aplicació de polítiques i càrrecs associats (PCEF). Aquesta entitat funcional, que es tradueix en anglès com *policy and charging enforcement function,* és localitzada en el PDN GW i s'encarrega d'aplicar les polítiques de QoS que defineixen les regles PCC que un o més PCRF li indiquin mitjançant el punt de referència Gx. Això significa que aquesta entitat funcional classifica els fluxos IP i aplica les polítiques de QoS associades en cada SDF activada (definides en cada regla PCC) per a cada usuari tant en pujada (*uplink* o sentit UE-PDN) com en baixada (*downlink* o sentit PDN-UE). La PCEF implementa els túnels EPS en un dels seus mapant en baixada (*downlink*) tots els fluxos de cada SDF en el túnel que garanteixi millor la QoS en el camí que recorren fins a l'UE.

PCRF

Aquest sigla correspon a *policy and charging rules function* i és l'element de la subcapa de control de transport del PCC que pren les decisions quant a control d'admissió sobre les sol·licituds de recursos.

Així, doncs, el PCEF és un únic element que aglutina un gran nombre de funcions en l'aplicació de polítiques (control d'accés, NAT/NAPT, assignació de trànsit IP a túnels EPS, etc.), incloent funcions que afecten el reportament d'esdeveniments cap al PCRF per a notificar la modificació o l'establiment d'un túnel EPS per part de l'usuari (mode *pull* de sol·licitud de recursos) o també incloent funcions relacionades directament amb la facturació del servei en ús.

Per exemple, el PCEF ha d'assegurar-se que si un paquet IP ha estat descartat com a resultat de l'aplicació d'una política o a causa del càrrec associat a un flux, mai no haurà de ser reportat per a facturació fora de línia ni serà causa de consum de crèdit en la facturació en línia.

Les **regles PCC** són en realitat el resultat de les decisions en l'àmbit de sessió que l'entitat funcional PCRF (servidor de polítiques en la subcapa de control de transport) pren una vegada ha avaluat informació de disponibilitat de recursos de la xarxa i polítiques de l'operador de la mateixa xarxa. És una decisió de control d'admissió en l'àmbit de SDF (la descripció del qual pot ser rebuda, per exemple, des del punt de referència Rx), i les regles PCC són el resultat d'aquesta.

OCS i OFCS

Aquestes sigles corresponen a *online charging system* i *offline charging system*.

Interfície Gy

La interfície entre PCEF i OCS és el Gy. És utilitzada per a transferir informació de facturació en línia (prepagament). 3GPP recomana el protocol Diameter per a implementar-la (TS 32.299).

Així, doncs, els SDF (associats a cada regla PCC a manera d'entrades de classificació de trànsit) també poden estar subjectes a un control de facturació si el servei al qual van associats ho requereix així. Conseqüentment, el PCEF també ha d'estar al corrent d'aquest control. De fet, 3GPP ha definit dues interfícies dedicades amb les entitats funcionals de facturació OCS i OFCS i uns punts de referència anomenats Gy i Gz respectivament.

Per exemple, en cas de tenir un SDF subjecte solament a control de facturació, el PCEF permet que un SDF (definit per una regla PCC activa) que estigui subjecte a control de facturació passi a través d'ell només si hi ha una regla PCC activa associada i l'entitat OCS ha autoritzat el crèdit per a l'ús del servei.

Interfície Gz

La interfície entre PCEF i OFCS és el Gz. És utilitzada per a transferir informació de facturació fora de línia (postpagament). 3GPP recomana el protocol Diameter per a implementar-la (TS 32.299).

En cas de tenir un SDF que estigui subjecte als dos controls de polítiques de QoS i de facturació, PCEF permet el pas d'aquest flux de dades a través d'ell només si es donen les condicions de control de polítiques i facturació correctes, és a dir, si l'accés corresponent (en l'àmbit de tallafoc) ha estat habilitat i, en cas de facturació en línia, l'OCS ha autoritzat el crèdit per al servei associat als fluxos.

GTP

Els operadors de xarxa mòbil usen el GPRS *tunneling protocol* (GTP) en diverses interfícies en itinerància, la xarxa d'accés ràdio i dins la xarxa troncal en xarxes 3G i 4G per a portar el servei general de ràdio per paquets (GPRS). GTP permet als subscriptors mòbils usar els seus telèfons (UE) per a mantenir una connexió a una *packet data network* (PDN) per a accedir a internet mentre estan en moviment.

Finalment, en cas que un flux de dades de servei estigui subjecte solament a control de polítiques i no a control de facturació, el PCEF permet el pas d'aquest flux de dades a través d'ell només si es compleixen les condicions imposades per les polítiques corresponents.

b) Funció d'associació de túnels i reportament d'esdeveniments (BBERF). Aquesta entitat funcional, que en anglès es diu *bearer binding and event reporting function,* és mapada sobre l'SGW en l'arquitectura EPS i interconnectada amb el PCRF via el punt de referència Gxx.

Interfície Sp

La interfície entre PCRF i SPR és el Sp. És utilitzada pel PCRF per a obtenir de l'SPR informació de subscripció en l'àmbit de xarxa d'accés LTE. 3GPP recomana el protocol Diameter per a implementar-la (TS 23.203).

Tal com les sigles indiquen, aquest element és capaç de mapar el trànsit als túnels EPS. Pot sorgir la pregunta de per què el BBREF fa aquesta funció si el PCEF ja la fa com a extrem del túnel. Això és perquè, depenent del tipus de protocol de mobilitat usat en l'EPC, la funció d'assignació de túnels es fa en el PCEF (protocol GTP) o en el BBERF (protocol IP *mobile*).

La capacitat de reportar esdeveniments al PCRF també pot estar associada a aquesta entitat funcional amb les mateixes condicions esmentades pel que fa al PCEF. Per això és possible que en una xarxa d'accés mòbil no hi hagi el BBERF ni la interfície Gxx.

2) Subcapa de control de transport

En el model de 3GPP, aquesta subcapa és formada per dues entitats funcionals: SPR i PCRF. Aquí hem inclòs també les dues entitats extres encarregades de controlar càrrecs associats: l'OCS i l'OFCS, que ja han estat esmentades anteriorment.

GBR i MBR

Aquestes sigles corresponen a *guaranteed bit rate* i *maximum bit rate*.

a) Repositori de perfils de subscripció (SPR). Aquesta entitat funcional, anomenada en anglès *subscriber profile repository*, emmagatzema els perfils d'usuari en l'àmbit de capa de transport (entre d'altres, el GBR i l'MBR associats a aquest usuari i la llista de serveis permesos) i està interconnectat amb el PCRF per una interfície anomenada Sp. Es transfereix aquesta informació de perfil al PCRF perquè la tingui en compte a l'hora de fer el control d'admissió i generar les corresponents regles PCC. Aquest element està integrat normalment en la mateixa plataforma que l'HSS (*home subscriber server*), encara que pot ser una entitat funcional per separat.

b) Funció de regles de polítiques i facturació (PCRF). En anglès es diu *policy and charging rules function*. És l'element que pren les decisions quant a control d'admissió sobre les sol·licituds de recursos rebuts des de l'AF (*application function*) mitjançant el punt de referència Rx (mode *push*) o des del PCEF via la interfície Gx/Gxx (mode *pull*). També controla les tasques del PCEF pel que fa al control de facturació (i la seva interacció amb l'OCS i l'OFCS).

Per a 3GPP, l'AF (***application function***) és l'entitat de la subcapa de control de servei que és capaç d'extreure la informació de descripció de sessió de servei amb la petició de recursos i remetre-la amb el format adequat al PCRF via la interfície Rx. 3GPP preveu que si el servei està basat en IMS l'AF està implementat en el P-CSCF, i si no està basat en IMS és una entitat equivalent. L'important és que la sol·licitud de recursos de la sessió de servei compleixi l'especificació de la interfície Rx definida per 3GPP.

Desglossant amb més detalls les tasques que fa la PCRF, s'obté la llista següent per aquest ordre:

1) **Autorització de la sol·licitud de recursos de servei i control d'admissió de subscripció.** En cas de rebre una sol·licitud de recursos de servei via interfície Rx, el PCRF comprova que aquesta descripció de la sessió de servei és conforme amb les polítiques de l'operador (polítiques arbitràries). Si supera aquest filtre, comprova que aquesta sol·licitud és conforme amb la informació de subscripció (emmagatzemada en l'SPR) de l'usuari que l'ha sol·licitada. En cas que no es compleixi una sola d'aquestes dues comprovacions, la sessió es rebutja. En definitiva, és el que s'anomena control d'admissió.

2) **Autorització de la QoS (generació de regles PCC).** El PCRF usa la informació de descripció de servei rebuda des de l'AF i/o la informació de subscripció per a extreure l'autorització de QoS per als SDF extrets d'aquesta descripció. Els paràmetres d'autorització de QoS són principalment el QCI i els GBR i MBR corresponents, si s'apliquen. El PCRF pot tenir en compte també les sol·licituds de QoS rebudes des del PCEF via interfície Gx.

3) **Reportament d'esdeveniments.** El PCRF pot reportar, per exemple, esdeveniments ocorreguts en la capa de transport (estatus de túnels EPS o sessions EPS) o esdeveniments de facturació a l'AF si aquesta ho ha sol·licitat expressament via interfície Rx.

HSS

Aquesta sigla correspon a *home subscriber server*. És una base de dades que emmagatzema la informació de subscripció d'un usuari juntament amb informació d'autenticació i autorització en l'àmbit de servei (explicat en la secció 3, on es descriu el model de referència de 3GPP per a la capa de servei).

P-CSCF

Proxy call session control function.

És el component del nucli IMS que exerceix d'element fronterer amb l'equip d'usuari en l'àmbit de senyalització SIP (IMS). És una entitat funcional definida per 3GPP i que s'explica en la secció 3.

Interfície Rx

L'especificació d'aquesta interfície per 3GPP és descrita en el document TS 29.214.

QCI

Aquesta sigla correspon a *QoS class identifier* i defineix el grup de característiques en l'àmbit de qualitat de servei d'un tipus de trànsit. És un terme bàsic utilitzat en xarxes LTE i clau en la garantia de la qualitat de servei. Es descriu amb més detalls més endavant.

El PCRF suporta la comunicació amb altres PCRF de dominis administratius diferents per a l'escenari d'itinerància. Aquesta comunicació es fa mitjançant un punt de referència dedicat anomenat S9. En aquest cas, es deriven dues instàncies del PCRF segons en quin domini administratiu sigui: el V-PCRF per al control de la xarxa visitada i l'H-PCRF per al control de la xarxa on l'usuari mòbil pertany com a subscriptor.

Interfície S9

La interfície entre el PCRF i un altre PCRF d'un domini administratiu diferent (un altre operador) és l'S9. És utilitzada pel PCRF per a sol·licitar recursos en una xarxa LTE diferent de la seva i quan un subscriptor de la seva xarxa hi és (itinerància). 3GPP recomana el protocol Diameter per a implementar-la (TS 29.215).

c) Sistema de facturació en línia (OCS). L'*online charging system* fa la gestió del crèdit per a la facturació de prepagament. En aquesta entitat funcional rau la funcionalitat de control de crèdit basat en els fluxos de dades de servei que fa el control del crèdit en línia. El PCEF interactua amb aquesta entitat per comprovar el crèdit i reporta l'estatus d'aquest sobre el punt de referència Gy.

Un exemple d'aquest tipus de facturació és quan tenim un límit en el volum de dades a gastar en un mes. Si se supera aquest límit, la velocitat màxima de descàrrega baixa.

Arquitectura PCC

Crida l'atenció que el model d'arquitectura PCC defineix les tasques de facturació amb dos blocs específics, i la seva interacció amb elements de processament de transport. És un aspecte que 3GPP vol deixar ben especificat a causa del gran consum que ha arribat a tenir la telefonia mòbil.

d) Sistema de facturació fora de línia (OFCS). L'*offline charging system* s'encarrega d'aglutinar els esdeveniments de facturació rebuts des del PCEF via un punt de referència anomenat Gz per generar registres de facturació. Aquests registres (*charging data records*) s'envien després al sistema de generació de factures.

D'aquests registres surt posteriorment la factura que ens arriba a casa per correu.

Els EPS *bearers* i els QCI

Túnel EPS

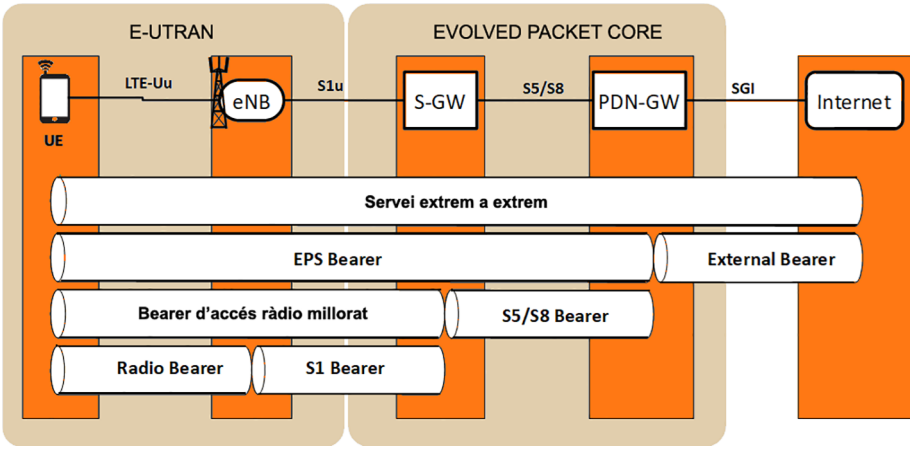
Com hem dit abans, 3GPP ha definit un concepte més abstracte associat al túnel EPS en els documents d'especificació: IP-CAN *bearer* (*IP-connectivity access network bearer*). Hi ha dos tipus d'IP-CAN o EPS *bearer*: *default bearer* i *dedicated bearer*.

Per començar, definirem amb més detalls el concepte d'**IP-CAN *bearer***, anomenat també **EPS *bearer***. L'EPS *bearer* és un canal virtual amb unes característiques de QoS i una amplada de banda particulars. És a dir, és una espècie de túnel els extrems del qual van des del mateix equip d'usuari (UE) fins a la PDN GW, i tot paquet IP que entri en aquest túnel gaudirà d'un tractament en l'àmbit de garantia de QoS específica al llarg de tot l'EPC.

Túnel EPS. Quan un paquet IP arriba a l'eNodeB, aquest mapa el túnel EPS a una portadora ràdio de característiques similars de QoS. És molt important entendre que el mapatge que l'eNodeB fa entre un túnel EPS i una portadora ràdio és d'un a un. L'estàndard de 3GPP prohibeix explícitament que més d'un túnel EPS es pugui mapar a una sola portadora ràdio.

Un EPS *bearer* és en realitat l'agrupació de diversos túnels establerts entre els elements de l'EPC i E-UTRAN. En la Figura 4 es pot veure com es divideix un EPS *bearer*.

Figura 4. EPS *bearers* i el seu desglossament entre entitats de l'EPC.



Així, un sol equip d'usuari (UE) pot tenir més d'un EPS *bearer* establert amb la corresponent PDN GW, i cadascun té les seves pròpies característiques de QoS. Els túnels EPS poden ser unidireccionals o bidireccionals i poden ser establerts, modificats o alliberats pel mateix UE o per la xarxa d'accés (MME o PCRF). Hi ha dos tipus de túnels:

Nombre màxim d'EPS *bearers*

El nombre màxim d'EPS *bearers* simultanis que un UE pot suportar és 11.

- ***Default***. És un túnel EPS que s'estableix de manera automàtica per la xarxa d'accés quan l'equip d'usuari s'adhereix a la xarxa d'accés LTE (MME) i se li assigna una adreça IP (activació d'una sessió EPS). A aquest tipus de túnel se li assigna sempre un QCI de tipus *non-GBR* (vegeu la taula 1). Aquest túnel es manté fins que el terminal s'apaga.

- **Dedicat.** Es un túnel que s'estableix per petició expressa del PCRF o de l'equip d'usuari quan s'invoca un servei que requereix una QoS diferent de l'oferta pel *default bearer* (per exemple, una trucada de veu). Aquest tipus de túnels poden tenir assignats qualsevol QCI: de tipus GBR o Non-GBR. Solament són establerts si el *default bearer* ja existeix.

Un UE pot tenir assignats diversos túnels EPS simultanis, tant *default* (perquè està associat a més d'un APN) com dedicat amb diferents característiques de QoS.

Quins paràmetres defineix 3GPP per a caracteritzar un túnel EPS en l'àmbit de QoS i on s'apliquen aquests paràmetres al llarg de l'EPS?

3GPP ha definit quatre paràmetres, els quals ja s'han anat esmentant anteriorment:

1) *QoS class identifier* (QCI), que defineix el comportament de QoS del trànsit associat a un túnel EPS. Aquest paràmetre, existent en la capçalera del túnel, és consultat en tots els nodes de l'EPC i E-UTRAN, ja que és un paràmetre molt important en el mapatge de cada túnel entre aquests nodes (vegeu la Figura 4).

Un **QCI** (***QoS class identifier***) identifica els valors d'un conjunt de paràmetres que defineixen com es tractarà el trànsit al llarg dels nodes que conformen l'EPS. Aquests paràmetres són quatre en total:

- **Tipus de recurs** (amb dos valors possibles: GBR velocitat de bit garantida o *non-GBR* velocitat de bit no garantida).
- **Prioritat** (valor sencer de l'1 al 9, que indica el nivell de prioritat respecte a altres fluxos).
- **Retard de paquet** (el retard màxim desitjat per a un paquet IP entre l'UE i la PDN GW).
- **Taxa de pèrdua de paquets** (la taxa de pèrdua de paquet màxima desitjada entre l'UE i la PDN GW).

3GPP ha estandarditzat un mínim de 9 QCI, amb valors assignats als paràmetres respectius, per a nou tipus de serveis predefinits. Aquests valors es poden veure en la taula 1.

QCIs

Tot i que els nou valors de QCI són els que s'implementen en xarxes LTE, 3GPP continua ampliant la llista de QCI en les successives versions de les seves especificacions per a cobrir altres serveis, com per exemple els de tipus *critical mission*. El document de 3GPP, en el qual es defineix la llista més actualitzada, és el TS 23.203 «*Policy and charging control*».

Taula 1. Llista de QCI.

QCI	Tipus de bearer	Prioritat	Retard de paquets	Pèrdua de paquets	Exemple d'aplicació
1	GBR	2	100 ms	10^{-2}	Trucada VoIP (veu)
2		4	150 ms	10^{-3}	Trucada de videoconferència (vídeo)
2		3	50 ms		Jocs en línia (temps real)
4		5	300 ms	10^{-6}	Transmissió de vídeo
5	Non-GBR	1	100 ms		Senyalització IMS
6		6	300 ms		Vídeo (flux de transmissió) basat en TCP (p. ex, WWW, correu electrònic, xat, FTP, P2P, o similars)
7		7	100 ms	10^{-3}	Veu, vídeo (transmissió en directe), jocs interactius
8		8	300 ms	10^{-6}	Vídeo (flux de transmissió) basat en TCP (p. ex, WWW, correu electrònic, xat, FTP, P2P, o similars). Utilitzat típicament com a bearer per defecte
9		9			Vídeo (flux de transmissió) basat en TCP (p. ex, WWW, correu electrònic, xat, FTP, P2P, o similars). Utilitzat típicament com a bearer per defecte

2) *Allocation and retention priority* (ARP). Aquest paràmetre indica el grau d'importància (nivell de prioritat) del túnel EPS en relació amb altres túnels. La consulta d'aquest paràmetre s'aplica principalment en nodes de l'EPC on es fa conformació de trànsit, com l'eNodeB i el PDN-GW.

Per exemple: Què succeeix si en un moment determinat un usuari es mou a una cel·la que està molt congestionada i la migració dels seus túnels EPS no es pot fer perquè no hi ha recursos suficients? Doncs que cal desallotjar altres túnels EPS actius, i el paràmetre ARP és el que ens dirà quins són els menys importants i, per tant, els candidats a ser alliberats.

3) *Guaranteed bit rate* (GBR). Indica la quantitat garantida de bits per segon que es necessiten (capacitat reservada) per a aquest túnel EPS. Aquest paràmetre s'especifica solament quan el túnel EPS té un QCI assignat de tipus GBR. El paràmetre GBR es pot modificar si es requereix una ampliació o disminució

del volum de trànsit a garantir. La garantia del *bit rate* s'aplica principalment en l'eNodeB i en el PDN-GW tant per al trànsit de pujada (*uplink*) com de baixada (*downlink*).

Per exemple: Què succeeix si ja existeix hi ha un SDF (regla PCC) que utilitza un túnel amb un QCI en concret i de sobte apareix un SDF o regla PCC nova que requereix un túnel amb el mateix QCI? Doncs que no s'establiran dos túnels amb el mateix QCI, sinó que es modificarà l'existent ampliant el GBR associat per fer lloc al nou flux de la segona regla PCC.

4) *Maximum bit rate* (MBR). Indica la quantitat màxima de bits per segon permesa (de pic) per a aquest túnel EPS. Aquest paràmetre s'especifica solament quan el túnel EPS té un QCI assignat de tipus GBR. En trànsit de pujada (*uplink*) aquesta conformació de trànsit es produeix en el mateix UE i posteriorment en l'eNodeB. En trànsit de baixada (*downlink*) aquesta conformació de trànsit es produeix en el PDN-GW.

Maximum bit rate

Cal destacar que el paràmetre *maximum bit rate* (MBR) sí que s'especifica per a un SDF de tipus *non-GBR*, mentre que en cas d'un túnel EPS no s'especifica (en el seu lloc aplica l'UE-AMBR i APN-AMBR).

A part dels quatre paràmetres de QoS que s'associen a cada EPS *bearer* esmentat anteriorment, hi ha uns altres dos paràmetres QoS que s'associen al perfil d'usuari en l'àmbit de xarxa d'accés LTE i que també es tenen en compte en la conformació del trànsit:

1) *APN-aggregated maximum bit rate* (APN-AMBR). Indica la quantitat màxima de bits per segon permesa (de pic) en pujada i baixada (*uplink* i *downlink*) per a l'agregat de tots els túnels EPS de tipus *non-GBR* associats a un APN (entre l'UE i una PDN-GW en concret). És a dir, que si un UE està associat a dues APN s'aplicaran dos paràmetres com aquest per separat, un per cada APN. Aquesta conformació de trànsit en baixada (*downlink*) s'aplica exclusivament en el PDN-GW. En pujada (*uplink*) s'aplica en dos llocs: el mateix UE abans d'encapsular i mapar el trànsit sortint en els túnels EPS, i de nou el PDN-GW abans d'enviar els paquets fos de l'EPS.

2) *UE-aggregated maximum bit rate* (UE-AMBR). Indica la quantitat màxima de bits per segon permesa (de pic) en pujada i baixada (*uplink* i *downlink*) per a l'agregat de tots els túnels EPS de tipus *non-GBR* associats a un UE. Aquest límit s'aplica a tot el trànsit *non-GBR* d'un usuari independentment de si està associat a més d'un APN o no. Aquesta conformació de trànsit l'aplica l'eNB tant en pujada (*uplink*) com en baixada (*downlink*) quan fa el mapatge dels *radio bearers*.

Els *service data flows* i el seu mapatge en els *EPS bearers*

Ja hem esmentat els **fluxos de dades de servei (*service data flows*)** quan hem descrit la regla PCC. Es defineixen una sèrie de filtres de fluxos IP que ajudaran el PCEF (PDN GW) a mapar els diferents fluxos IP en cada servei i, a més, a aplicar els paràmetres QoS associats a cada servei activat via la regla PCC corresponent.

Els **fluxos de dades de servei (*service data flows*)** es defineixen com un agregat de fluxos de paquets IP caracteritzats cadascun per la tupla de cinc paràmetres típica: adreces IP tant d'origen com de destinació, ports usats en origen i destinació, i el protocol. Igual que amb els túnels EPS, cada SDF especificat pel PCRF es classifica en dos tipus: GBR i *non-GBR*.

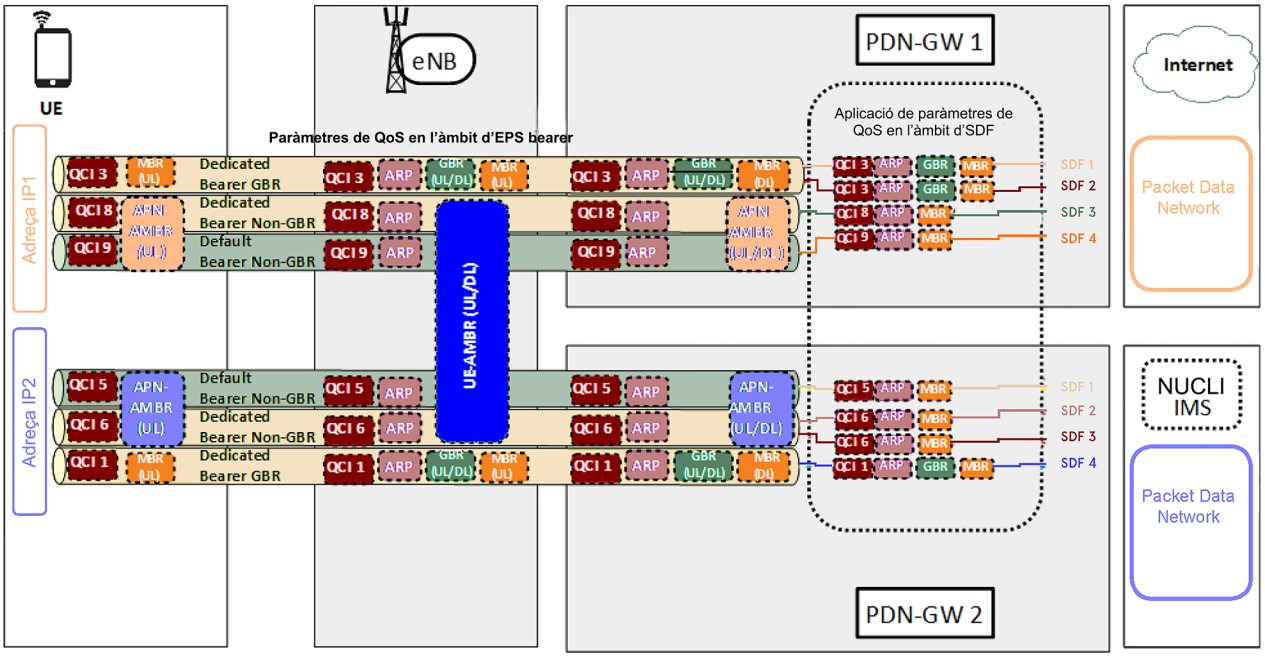
A cadascun d'aquests SDF s'associen uns paràmetres de QoS particulars que són independents dels fixats en cada túnel EPS.

Per a un SDF de tipus GBR, els paràmetres de QoS especificats són: QCI, ARP, GBR (*uplink/downlink*), MBR (*uplink/downlink*).

Per a un SDF de tipus *non-GBR*, els paràmetres de QoS especificats són: QCI, ARP, MBR (*uplink/downlink*).

Els paràmetres de QoS en els àmbits de SDF i de túnel EPS s'apliquen de manera independent. Mentre que els primers s'apliquen exclusivament en el PDN-GW (tant per a trànsit de pujada com de baixada), l'aplicació dels segons es distribueix al llarg de tot l'EPS, tal com hem explicat anteriorment i tal com es pot veure en la Figura 5.

Figura 5. Aplicació de paràmetres QoS en EPS *bearers* i SDF al llarg de l'EPC.



El mapatge entre un trànsit IP que ja ha estat assignat a un SDF i un túnel EPS es fa principalment mitjançant una correspondència directa entre el QCI del perfil QoS de l'SDF i el QCI del túnel EPS. Aquesta correspondència es fa realment aplicant altres filtres IP pensats específicament per a classificar el trànsit IP dins dels túnels EPS. Aquests filtres s'anomenen *traffic filtering templates* (TFT).

En el sentit de baixada (*downlink*), aquest mapatge SDF túnel EPS sembla evident, ja que la classificació prèvia a SDF es produeix en el PDN GW, però què succeeix en el sentit oposat (*uplink*)?

En pujada l'UE aplica directament els TFT (proporcionats a l'UE durant l'establiment o actualització del túnel EPS) per classificar el trànsit IP de les aplicacions en el túnel EPS corresponent. Com ja hem dit, el trànsit es classifica en l'àmbit de SDF en el PDN-GW, tant en pujada com en baixada, per aplicar els seus propis paràmetres QoS.

2.3. Elements del *mobile offload*

Tornant a la Figura 2 del principi, apareixen les xarxes Wi-Fi com una xarxa d'accés que l'UE pot usar per a accedir als serveis contractats amb l'operador de xarxa. Aquesta xarxa d'accés es considera com a *non-3GPP*, ja que no ha estat especificada per aquest organisme. No obstant això, aquestes xarxes són pràcticament a qualsevol espai públic (biblioteques, recintes esportius, centres comercials, etc.) i en recintes privats (hotels, cases particulars, empreses, etc.), i també s'han acabat integrant en el context d'especificació d'aquest organisme.

Com detecta un UE si és en una xarxa Wi-Fi confiable o no confiable?

Hi ha diverses maneres de fer-ho. Podria ser que l'UE tingués preconfigurades una sèrie de polítiques estàtiques o que el mateix operador comuniqués a l'UE si és una Wi-Fi confiable o no usant un protocol (anomenat ANDSF) que ha de ser suportat per l'UE, o que s'aprofités finalment la mateixa senyalització d'autenticació (EAP-AKA) en el punt d'accés per a transferir aquesta informació a l'UE.

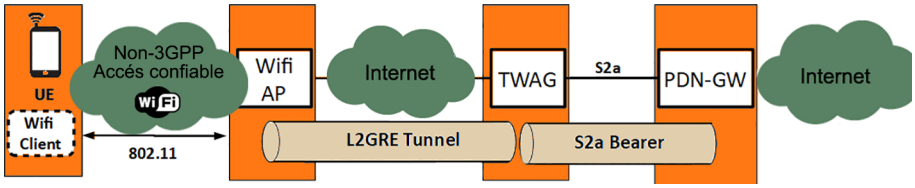
En la figura esmentada apareixen dues passarel·les segons si la xarxa Wi-Fi des de la qual es connecta és confiable (*trusted*) o no confiable (*untrusted*) des del punt de vista de l'operador de telefonia mòbil.

Una **xarxa Wi-Fi confiable** és aquella que és gestionada pel mateix operador i a la qual solament es poden associar subscriptors d'aquest operador.

Un exemple d'aquestes xarxes són les existents en les botigues dels mateixos operadors.

L'autenticació en aquestes xarxes es fa via credencials de la mateixa USIM de l'equip d'usuari. Entre l'UE i el punt d'accés de Wi-Fi no hi ha res més que una connexió Wi-Fi normal, i des del punt d'accés fins al punt d'ancoratge de la xarxa de l'operador s'estableix un túnel sense encriptació. Aquest punt d'ancoratge s'anomena **TWAG (*Trusted WLAN access gateway*)** .

Figura 6. Integració de l'EPC amb xarxes Wi-Fi confiables.



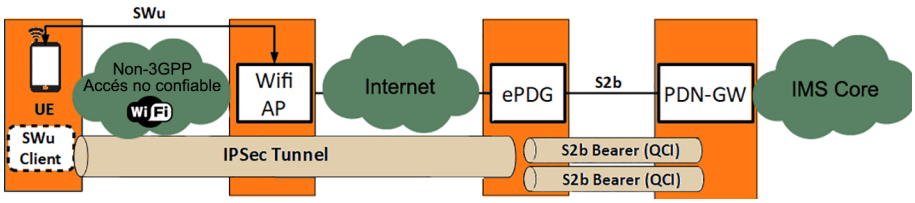
La particularitat d'usar aquesta xarxa Wi-Fi és que es va concebre (fins a la versió 11 de l'especificació de 3GPP) perquè l'UE descarregués la xarxa d'accés LTE del trànsit a internet. És a dir, que la PDN-GW a la qual es connecta el TWAG és exclusivament la corresponent a l'APN d'internet. I, de fet, el TWAG especificat en aquesta versió permet solament assignar una adreça IP i connectivitat a un PDN-GW per defecte, el de l'APN d'internet.

Connexió multi-APN amb TWAG

En la versió 12 de l'especificació de 3GPP s'ha inclòs una modificació en l'arquitectura perquè el nou TWAG permeti que des d'una xarxa confiable un UE pugui accedir a més d'un APN fent possible trucades IMS per Wi-Fi. Això comporta que l'UE hagi de suportar certes capacitats en l'àmbit de microprogramari que no feia falta amb la versió 11.

Una **xarxa Wi-Fi no confiable** és aquella que no ha estat desplegada pel mateix operador, i aquest és el cas més típic avui dia. En aquest cas l'UE ha d'establir un túnel IPsec (interfície anomenada SWu en l'especificació 3GPP) amb el punt d'ancoratge, que és una passarel·la dedicada. Aquesta passarel·la és l'ePDG (*evolved packet data gateway*) i està pensada per a proporcionar connectivitat amb la PDN-GW que dona accés al nucli IMS i poder fer així trucades de veu usant el mateix *dialpad* de marcatge del terminal sense necessitat d'instal·lar cap aplicació extra.

Figura 7. Integració de l'EPC amb xarxes Wi-Fi no confiables.



Com es pot veure en la Figura 7, entre l'ePDG i el PDN-GW s'estableixen túnels (*bearers*) dedicats amb els seus respectius QCI (interfície S2b), els quals poden ser, per exemple, per a la senyalització IMS (QCI 5) o per al trànsit de veu (QCI 1) segons les sessions que estableix l'usuari.

Nucli IMS

IMS és la sigla d'IP *multimedia subsystem*. Com veurem en la secció 3, és el model de referència per a processar la senyalització d'establiment i alliberament de sessions multimèdia.

***Wi-Fi calling*, trucades Wi-Fi** o **VoWiFi** són els noms comercials usats per a denominar aquest servei de trucades IMS per Wi-Fi. A diferència del cas de la Wi-Fi confiable, en el cas d'accedir a una Wi-Fi no confiable l'usuari ha de tenir un terminal mòbil que suporti aquesta tecnologia i el mateix operador ha d'haver implementat aquest tipus de connexió.

Malgrat utilitzar el nucli IMS i el protocol SIP per a senyalitzar l'establiment de trucada com en VoLTE, **la QoS no està garantida d'extrem a extrem**, ja que el trànsit travessa la xarxa Wi-Fi, la qual no està gestionada pel mateix operador. Així que s'assumeix que hi ha sobredimensionament de la capacitat de la xarxa d'accés entre l'UE i l'ePDG, que en la majoria dels casos no hauria de patir col·lapses davant una trucada de veu.

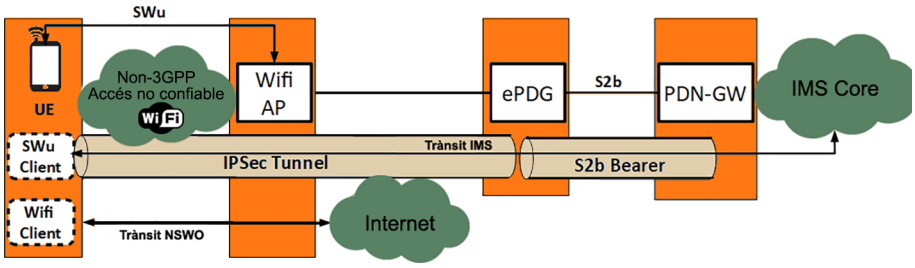
WiFi calling

El primer operador a Espanya a oferir *Wi-Fi-calling* als seus subscriptors ha estat Orange, encara que sense transferència transparent amb la xarxa mòbil.

En un escenari de Wi-Fi no confiable, com encamina l'UE el trànsit que no és de serveis IMS, com per exemple internet?

Hom podria pensar que pot utilitzar el mateix client SWu que incorpora el terminal i establir més túnels en la interfície S2b, però com que està connectat a l'APN d'IMS aquesta connexió es fa d'una altra manera gràcies a la definició per part de 3GPP del NSWO (*non-seamless WLAN offload*). És una prestació que ha de suportar també el mateix terminal, en el qual li indica que per a trucades IMS usi la interfície SWu (túnel IPsec) però per a trànsit no-IMS usi directament la Wi-Fi de manera transparent (vegeu la Figura 8).

Figura 8. NSWO en xarxes Wi-Fi no confiables.



WebRTC

L'acrònim WebRTC respon a ***web real-time communications*** i és el nom d'un entorn o estàndard que estén les capacitats del navegador de web. Aquest estàndard ha estat definit per W3C partint d'un projecte en codi obert al qual donen suport grans companyies tecnològiques com Google, Mozilla Foundation, Opera Software i Apple. Fa possible comunicacions multimèdia d'igual a igual utilitzant el mateix navegador web i és compost per tres components principals: àudio, vídeo i dades.

W3C

Correspon a World Wide Web Consortium. Amb seu al MIT (Massachusetts Institute of Technology), té com a objectiu desenvolupar protocols i directrius que garanteixen el creixement de la web a llarg termini. (http://www.w3.org)

Bàsicament, encapsula en dos *web-sockets* la informació d'àudio i vídeo capturada del micròfon i la càmera del terminal (PC o telèfon intel·ligent) directament des del navegador.

Web-socket

És una tecnologia que proporciona un canal de comunicació bidireccional i dúplex sobre un únic socket TCP. És dissenyada per ser implementada en navegadors i servidors web, però pot ser utilitzada per qualsevol aplicació client-servidor. IETF ha definit les seves característiques en l'RFC 6455.

En les últimes versions de pràcticament qualsevol navegador existent aquests ja suporten WebRTC (principalment han de suportar HTML5).

> Això permet integrar en la pròpia web comunicacions multimèdia que tenen molt èxit en pàgines on es requereixi algun tipus d'interacció amb algun servei d'atenció al client o assessorament, com per exemple webs de bancs o fins i tot en atenció mèdica remota.

El principal avantatge d'usar WebRTC és la integració total de comunicacions multimèdia en el mateix navegador, que el converteixen en un terminal de comunicacions i enriqueixen l'experiència de l'usuari.

El principal desavantatge és que no hi ha garantia de QoS en aquest intercanvi multimèdia. S'assumeix que la connectivitat a internet és prou folgada per a garantir una qualitat mínima.

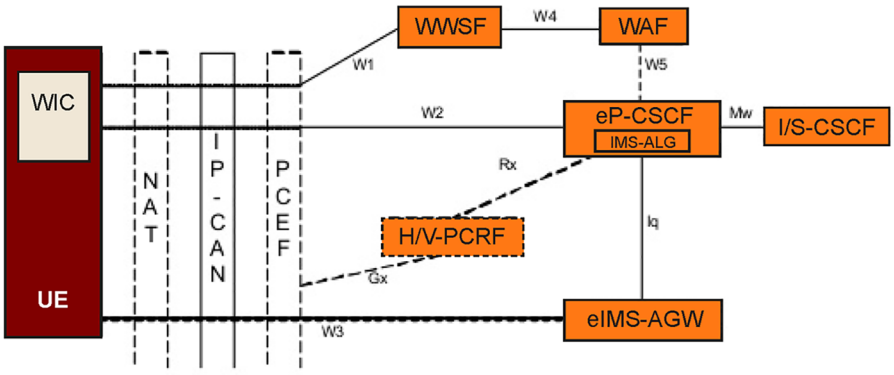
L'especificació d'aquest estàndard solament defineix com negociar els components multimèdia (còdecs de veu i vídeo, per exemple) entre dos navegadors web (usant el protocol SDP), però no especifica cap mecanisme d'establiment de trucada. Això s'ha de fer mitjançant altres mecanismes i protocols que aquest estàndard no permet.

SDP

Session description protocol. Protocol per a negociar paràmetres multimèdia d'establiment de sessió (còdecs o ports UDP on enviar els fluxos RTP). És especificat en l'RFC4566.

La senyalització SIP que l'estàndard IMS inclou pot ser una manera de permetre que aquesta informació de negociació pugui ser intercanviada i afegir així un altre tipus d'UE des del qual poder accedir als serveis contractats. No obstant això, la integració d'IMS amb WebRTC no és trivial. 3GPP ha fet esforços per a proposar una especificació sobre com integrar-ho (TS 24.371) i proposa bàsicament això:

Figura 9. Model de referència proposat per 3GPP per a integrar WebRTC i IMS.



P-CSCF

El P-CSCF és un element que pertany a la capa de servei, en concret al nucli IMS. Aquest element és descrit detalladament en la secció 3.1.3.

- El **WIC** (***WebRTC IMS client***) és integrat en el mateix codi de la web (JavaScript) per implementar un *stack* senzill que proporcioni el client IMS en el mateix navegador. Tota la senyalització entre l'UE i l'eP-CSCF seria encapsulada en un *web-socket* específic per a la senyalització IMS.

- L'**eP-CSCF** (***enhanced P-CSCF for WebRTC***) s'encarrega de fer les funcions del P-CSCF amb la particularitat d'encapsular i desencapsular en *web sockets* tota la senyalització IMS intercanviada amb l'UE (interfície W2).

- El **WWSF** (***WebRTC web server function***) és el servidor web on s'alberga la pàgina en la qual és integrat el WIC. L'usuari haurà de connectar-se a aquest servidor (interfície W1) com a primer pas i descarregar-se així aquesta web. Aquest element pot estar en un servidor separat (proporcionat per un tercer) o integrat en el mateix eP-CSCF. Aquesta entitat inclou una **WAF** (***WebRTC authorization function***), que s'encarrega d'autenticar l'usuari (interfície W4) amb les seves credencials quan aquest intenta descarregar-se la web.

- L'**eIMS-AGW** (***enhanced IMS access gateway for WebRTC***) fa les funcions de passarel·la multimèdia per als fluxos de veu, vídeo i dades que arriben encapsulats en els *web-sockets* respectius (interfície W3).

El conjunt de l'eP-CSCF més l'eIMS-AGW fan les funcions del WebRTC GW que apareix en la Figura 2 al principi.

3. Capa de servei

En la capa de servei hi ha un subconjunt d'elements que és predominant com a plataforma de provisió i habilitació de serveis multimèdia i que volem destacar: el **nucli IMS**. 3GPP, com a creadora de l'IMS, centra la seva arquitectura de control de servei en aquesta tecnologia, que és la que es descriurà detalladament en les seccions següents.

El **nucli IMS** s'encarrega de rebre i processar la senyalització d'establiment de sessions de servei multimèdia (SIP) provinent dels usuaris i, a més, compleix les funcions següents:

- Emmagatzematge de perfils d'usuari en l'àmbit de servei.
- Mecanismes associats de registre, autenticació i autorització.
- Negociació de prestacions (com els codificadors de veu i vídeo en l'establiment d'una videoconferència) i control de recursos (amb les subcapes de transport).
- Encaminament de senyalització cap a destinatari basat en adreces de domini.

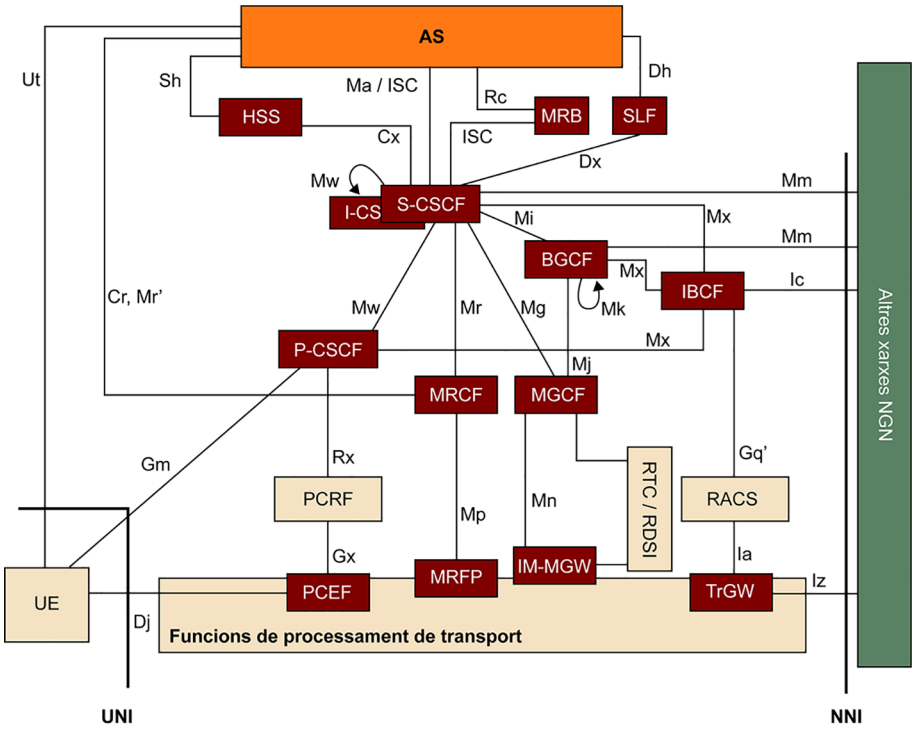
Normalment, el nucli IMS serveix a un sol domini administratiu i aquest és associat a un operador, en el qual els usuaris són subscriptors d'una llista de serveis, representats pels AS (*application servers* i que veurem en la secció 4), als quals accedeixen pel nucli IMS.

A continuació veurem una descripció detallada de les entitats que conformen un nucli IMS i com interactuen entre elles segons el servei que s'invoca des de l'usuari.

3.1. Components del nucli IMS

En la Figura 10 es pot veure l'arquitectura de referència que 3GPP defineix per al nucli IMS.

Figura 10. Arquitectura de referència d'IMS per a 3GPP.



Al llarg de totes les versions que 3GPP ha publicat, el nombre d'elements funcionals que conformen el nucli IMS s'ha incrementat, com també ho ha fet la quantitat de punts de referència que en connecten uns amb uns altres. Hi ha elements funcionals amb una diferència entre ells que és mínima, i aquesta sobrefragmentació de les funcions ha donat lloc a un sistema molt complex la implementació del qual requereix una inversió més que considerable per part dels operadors. Això és així perquè la tecnologia IMS ja té una certa maduresa i arriba la fase d'adaptació als requeriments que el mateix mercat imposa en l'àmbit de serveis.

Nucli IMS

Hi ha un consens bastant estès entre els operadors de telefonia mòbil i els fabricants d'equips del nucli IMS en el fet que l'especificació d'aquest ha esdevingut excessivament complexa, i és per això que, vistos els serveis que tenen més sortida comercial, com VoLTE, han sol·licitat que en futures versions de 3GPP es faci una simplificació del mateix nucli.

Tenint en compte això, orientarem el contingut d'aquesta secció a descriure els elements més bàsics del nucli IMS, que avui dia ja usen aquells operadors que han optat per implantar-los.

3.1.1. S-CSCF (*serving call session control function*)

L'S-CSCF és el punt central i principal node de control de sessió SIP en una xarxa IMS. És responsable de mantenir el procés de registre, prendre decisions d'encaminament i manteniment de l'estat de sessió SIP, i emmagatzemar els perfils de servei per a usuaris registrats activament.

Molts S-CSCF poden existir concurrentment en la xarxa d'un operador per a garantir un equilibri de càrrega.

Per a explicar amb més detall el paper de l'S-CSCF en el nucli IMS, ens centrarem en el fet de com actua quan es donen els dos processos més importants: el registre d'un client IMS (via missatge SIP REGISTER) i l'establiment d'una sessió (via missatge SIP INVITE):

Registre i establiment de sessió en IMS

En seccions posteriors es presenten exemples de senyalització intercanviada durant un registre i una trucada de VoLTE. Allí es veu més clarament el paper dels missatges SIP REGISTER i SIP INVITE.

a) En el **procés inicial de registre de l'usuari** , un usuari envia una petició de registre (SIP REGISTER) que és encaminada cap a un S-CSCF que ha estat seleccionat prèviament per un altre element del nucli IMS, l'I-CSCF, que veurem posteriorment. En l'intent inicial de registre, l'S-CSCF descàrrega les dades d'autenticació des de l'HSS (via interfície Cx) i respon a la petició de registre amb un error «401 Unauthorized». En aquesta resposta repta l'UE perquè proporcioni la informació d'autenticació (un residu calculat usant la contrasenya) en l'intent següent.

b) En el **procés final de registre de l'usuari** , el mateix S-CSCF rebrà (des de l'I-CSCF via interfície Mw) un segon intent de registre que conté informació d'autenticació, que compara amb la que el mateix S-CSCF ha calculat per saber si l'autenticació és correcta. Si ho és, emmagatzema l'associació entre l'adreça IP de contacte que usa l'UE i almenys una identificació pública (anomenada IMPU) de l'usuari (la que ha usat per a registrar-se). Finalment, l'S-CSCF descarrega de l'HSS un perfil de servei (*service profile*) de l'usuari associat a l'IMPU, usat com una part del procés de registre.

Interfície Mw

La interfície entre les CSCF d'un nucli IMS és l'Mw. És utilitzada per les CSCF per a reexpedir-se senyalització SIP de registre o control de sessió (originada des d'una destinació i fins a un UE) entre ells segons els seus criteris d'encaminament. 3GPP recomana el protocol SIP per a implementar-la (TS 23.517).

c) En el **procés d'encaminament de missatges SIP d'una nova sessió de servei multimèdia**, l'S-CSCF farà una funció o una altra segons si la trucada arriba a l'usuari (*call terminating*) o és iniciada per l'usuari (*call originating*):

Interconnexió entre operadors amb IMS

El model de referència de 3GPP especifica que la senyalització SIP entre dos operadors ha de passar per l'IBCF, però això és així si aquesta interconnexió entre operadors ha estat implementada específicament així. En cas contrari, la trucada s'encamina via xarxes heretades usant la BGCF. De fet, aquest és el cas més habitual encara avui dia entre operadors de telefonia mòbil que implementen VoLTE.

- *Terminating*. Si el missatge SIP de *request* (principalment SIP INVITE) és rebut per l'S-CSCF de l'usuari destinació, l'S-CSCF trobarà l'adreça IP associada en el registre de l'usuari. Reenviarà el missatge a l'usuari final fent-lo passar abans pel P-CSCF, després del qual hi ha aquest usuari (via interfície Mw).

- *Originating*. Consulta la capçalera SIP Request-URI del missatge SIP de *request* per saber el salt següent (és a dir, a quin element del nucli IMS s'ha de reexpedir). Aquest salt pot ser a un dels elements següents:
  - A UE destinació directament (fent-lo passar pel P-CSCF corresponent) **si l'usuari trucat està registrat en el mateix S-CSCF**.
  - A un I-CSCF **si l'usuari està registrat en un altre S-CSCF** del mateix nucli IMS.
  - A un SIP *proxy* específic anomenat *breakout gateway control function* (BGCF) **si l'usuari destinació és un àlies no-IMS** (per exemple, un número telefònic). Aquest, si veu que és de tipus telefònic, el reexpedirà

a una *media gateway control function* (MGCF) (passarel·la de control cap a RTC/RDSI) de la seva elecció.

– A l'element fronterer que comunica amb un altre nucli IMS d'un altre domini administratiu **si l'usuari trucat s'identifica amb un àlies d'IMS**. Aquest element s'anomena *interconnection border control function* (IBCF).

– A un servidor de continguts multimèdia administrat pel mateix operador **si la trucada és redirigida, per exemple, a una bústia de veu o contestador automàtic**. Aquest servidor és l'MRF (*media resource function*), que està dividit en dos blocs: el *multimedia resource function controller* (MRFC) (que rep la senyalització SIP) i el *multimedia resource function processor* (MRFP) (que processa fluxos multimèdia).

d) L'S-CSCF pot fer **funcions d'invocació de serveis externs que rauen en SIP AS (servidors d'aplicació)** . En aquest procés l'S-CSCF, abans d'aplicar les funcions d'encaminament descrites abans, consulta el perfil de servei descarregat des de l'HSS de l'usuari. Aquest perfil inclou els iFC (*initial filter criteria*), que s'usen per a decidir a quins servidors d'aplicacions (SIP AS), i en quin ordre, s'han d'enviar els missatges SIP de *request*. La interconnexió entre l'S-CSCF i els SIP AS es fa via interfície ISC. A més, el perfil de servei pot incloure més instruccions sobre quin tipus de política de comunicació necessita aplicar l'S-CSCF (per exemple, podria indicar que un usuari està habilitat per a utilitzar components d'àudio però no de vídeo).

Interfície ISC

La interfície entre l'S-CSCF i un SIP AS és l'ISC. És utilitzada per l'S-CSCF i l'AS per a reexpedir i rebre peticions SIP (TS 23.218).

3.1.2. I-CSCF (*interrogating call session control function*)

L'I-CSCF és usat per a reexpedir un missatge SIP *request* inicial (com, per exemple, de registre SIP REGISTER o d'inici de sessió SIP INVITE) cap a un S-CSCF (via interfície Mw) quan l'iniciador del missatge no sap a quin S-CSCF hauria de rebre aquest missatge. De fet, per a trucades entrants des d'un altre domini administratiu o operador, l'I-CSCF és el punt de contacte dins de la xarxa de l'operador local per a totes les connexions destinades a un subscriptor d'aquest operador de xarxa.

Per a obtenir la informació sobre l'S-CSCF al qual s'ha de reexpedir un missatge SIP *request*, l'I-CSCF contacta l'HSS (*home subscriber server*) usant la interfície Cx.

Interfície Cx

La interfície entre l'S-CSCF/I-CSCF i un HSS és el Cx. És utilitzada per l'S-CSCF i l'I-CSCF per a consultar a l'HSS informació d'autenticació i autorització d'usuari, perfil de subscripció, localització (S-CSCF assignat). 3GPP recomana usar el protocol Diameter per a implementar-la (TS 29.229).

Seguint la mateixa filosofia que en la descripció de l'entitat funcional anterior, les funcions més importants que ha de fer l'I-CSCF s'especifiquen a continuació:

a) En el **procés inicial de registre de l'usuari** , l'I-CSCF, en rebre el SIP REGISTER des del P-CSCF, assigna un S-CSCF en funció de les capacitats rebudes des de l'HSS (l'I-CSCF demana a l'HSS quines opcions hi ha i selecciona l'S-CSCF d'una llista) i la reenvia a aquest S-CSCF.

Interfície Dt.

La interfície entre l'I-CSCF i un SIP-AS és el Dt. És utilitzada per l'I-CSCF per a reexpedir peticions SIP a l'AS amb serveis públics d'identitats (PSI). 3GPP recomana usar el protocol SIP per a implementar-la (TS 23.228).

b) En el **procés d'encaminament de missatges SIP d'inici de sessió de servei multimèdia (SIP INVITE)**, l'I-CSCF s'encarrega d'obtenir el nom del salt següent (S-CSCF) cap a on dirigir (via interfície Mw) aquest missatge SIP. Es diferencien dos casos segons si la xarxa nucli IMS a la que pertany l'I-CSCF és l'origen o la destinació de l'inici de la sessió:

- *Terminating*. Si el missatge SIP de *request* (principalment SIP INVITE) és rebut per l'I-CSCF i és en la mateixa xarxa o domini que l'usuari destinació, l'I-CSCF consulta l'HSS per saber l'S-CSCF al qual l'usuari destinació està associat. Per a fer aquesta consulta, es basa en la capçalera SIP Request-URI que el mateix SIP INVITE porta.

- *Originating*. Perquè l'I-CSCF rebi un missatge SIP de *request* mentre el missatge de *request* és a la xarxa d'origen, ha d'haver-se originat des d'un servidor SIP d'aplicació (via interfície Dt.) en nom d'un usuari. Aquest servidor no sap l'S-CSCF de l'usuari que ha originat la trucada. En aquest cas concret, l'I-CSCF consultarà l'HSS per saber en quin S-CSCF és registrat l'usuari que origina la trucada i enviar el missatge SIP a aquest S-CSCF.

c) L'I-CSCF pot proporcionar **funcionalitat THIG (*topology hiding inter-network gateway*)** de manera opcional. Un altre operador que vulgui enviar senyalització SIP cap al domini local, l'enviarà a l'I-CSCF com si fos un servidor intermediari, ja que serà l'únic element del nucli IMS visible des de l'exterior (des d'altres operadors). L'I-CSCF pot actuar com un element SBC (*session border controller*, concepte definit en la secció següent) solament en l'àmbit de senyalització SIP per a la interfície entre dos dominis o xarxes NGN (interfície NNI).

3.1.3. P-CSCF (*proxy call session control function*)

El **P-CSCF** és el primer punt de contacte dins d'IMS per als usuaris adherits a una xarxa d'accés, i aquesta és la raó per la qual es considera un element de control fronterer (*session border controller*) amb l'usuari (interfície UNI).

En realitat, el concepte de *session border controller* s'aplica en tot aquell punt de la xarxa NGN on hi hagi una frontera de domini administratiu (és a dir, tant en la interfície UNI, on UE i domini IMS s'uneixen, com en la interfície NNI, on dos dominis IMS s'uneixen).

SBC (*session border controller*)

Un *session border controller* (SBC) és un element col·locat en les fronteres administratives d'una xarxa gestionada o domini. Aborda els problemes que sorgeixen de la provisió de servei multimèdia basat en sessions IP. Una de les seves funcions és la **seguretat**, respecte a la qual controla l'admissió de trucades a les fronteres de la xarxa per garantir QoS del trànsit que hi entra i en surt, i així s'evita l'abús en l'ús del servei i es fan tasques de protecció de la privadesa de l'operador i l'usuari. Altres funcions de l'SBC són usar protocols com SIP en presència d'un **tallafocs o NAT** (SIP ALG o *application level agreement*) o fer **monitoratge de regulació**, com la intercepció de trànsit per llei (*lawful interception*), **facturació i monitoratge del servei**. Un SBC pot tenir entitats funcionals separades per a senyalització i mitjans.

Així, doncs, tot el trànsit de senyalització IMS que parteixi de l'UE o hi arribi haurà d'haver passat abans pel P-CSCF. Aquesta interfície de senyalització entre aquests dos elements és anomenada Gm, i l'UE posarà sempre l'adreça IP del P-CSCF com a destinació, ja que aquest fa de servidor intermediari per a totes les transaccions SIP.

Interfície Gm

Interfície entre UE i P-CSCF per a intercanviar missatges de senyalització SIP d'IMS (registre, control de sessions i transaccions). 3GPP recomana usar el protocol SIP per a implementar-la (TS 23.002).

Les funcions més importants que ha de fer el P-CSCF s'especifiquen a continuació:

a) En el **procés inicial de registre de l'usuari** , el P-CSCF haurà de reexpedir la petició de SIP REGISTER arribada des de l'UE a l'element del nucli IMS que s'encarrega de redirigir el missatge de registre al S-CSCF assignat, i aquest element és l'I-CSCF. Per a això, observa la capçalera del missatge SIP, en concret la part que descriu el domini en el SIP URI al qual pertany l'usuari. A partir d'aquest domini pot descobrir a quin I-CSCF (és a dir, el seu *hostname*) ha de reexpedir el SIP REGISTER (sia resolent via DNS o consultant alguna taula preconfigurada).

Paper de l'I-CSCF

Quan un UE es registra per primera vegada, el P-CSCF no sap a quin S-CSCF ha de redirigir el SIP REGISTER, i per defecte ha de trobar almenys un I-CSCF al qual reexpedir aquest missatge. En cas de ser un missatge SIP d'inici de trucada (SIP INVITE), el P-CSCF ja sabrà a quin S-CSCF ha de reexpedir el missatge, ja que aquesta informació haurà quedat emmagatzemada en la fase de registre. En aquest últim cas, l'I-CSCF no participa en absolut.

b) En el **procés final de registre de l'usuari** , el P-CSCF haurà d'emmagatzemar informació del mateix registre que relacioni unívocament l'UE amb l'S-CSCF assignat. Per exemple, emmagatzema la informació de contacte de l'UE (IP assignada) i l'adreça de l'S-CSCF, i també els identificadors públics de l'usuari (IMPU) que l'S-CSCF ha associat en el registre.

c) Quan **l'UE inicia o rep una nova sessió de servei multimèdia**, el P-CSCF haurà de verificar que els camps de la capçalera del missatge SIP INVITE continguin els valors concordes a la informació emmagatzemada durant la fase de registre. Una vegada verificat el missatge, s'encarregarà de redirigir els missatges SIP al S-CSCF assignat o a l'UE (segons si l'UE és l'iniciador d'aquesta sessió o el receptor) via interfície anomenada Mw.

Seguretat entre UE i P-CSCF

Això s'aconsegueix després del primer intent de registre SIP, quan l'UE rep resposta amb un codi d'error 401 originat per l'S-CSCF corresponent, el qual inclou un *authentication vector* en el qual hi ha dues claus: IK (*integrity key*) i CK (*cipher key*), que haurà d'usar el P-CSCF per a negociar associacions de seguretat IPsec. Així poden aplicar protecció de confidencialitat i integritat per a la resta de la senyalització SIP.

d) En fer el **paper d'element fronterer amb l'UE** (interfície UNI), pot oferir **funcionalitats de garantia d'integritat i confidencialitat** de tota la informació de senyalització intercanviada entre l'UE i el nucli IMS (sobretot en cas que l'UE es connecti usant una xarxa d'accés no gestionada pel mateix operador o susceptible de ser escoltada per tercers). Aquesta funcionalitat la fa establint una connexió segura entre l'UE i el P-CSCF, sia usant una connexió IPsec o TLS.

e) Té un **paper molt important en la garantia de la QoS dels serveis invocats**. Com que és un SBC, processa la informació relacionada amb els recursos multimèdia associats a una sessió (com, per exemple, els requeriments en bits per segons associats a l'ús d'un codificador de veu en concret). Aquesta informació de recursos està inclosa implícitament o explícitament en la senyalització SIP que el mateix UE genera, i el P-CSCF la sintetitza per enviar-la a la subcapa de control de transport via interfície Rx. Aquesta informació de recursos multimèdia pot ser manipulada fins i tot pel mateix P-CSCF (a manera de SBC) per a fer funcions de transcodificació i així resoldre problemes d'incompatibilitat entre UE (recolzant en elements de la capa de transport que processin el trànsit de veu).

f) Opcionalment, pot fer funcions de **compressió i descompressió dels missatges SIP** que provenen de l'UE si la connexió establerta entre el client IMS (UE) i el P-CSCF és suportada i s'ha negociat així.

P-CSCF i UE en itinerància

En cas de ser un I-CSCF del mateix domini que el P-CSCF, el SIP REGISTER es reenvia a aquest element. Si l'I-CSCF és de diferent domini (en cas d'itinerància) el SIP REGISTER s'envia a l'I-CSCF per via del corresponent element de control fronterer o SBC de la xarxa visitada, que en aquest cas és l'entitat IBCF (usant una interfície anomenada Mx)

g) **Detectar i gestionar les peticions de sessió d'emergència** (selecció d'un S-CSCF dedicat exclusivament a emergències, anomenat I-CSCF).

Quan el P-CSCF rep un inici de trucada (SIP INVITE que podria provenir fins i tot d'un UE no registrat), l'àlies (SIP URI del tipus sip:usuari@domini.com) o número de telèfon de destinació (Tel URI del tipus tel: 933219876) es compara amb una llista preconfigurada de telèfons d'emergència (normalment, és el mateix amb independència del país gràcies a acords internacionals, com el número 112).

h) Tal com hem abans, pot també actuar opcionalment **com a passarel·la de senyalització (entre la interfície W2 basada en *web-socket* i la interfície Mw basada en SIP) per a trucades fetes des de l'UE usant tecnologia WebRTC**. En aquest cas se l'anomenaria eP-CSCF (*enhanced* P-CSCF).

3.2. Components d'emmagatzematge d'informació de subscripció

A continuació, explicarem les entitats especialitzades en l'emmagatzematge de subscripcions d'usuari i que són clau en la provisió de serveis.

3.2.1. HSS (*home subscriber server*)

És la base de dades principal de subscriptors per a IMS. Conté informació de subscripció de cada usuari i la distribueix a diferents entitats funcionals del nucli IMS o servidors d'aplicacions (SIP AS o *SIP application servers*).

La informació de subscripció que el nucli IMS usa conté principalment la informació següent:

Altres funcions de l'HSS no relacionades amb IMS

En un context de telefonia mòbil, l'HSS també fa una sèrie de funcions. Amb l'objecte d'interaccionar amb els dominis de commutació de paquets (formats pel mateix nucli IMS i l'EPS) i commutació de circuits, l'HSS conté funcionalitats de *home location register* (HLR) en xarxes mòbils LTE i *authentication center* (AUC), tal com defineix 3GPP.

- **Informació d'autenticació del subscriptor en l'àmbit de registre en el nucli IMS**, la qual és composta per una identitat privada o IMPI i una contrasenya, com a mínim.

- **Relació entre les diferents identitats privades (IMPI) i públiques (IMPU)**, anomenades *implicit registration set*.

- **Informació d'invocació de serveis en SIP AS o *service triggering data***, la qual és composta pels *service profiles* associats als IMPU i que contenen les regles d'orquestració de missatges SIP cap als diferents SIP AS. Aquestes regles s'anomenen *initial filter criteria* (IFC).

Informació relacionada amb els serveis proporcionats a l'usuari, informació de tarifació, màxim nombre de trucades per sessió, màxim nombre de sessions simultànies, components multimèdia habilitats (si pot usar vídeo i/o àudio en una trucada), etc.

Un **IRS (*implicit registration set*)** és l'associació implícita de diverses identitats públiques (IMPU) amb una identitat privada (IMPI). És a dir, que si un usuari es registra en el nucli IMS usant la identitat privada o IMPI i una identitat pública o IMPU en concret, podrà ser trucat usant tant l'IMPU que ha usat en el registre com tots els IMPU extres associats a aquest IRS. Aquestes associacions entre identitats es bolquen de l'HSS al S-CSCF en la fase de registre perquè aquest pugui identificar aquests IMPU com a vàlids.

Interfície Sh

És una interfície entre SIP AS i l'HSS utilitzada per l'AS per a consultar a l'HSS informació d'autenticació i autorització d'usuari, perfil de subscripció i localització (S-CSCF assignat). 3GPP recomana usar el protocol Diameter per a implementar-la (TS 29.329).

Aquesta informació de subscripció pot ser proporcionada directament mitjançant la interfície de control Cx (en l'I-CSCF o S-CSCF) o indirectament aprofitant la mateixa senyalització SIP d'alguna transacció en curs (en el P-CSCF o l'UE).

Els SIP AS també poden usar l'HSS per a emmagatzemar i obtenir informació específica del servei que proporcionen (via interfície Sh) a un usuari. Aquesta informació es classifica en dos tipus en funció de si el format de la infor-

mació no està estandarditzat (*transparent*) o sí que ho està (*non-transparent*). L'operador podrà configurar una llista de SIP AS autoritzats i polítiques de privadesa per als usuaris.

L'HSS és capaç de manejar altres identificadors públics diferents dels IMPU. Són identificadors de servei o PSI (*public service identifier*) d'acord amb les especificacions de 3GPP.

Un **PSI (*public service identifier*)** identifica tot allò que pugui ser receptor d'un missatge de petició SIP i no és un usuari (per al qual s'usaria un IMPU). Per tant, un PSI pot identificar qualsevol recurs d'un servei proveït per un servidor d'aplicació (AS), el qual pot ser el mateix servei. Per exemple, un PSI pot identificar un contingut en concret, una conferència predefinida, una habitació de xat, etc. Pot identificar també, per exemple, tot un grup d'usuaris.

A continuació es resumeix la participació de l'HSS en els processos de registre i encaminament de missatge SIP durant l'establiment de sessions:

Mètodes d'autenticació en IMS

L'HSS ha de suportar diversos models d'autenticació: IMS AKA, IETF HTTP *Digest* i IMS SSO.

a) En el **procés inicial de registre de l'usuari** , se li assigna un S-CSCF. Abans d'aquesta assignació, l'HSS decideix si l'usuari està autoritzat a registrar-se en el subsistema IMS basant-se en les identitats públiques (IMPU) rebudes en la petició de registre (comunicades per l'I-CSCF via interfície Cx), en les dades de configuració de l'HSS i en la informació d'usuari emmagatzemada. L'HSS permet el procés d'assignació de S-CSCF comunicant a l'I-CSCF la identitat de l'S-CSCF en el qual l'usuari està registrat, o bé un conjunt de capacitats que seran emprades per l'I-CSCF per a seleccionar el més adequat. L'HSS emmagatzema la informació de l'S-CSCF assignat a aquest usuari. Finalment, l'S-CSCF sol·licita a l'HSS informació d'autenticació per reptar l'UE a autenticar-se en un segon intent de registre.

b) En el **procés final de registre de l'usuari** , l'S-CSCF, una vegada que ha autenticat l'usuari correctament, sol·licita a l'HSS l'abocament de la llista d'IMPU associats a l'IRS (si n'hi ha) i la llista d'IFC associats al *service profile* de l'IMPU o grup d'IMPU usats.

c) L'**HSS participa en l'establiment de la sessió IMS** quan l'usuari la inicia. No encamina missatges SIP, però retorna a l'I-CSCF, via interfície Cx, el*hostname* de l'S-CSCF assignat a un usuari en cas que la identitat pública involucrada en la sessió hagi estat registrada amb anterioritat. Si la identitat pública (IMPU) no està registrada, l'HSS indica a l'I-CSCF que l'usuari no és accessible.

3.2.2. SLF (*subscriber location function*)

Normalment, un operador distribueix la informació dels subscriptors en múltiples HSS. En una xarxa amb aquesta característica, ni l'I-CSCF ni l'S-CSCF no coneixen en quina d'aquestes HSS està la informació que necessiten consultar. Per tant, han de contactar primer amb l'SLF.

Interfície Dx

És utilitzada per l'S-CSCF i l'I-CSCF per a consultar a l'SLF sobre la localització de l'HSS que conté la informació de subscripció d'un usuari. 3GPP recomana Diameter per a implementar-la (TS 29.229).

L'SLF ha de proveir una funcionalitat d'encaminat que permeti que altres entitats descobreixin quin node HSS conté la informació de subscripció d'un determinat usuari (que proporciona l'IMPU), atorgant a l'operador la flexibilitat de distribuir els seus usuaris lliurement entre diverses HSS. Llavors cal la implementació d'una entitat funcional com la de l'SLF i dels seus punts de referència anomenats Dx (connexió amb S-CSCF i I-CSCF) i Dh (connexió amb servidors d'aplicacions).

Interfície Dh

És utilitzada per l'AS per a consultar al SLF sobre la localització de l'HSS que conté la informació de subscripció d'un usuari. 3GPP recomana Diameter per a implementar-la (TS 29.328).

3.3. Mecanismes de garantia de recursos i QoS en xarxa de transport

En les xarxes NGN s'han especificat dos mecanismes de reserva de recursos que s'apliquen tant a la xarxa d'accés com a troncal de transport: mode *push* i mode *pull*.

Mode *push*

La Figura 11 ens mostra pas a pas un exemple del procés de reserva de recursos i garantia de QoS corresponent al mode *push*, i en concret d'una trucada de VoLTE. Cal tenir en compte que, seguint l'ordre dels passos, la reserva es dispara des de la capa de control de servei (en aquest cas el nucli IMS), amb el P-CSCF si és la xarxa d'accés i es tradueix posteriorment en la instal·lació de polítiques de QoS (en el cas de LTE, regles PCC) sobre la capa de processament de transport.

Negociació de paràmetres multimèdia de trucada

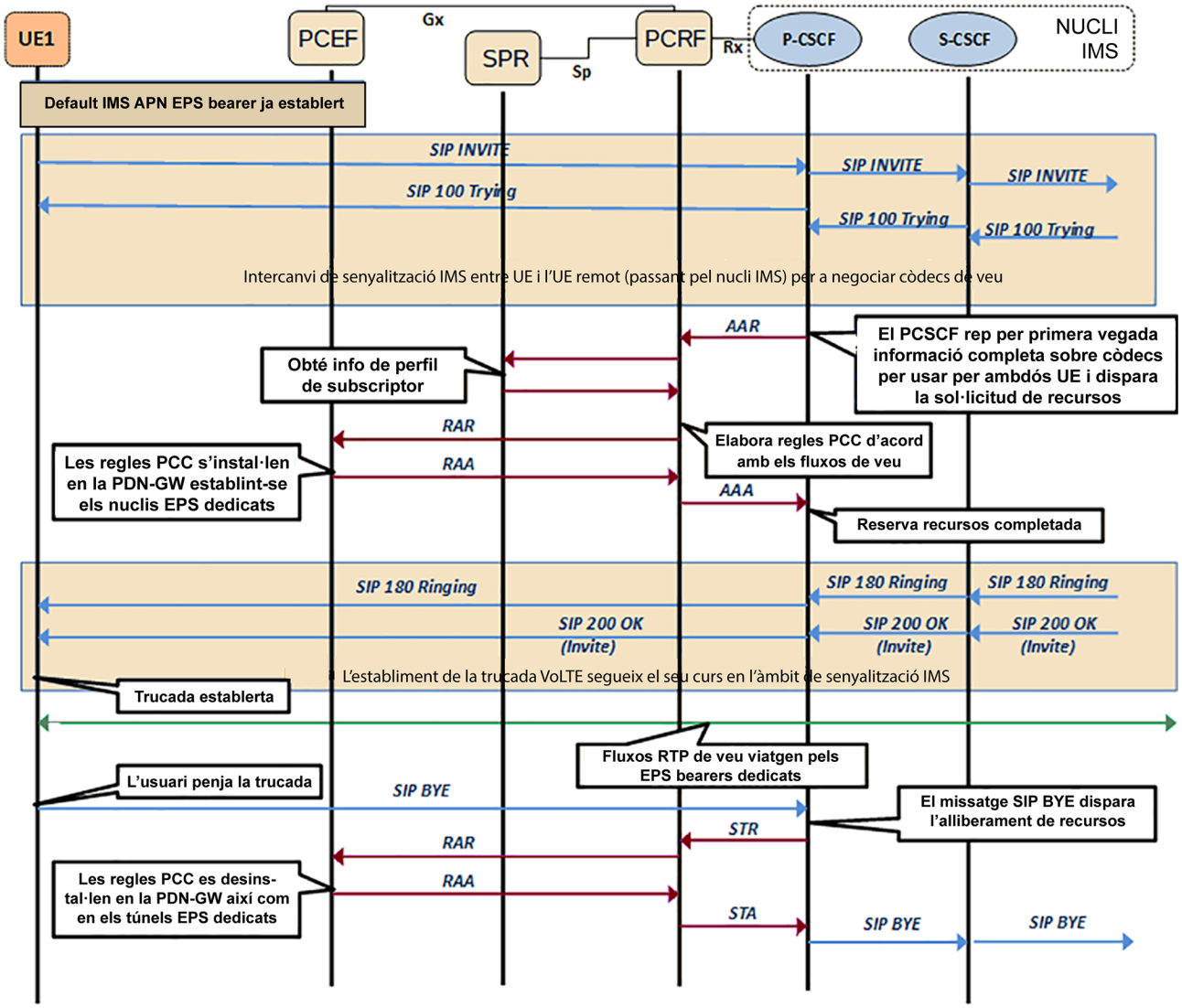
La informació de negociació de paràmetres multimèdia per a la comunicació (còdecs de veu i vídeo, ports UDP a usar, etc.) es fa amb el protocol SDP, el qual és integrat en alguns dels missatges SIP intercanviats durant l'establiment de la trucada. Aquests paràmetres els proposen sempre els UE.

Entre el P-CSCF (capa de servei) i el PCRF (en la capa de transport) la interfície de control està basada en Diameter i l'especificació de 3GPP l'anomena Rx (3GPP TS 29.214). En aquesta figura veureu que el P-CSCF, després d'haver avaluat la negociació dels còdecs de veu entre tots dos UE (feta amb el protocol SDP), extreu aquesta informació i l'envia en un missatge AAR (*authorization authentication request*) al PCRF. Esperarà fins que aquest li respongui amb un AAA (*authorization authentication answer*) per saber si la reserva sol·licitada ha acabat reeixidament o no per a continuar encaminant els missatges SIP de la trucada o cancel·lar-la directament (enviant a tots dos extrems de la trucada un missatge de SIP CANCELL).

El PCRF, abans de respondre l'AAR enviat pel P-CSCF, haurà d'avaluar la informació de perfil de l'usuari en l'àmbit de capa de transport per a decidir si instal·la una regla PCC o no en el PCEF (PDN-GW). En cas afirmatiu, enviarà un missatge Diameter RAR (*re-auth request*) via interfície Gx (3GPP TS 29.212)

sol·licitant la instal·lació de la regla PCC i esperarà la resposta (afirmativa o negativa) en el missatge RAA (*re-auth answer*) sobre el procediment d'instal·lació de la regla.

Figura 11. Exemple de mecanisme de reserva de recursos en mode *push*.



Mode *pull*

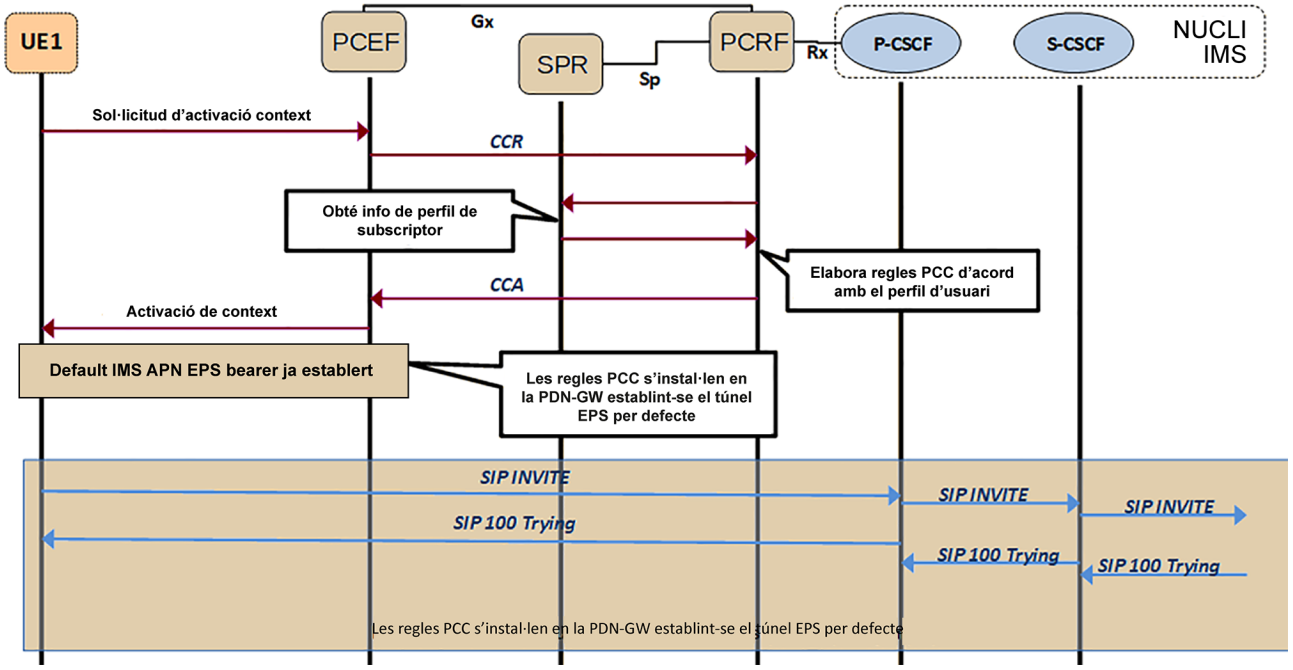
La Figura 12 ens mostra pas a pas un exemple del procés de reserva de recursos i garantia de QoS corresponent al mode *pull*, en concret quan un UE s'encén i s'adhereix a la xarxa LTE iniciant una sessió EPS.

Mode *pull*

Un UE pot també iniciar la reserva de recursos durant l'establiment d'una trucada VoLTE mitjançant la sol·licitud d'establiment d'un túnel EPS dedicat per a la veu.

Quan el PCEF rep la sol·licitud des de l'UE, aquest dispara una petició d'instal·lació d'una regla PCC al PCRF, el qual consulta el perfil d'usuari en l'àmbit de transport i pren les decisions pertinents sobre l'establiment de la regla PCC que possibilita l'establiment del túnel EPS per defecte associat a l'APN IMS. Aquesta sol·licitud es fa via interfície Gx i amb un intercanvi de missatges CCR/CCA (*credit control request / credit control answer*) entre el PCEF i el PCRF.

Figura 12. Exemple de mecanisme de reserva de recursos en mode *pull*.



Els missatges CCR també s'usen per a transmetre esdeveniments al PCRF relacionats amb la connectivitat de l'UE (per exemple, si l'UE s'ha apagat) i l'*accounting* d'un servei en concret. El PCRF pot, d'una banda, retransmetre aquests esdeveniments al P-CSCF (sempre que aquest l'hagi sol·licitat en la sol·licitud de recursos en *mode push*) i, de l'altra, prendre decisions sobre alteracions en les regles PCC afectades per aquest esdeveniment (pot disparar fins i tot la desinstal·lació de regles PCC).

Transmissió d'esdeveniments

Els missatges CCR/CCA estan definits tant en l'especificació de la interfície Rx com en la del Gx. En aquest últim s'usa tant per a sol·licitar reserva de recursos en mode *pull* com per a transmetre esdeveniments.

3.4. Protocols bàsics emprats en les xarxes NGN i IMS

Tal com hem vist en les descripcions dels punts de referència en apartats anteriors, els protocols que dominen la capa de servei són SIP i Diameter. En aquest apartat veurem les característiques principals de cadascun.

3.4.1. Protocol SIP

Session initiation protocol (SIP, protocol d'iniciació de sessió) és un protocol de senyalització definit pe IETF (*Internet Engineering Task Force*) que permet establir, alliberar i modificar sessions multimèdia (RFC3261). Aquest protocol hereta certes funcionalitats dels protocols HTTP, utilitzats per a navegar sobre la WEB i SMTP, per transmetre missatges electrònics (*e-mails*). SIP recolza sobre un model transaccional client-servidor com a HTTP. Com en SMTP, el format d'un missatge SIP està basat en capçaleres (*headers*), les quals estan expressades en text. El protocol SIP es pot usar sota TCP, UDP o SCTP.

Per a temes d'adreçament, SIP utilitza el concepte *uniform resource identifier* o SIP URI, el qual és semblant a una adreça de correu electrònic (usuari@domini.com). Llavors cada participant en una xarxa SIP és localitzable per mitjà d'una SIP URI.

És important remarcar que SIP és un protocol de senyalització per a iniciar, modificar i alliberar sessions multimèdia, però no és un protocol de reserva de recursos i, en conseqüència, no pot per si sol assegurar la qualitat de servei d'extrem a extrem. Es tracta d'un protocol de control de trucada i no de control del mitjà. Tal com hem dit, empra el protocol SDP (*session description protocol*) per a intercanviar paràmetres de capacitat i dels usuaris en termes de codificació i amplada de banda dels fluxos multimèdia que s'intercanviaran. Aquests fluxos recolzen en el protocol RTP/RTCP (*real time protocol / real time control protocol*).

A continuació veurem les entitats que defineix el protocol SIP. Aquestes entitats descriuen els actors que poden aparèixer en tota comunicació SIP. Posteriorment veurem com són els missatges SIP juntament amb els tipus de peticions i respostes que especifica el protocol. Finalment veurem les extensions a l'especificació SIP d'IETF que IMS ha introduït.

Entitats SIP

SIP defineix dos tipus d'entitats: els clients i els servidors. Més concretament, les entitats definides per SIP són:

- **Servidor intermediari** (*proxy server*). Rep sol·licituds de clients que ell mateix tracta o encamina cap a altres servidors després d'haver fet certes modificacions sobre aquestes sol·licituds. Aquest element es troba implementat en diversos elements del nucli IMS, com P-CSCF, I-CSCF, S-CSCF, I-CSCF i, en definitiva, en qualsevol element que s'encarregui d'encaminar missatges SIP.

- **Servidor de redirecció** (*redirect server*). Es tracta d'un servidor que accepta sol·licituds SIP, tradueix l'adreça SIP de destinació en una o diverses adreces de xarxa i les retorna al client. De manera contrària al servidor intermediari, el *redirect server* no encamina les sol·licituds SIP. En cas de la devolució d'una trucada, el servidor intermediari té la capacitat de traduir el número del destinatari en el missatge SIP rebut a un número de reexpedició de trucada i encaminar la trucada a aquesta nova destinació de manera transparent per al client d'origen; per al mateix servei, el *redirect server* retorna el nou número (número de reexpedició) al client d'origen, que s'encarrega d'establir una trucada a aquesta nova destinació.

- **Agent usuari** (*user agent*, UA). Es tracta d'una aplicació sobre un equip d'usuari que emet i rep sol·licituds SIP. En un context IMS, aquest element

estaria localitzable, per exemple, en un UE en mode de client SIP o també en un MGCF en què la trucada SIP es transforma en una trucada a RDSI o RTC.

- **Enregistrador** (*register*). Es tracta d'un servidor que accepta les sol·licituds SIP REGISTER. SIP disposa de la funció de registre dels usuaris. L'usuari indica, amb un missatge REGISTER emès a l'enregistrador, l'adreça on és localitzable (adreça IP). Llavors l'enregistrador actualitza una base de dades de localització. El registrador és una funció associada a un servidor intermediari o a un *redirect server*. Un mateix usuari pot registrar-se sobre diferents UA SIP; en aquest cas, la trucada li serà lliurada sobre el conjunt d'aquestes UA. Aquest element es trobaria implementat en l'S-CSCF en el nucli IMS, i la base de dades de localització seria implementada en l'HSS.

Missatges SIP

A continuació veurem quin tipus de missatges i quines funcions exerceixen en l'especificació del protocol SIP. Primer donarem un cop d'ull a l'estructura típica de la capçalera SIP i els tipus de peticions i resposta que preveu l'especificació.

Capçalera SIP

Un missatge SIP és compost per una sèrie de camps, tots basats en text. L'ordre en què apareixen és indistint i, fins i tot, un mateix camp pot aparèixer diverses vegades contenint valors diferents. En SIP, quan hi ha més d'un camp repetit, sí que pot importar en quin ordre apareixen els camps introduïts.

A continuació mostrem un exemple d'una capçalera SIP (sense capçalera SDP):

```
INVITE sip:bob@iptel.org SIP/2.0
Via: SIP/2.0/UDP 176.54.75.23:5040;rport
Max-Forwards: 10
From: "jiri" <sip:jiri@iptel.org>;tag=76ff7a07-c091-4192-84a0-
d56i91fe104f
To: Bob <sip:bob@iptel.org>
Call-ID: d10815i0-bf17-4afa-8412-d9130a793d96@176.54.75.23
CSeq: 2 INVITE
Contact: <sip:jiri@176.54.75.23:5040>
User-Agent: Windows RTC/1.0
Proxy-Authorisation: Digest username="jiri", realm="iptel.org",
algorithm="MD5", uri="sip:jiri@bat.iptel.org",
nonce="3cef753900000001771328f5ae1b8b7f0d742dóna1feb5753c",
response="53fe98db10i1074
b03b3i06438bda70f"
```

```
Content-Type: application/sdp
Content-Length: 451
v=0
o=jku2 0 0 IN IP4 176.54.75.23
s=sesión
...
```

En la primera línia trobem la paraula *INVITE*, que és el nom del mètode SIP del missatge. En aquest cas es tracta d'un missatge del tipus petició (*request*) per a l'inici de sessió. En el subapartat següent podeu veure la resta de mètodes SIP que existeixen. En lloc del mètode, també hi pot anar el codi o número quan es tracta d'un missatge de resposta. Els codis de resposta els podeu trobar més endavant. A continuació apareix un SIP URI representant el destinatari d'aquest missatge (se l'anomena *request* URI). En aquest cas es tracta de l'equip amb *hostname* iptel.com.

Una petició SIP pot contenir un o més camps Via:, que són usats per a registrar el camí que aquesta petició fa fins a la destinació. Després són usats per a encaminar les respostes exactament de la mateixa manera. En l'exemple veiem que hi ha un sol camp Via:, que ens diu que el client SIP (anomenat també *user agent*) s'executa en un PC amb IP 176.54.75.23 i usa el port 5040.

Els camps *From:* i *To:* contenen, igual que en SMTP, identificadors de l'originador de la petició (usuari que truca) i el destinatari (usuari trucat).

El camp Call-ID: és un identificador del diàleg SIP i la seva funció és identificar missatges pertanyents a la mateixa trucada.

El camp CSeq: és usat per a mantenir l'ordre de les peticions. S'utilitza en les respostes també per a identificar a quina petició fa referència.

La capçalera Contact: conté l'adreça IP i el port sobre el qual el sol·licitador espera peticions posteriors enviades per l'usuari trucat.

Les altres capçaleres de l'exemple no són importants i no val la pena descriure-les. No obstant això, el protocol SIP preveu altres capçaleres com Route: o Record Route:, que indiquen informació d'encaminament (salt a salt) del missatge SIP.

La capçalera Message: és delimitada en el cos del missatge per una línia buida. El contingut del cos del missatge pot ser un altre protocol que aporta informació addicional sobre la sessió. Exemples d'aquests protocols són SDP (*session description protocol*) i XML.

Mètodes SIP

Els mètodes SIP poden dividir-se en dos tipus: peticions i respostes. A continuació es mostra una llista de les peticions:

Taula 2. Mètodes SIP (peticions).

Mètode	Descripció
INVITE	És enviat del terminal UA que truca a l'UA trucat. Indica que un client és convidat a participar en una sessió de trucada.
ACK	Confirma que el client ha rebut una resposta final a una petició INVITE (resposta amb codis 2xx, 3xx, 4xx, 5xx i 6xx). No es rep resposta en enviar un ACK.
BYE	És enviat pel qui truca o el trucat per acabar una sessió.
CANCELL	Cancel·la qualsevol petició pendent de resposta o qualsevol transacció.
OPTIONS	Sol·licita a un altre UA o a un servidor intermediari les capacitats que tenen (els mètodes suportats, els tipus de continguts, les extensions, els còdecs, etc. sense haver de provocar el «ringing» de l'altra part).
REGISTER	És usat per un UA per a notificar a una xarxa SIP de la seva adreça IP actual (*Contact URI* en la capçalera) i de l'URI als quals s'hauria d'encaminar les peticions.
PRACK	ACK provisional. És com un ACK per a respostes provisionals amb codi 1xx (RFC 3262).
SUBSCRIBE	És una subscripció a un esdeveniment de notificació enviada des d'un notificador (RFC 3265).
NOTIFY	És usat per a notificar a les entitats subscriptores un esdeveniment d'actualització de registre (RFC 3265).
PUBLISH	És enviat per un client per publicar un esdeveniment a un servidor intermediari.
INFO	Envia informació a meitat de sessió que no modifica l'estat d'aquesta sessió (RFC 2976). Entre els exemples d'informació, hi ha els dígits DTMF, les informacions relatives a la taxació d'una trucada, etc.
REFER	Un UA el pot usar per a instar a un altre UA que iniciï una petició SIP (normalment un SIP INVITE) cap a un tercer UA. Permet emular diferents serveis o aplicacions incloent la transferència de trucada (RFC 3515).
MESSAGE	Transporta missatges instantanis de text usant SIP. El missatge SIP MESSAGE pot transportar diversos tipus de continguts basant-se sobre la codificació MIME (RFC 3428).
UPDATE	Modifica l'estat de la sessió sense canviar l'estat del diàleg SIP. Permet a un client SIP actualitzar els paràmetres d'una sessió multimèdia (fluxos multimèdia i els seus còdecs). El mètode UPDATE pot ser enviat abans que la sessió hagi estat establerta (RFC 3311), és a dir, abans de rebre el 200 OK corresponent al SIP INVITE que ha iniciat la sessió.

Respostes SIP

Una resposta és enviada per un servidor SIP a un client i té l'estructura següent:

```
SIP VERSION (space) STATUS CODE (space) EXPLANATION
```

L'STATUS CODE és un codi numèric usat pel receptor per a identificar l'estatus de la petició. Està format per tres dígits seguits per una descripció textual del codi.

L'STATUS CODE és dividit per 6 famílies diferents, en què el primer dígit indica la classe de codi tal com és mostrat en la taula següent.

Taula 3. Mètodes SIP (respostes).

Codi	Descripció	Exemple
1xx	Respostes provisionals/informacionals	100 Trying, 180 Ringing
2xx	Respostes reeixides	200 OK
3xx	Respostes de redirecció	302 Moved Temporarily, 305 Use Proxy
4xx	Respostes d'error de client	401 Unauthorized, 408 Request Timeout
5xx	Respostes d'error de servidor	500 Server Internal Error, 503 Service Unavailable
6xx	Respostes d'error globals	600 Busy Everywhere, 603 Decline

Extensions per a IMS

El protocol SIP va ser triat pel 3GPP com a base per a senyalitzar IMS. No obstant això, hi havia molts buits entre el protocol SIP de base definit per IETF i les característiques requerides per a suportar les prestacions d'IMS per complet. Per a resoldre aquest problema, 3GPP va definir dotzenes d'extensions SIP específiques per a xarxes IMS. Col·lectivament, aquestes extensions comprenen el protocol SIP IMS definint un perfil propi de SIP. El protocol SIP IMS és definit en l'estàndard del 3GPP TS 24 229.

Aquestes extensions, com el control de trucada estès, la presència o la missatgeria instantània, estenen la funcionalitat de SIP sobre les xarxes IMS. Aquest nou perfil d'ús del protocol SIP per a IMS representa el més important en la indústria de les telecomunicacions i és, de manera exclusiva, el més apropiat per a les xarxes NGN.

Per a il·lustrar la complexitat inherent del SIP IMS i totes les seves extensions, veurem per sobre les extensions més importants:

1) SigComp. Defineix com comprimir les dades en text de la senyalització SIP, les quals poden ser molt extenses i problemàtiques de transmetre, causant retards. SigComp soluciona els reptes de retards d'anada i tornada de la senyalització, i la vida de la bateria dels UE mòbils. Es pot trobar més informació sobre SigComp en l'RFC 3320.

2) Capçaleres privades (*P-headers*). A més de les capçaleres estàndard, 3GPP va definir capçaleres addicionals dirigides a solucionar problemes específics de la xarxa IMS, com obtenir informació sobre la xarxa d'accés i la xarxa visitada (en itinerància), i també determinar la identitat del qui truca. Es pot trobar més informació sobre els *P-headers* en els RFC 3455 i RFC 3325.

3) Negociació en l'àmbit de seguretat (*security agreement*). Especifica com negociar les capacitats de seguretat per a molts tipus de terminal. Es pot trobar més informació sobre *security agreement* en l'RFC 3329.

4) AKA-MD5. Determina com terminals i xarxes són autenticats utilitzant mecanismes ja definits (per exemple, ISIM) i intercanvi de claus específiques. Es pot trobar més informació sobre AKA-MD5 en l'RFC 3310.

5) IPsec.[1]. És utilitzat en diverses interfícies IMS (com el Gm) entre diferents xarxes IMS per a garantir confidencialitat i integritat de les dades. IMS usa IPsec en mode transport, en oposició a l'estàndard usat en serveis VPN.

(1)Un enllaç IPsec entre dos terminals es pot establir en dos modes: mode túnel per a VPN *site-to-site* o *LAN-to-LAN*, i mode transport per a connectar un amfitrió amb un altre amfitrió que exerceix de concentrador de VPN. Aquestes VPN es diuen VPN en mode accés remot.

6) Autorització de mitjans (*media authorization*). S'assegura que solament els recursos de mitjans autoritzats són utilitzats. Es pot trobar informació més detallada en l'RFC 3313.

7) Registre en mobilitat (*mobile registration*). En xarxes IMS, el procés de registre del terminal és més complicat, ja que inclou diverses extensions de seguretat i ha de gestionar registres des d'una xarxa visitada. En l'RFC 3608 i l'RFC 3327 es defineix la sintaxi i l'ús per part de les entitats SIP de les capçaleres *service-route* i *path*.

8) *Reg-event package*. És usat pel terminal i el P-CSCF per a saber l'estatus de registre del terminal a la xarxa. IMS IPv6 prefereix xarxes IPv6, que ofereixen diferents avantatges. Permet un rang més ampli d'adreces i conté funcionalitat IPsec integrada que pot eliminar la necessitat de tallafocs i NAT per a les entitats. Se'n pot trobar informació més detallada en l'RFC 3680.

9) Precondicions (*preconditions*). Especifica un mètode de negociació de QoS, seguretat i altres comportaments de trucada entre dos terminals. Se'n pot trobar informació més detallada en l'RFC 4032.

10) Reserva de recursos IMS. Especifica com fer reserva de recursos per a trucades de telèfon o sessions. Se'n pot trobar més informació en l'RFC 3312.

11) SDP (*session description protocol*). l'SDP defineix el procés de negociació bàsica per als fluxos de mitjans i inclou el còdec i amplada de banda que cal usar, i també altres atributs. IMS estén l'SDP fins i tot amb més extensions, com l'agrupació de fluxos, QoS i atributs de precondicions, suport de còdec suplementaris i modificadors d'amplada de banda.

A continuació posem un exemple en el qual cal destacar la línia m=, a partir de la qual es descriu un component multimèdia amb atributs (a=):

```
v=0
o=jku2 0 0 IN IP4 213.20.128.35
s=sesión
c=IN IP4 213.20.128.35
b=CT:1000
t=0 0
m=audio 54742 RTP/AVP 97 111 112 6 0 8 4 5 3 101
a=rtpmap:97 red/8000
a=rtpmap:111 SIREN/16000
a=fmtp:111 bitrate=16000
a=rtpmap:112 G7221/16000
a=fmtp:112 bitrate=24000
a=rtpmap:6 DVI4/16000
a=rtpmap:0 PCMU/8000
a=rtpmap:4 G723/8000
a=rtpmap: 3 GSM/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
```

12) XML. La senyalització de SIP IMS usa els protocols XML, incloent XCAP, per a implementar diversos tipus de continguts de missatges SIP i permetre interfícies de funcionalitat completa entre les entitats IMS.

13) Extensions IMS SIMPLE. El SIMPLE és un grup de treball d'IETF que defineix els requeriments en senyalització dels serveis de presència i missatgeria instantània. Les definicions bàsiques de SIMPLE van ser inadequades per a les aplicacions d'IMS perquè no eren prou eficients per a ser usades en un enllaç sense fil. SIP IMS van estendre aquest estàndard amb això: publicacions i notificacions parcials; filtratge de notificacions, i llista de recursos.

3.4.2. Protocol Diameter

El protocol Diameter deriva del protocol RADIUS amb moltes millores en diferents aspectes, com la gestió d'errors i la fiabilitat de lliurament de missatges. Utilitza l'essència del protocol AAA de RADIUS i defineix una sèrie de missat-

ges bàsics definits en la recomanació Diameter Base Protocol (RFC3588). Diameter és usat en IMS per a intercanviar informació relacionada amb tasques d'AAA (*authentication, authorization, accounting*).

Amb el Diameter Base Protocol, es poden implementar aplicacions de gestió d'AAA, i de fet IMS ho fa així. Per exemple, quan diem que un punt de referència entre un S-CSCF i l'HSS és el Cx, significa que l'aplicació que s'implementa amb el protocol Diameter és precisament el Cx, el qual inclourà els seus mateixos missatges de petició-resposta i els paràmetres (anomenats *attribute-value pair* o AVP) que els componen. I així es dona amb totes les interfícies basades en Diameter que hem esmentat en aquest document.

Per exemple, la interfície Rx, com a aplicació que és, té un identificador associat (*application ID*) que és únic i té uns missatges (també anomenats ordres) ben definits per a escometre la seva funció. Cada missatge conté una llista d'AVP que en defineixen el contingut. Aquesta especificació de l'aplicació ha d'estar recollida en un document, que en el cas de l'Rx és el 3GPP TS 29 214.

El protocol Diameter es pot basar en TCP o en SCTP.

Nodes i agents Diameter

El protocol Diameter és dissenyat per a arquitectures d'igual a igual. Cada amfitrió que implementa el protocol Diameter pot actuar com a client o servidor depenent del desplegament de la xarxa. Així, doncs, el terme ***node*** de Diameter es refereix a un client, a un servidor o a un agent de Diameter.

En un entorn en el qual els usuaris estableixen connexions punt a punt amb un NAS (servidor d'accés a la xarxa), el NAS és el client Diameter pel que fa al servidor d'autenticació, el qual és el *Diameter server*. És a dir, que el NAS rep un missatge de petició de connexió d'usuari i, gràcies al node Diameter que té el NAS, aglutina la informació de credencials de l'usuari i la envia en un missatge de petició d'autenticació al servidor Diameter, que processa el missatge. Aquest servidor envia un missatge de resposta amb el resultat de l'autenticació (sia satisfactòria o no) al client.

En les transaccions amb missatges Diameter hi ha, com en SIP, el concepte de domini, el qual va sempre especificat en tots els missatges Diameter. Aquesta informació de domini ajuda els nodes a processar-los d'una manera o altra.

Hi ha un tipus especial de node de Diameter anomenat agent. Hi ha quatre tipus d'agents:

- ***Relay agent***. S'usa per a traspassar un missatge a la destinació apropiada depenent de la informació continguda en el missatge (domini de destinació).

- ***Proxy agent***. S'usa per a traspassar missatges a la destinació apropiada (encara que sigui un altre domini), però, a diferència del *relay agent*, pot modificar el contingut del missatge i, per tant, proporcionar serveis de valor afegit, aplicar regles o fer tasques administratives en un domini específic.

- ***Redirect agent***. Actua com un repositori de configuració centralitzat per a altres nodes Diameter. Quan rep un missatge, examina la seva taula de rutes i retorna un missatge de resposta juntament amb informació de redirecció al node que ha enviat la petició. Això és molt útil perquè un node no hagi d'emmagatzemar una llarga llista de rutes.

- ***Translation agent***. Converteix un missatge d'un protocol AAA a un altre (per exemple, de Radius a Diameter).

Missatges Diameter

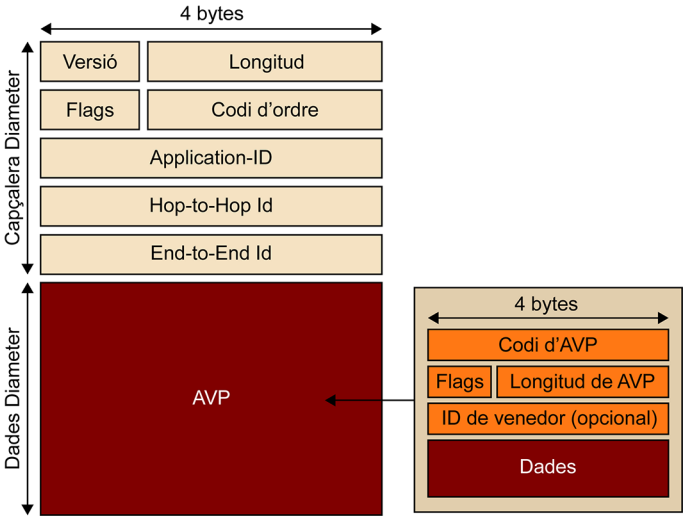
Un missatge Diameter és la unitat base per a enviar una ordre o lliurar una notificació a altres nodes Diameter. Depenent de l'aplicació a implementar, el protocol Diameter ha definit diversos tipus de missatges, que són identificats pel seu codi d'ordre.

Com que l'intercanvi de missatges és síncron en Diameter, cada missatge té la seva contrapart corresponent (petició-resposta), que comparteix el mateix codi d'ordre.

Per exemple, el Diameter Base Protocol defineix el CER (*capability-exchange-request*) i la CEA (*capability-exchange-answer*), i tots dos tenen el mateix codi, amb la diferència d'un *flag* de *request* activat o no. A més, l'intercanvi de CER/CEA ha de ser dut a terme entre dos nodes Diameter per a intercanviar informació d'aplicacions suportades per tots dos.

El codi d'ordre indica la intenció del missatge, però les dades reals que porta a l'interior són continguts en un grup de parells atribut-valor o AVP (*attribute-value-pair*) en anglès. El protocol Diameter fixa una llista d'AVP fixos comuns i imposa, per cada AVP, una semàntica corresponent. Aquests AVP porten els detalls de la informació d'AAA i encaminament, seguretat i capacitats entre dos nodes. A més, cada AVP s'associa amb un AVP *data format*, que és definit en el Diameter Base Protocol (per exemple, OctetString, Integer32), amb el qual cada AVP ha de seguir el format de dades concret. La Figura 13 mostra els camps que componen un missatge de Diameter.

Figura 13. Camps de missatge Diameter i AVP.



Cada AVP té un codi que identifica el tipus d'informació que conté. Si hi ha dos AVP definits amb el mateix codi, la manera de diferenciar-los és amb el *vendor ID*, que indica l'identificador del fabricant o entitat que ha definit aquest AVP (es tracta d'un identificador assignat per la IANA[2]).

(2)L'ETSI o 3GPP tenen el seu identificador de la IANA: 13019 i 10415 respectivament.

Hi ha una sèrie d'AVP que han d'existir per a facilitar l'encaminament cap al node destinació.

Segons l'especificació de l'aplicació de Diameter a implementar, s'indicarà un valor en el camp d'*application-ID*[3] o un altre (assignat també per la IANA).

(3)Per a la interfície Rx, l'*application-ID* és 16777236.

Entitats d'estandardització com 3GPP

Les entitats d'estandardització, com 3GPP, han publicat documentació en la qual descriuen totes les interfícies basades en Diameter que apareixen en les seves especificacions, on se'ls assigna un *application-ID*. En aquests documents es proposen totes les ordres que formen la interfície i, per cada ordre, depenent de si és *request* o *answer*, es defineixen tots els AVP.

Exemple

Per exemple, es necessita l'AVP *destination-host* (codi AVP 293) i el *destination-realm* (codi AVP 283). Aquests AVP estan definits en l'RFC 3588 com a Diameter Base Protocol (amb la qual cosa el *vendor ID* és 0).

3.5. Exemples de fluxos de trucades IMS

Per tal d'afermar els conceptes explicats fins ara, donem dos exemples típics de senyalització IMS. En aquests exemples es veu més clara la interacció entre el nucli IMS i les entitats de control d'admissió i recursos de la subcapa de control de transport en la garantia de QoS d'extrem a extrem.

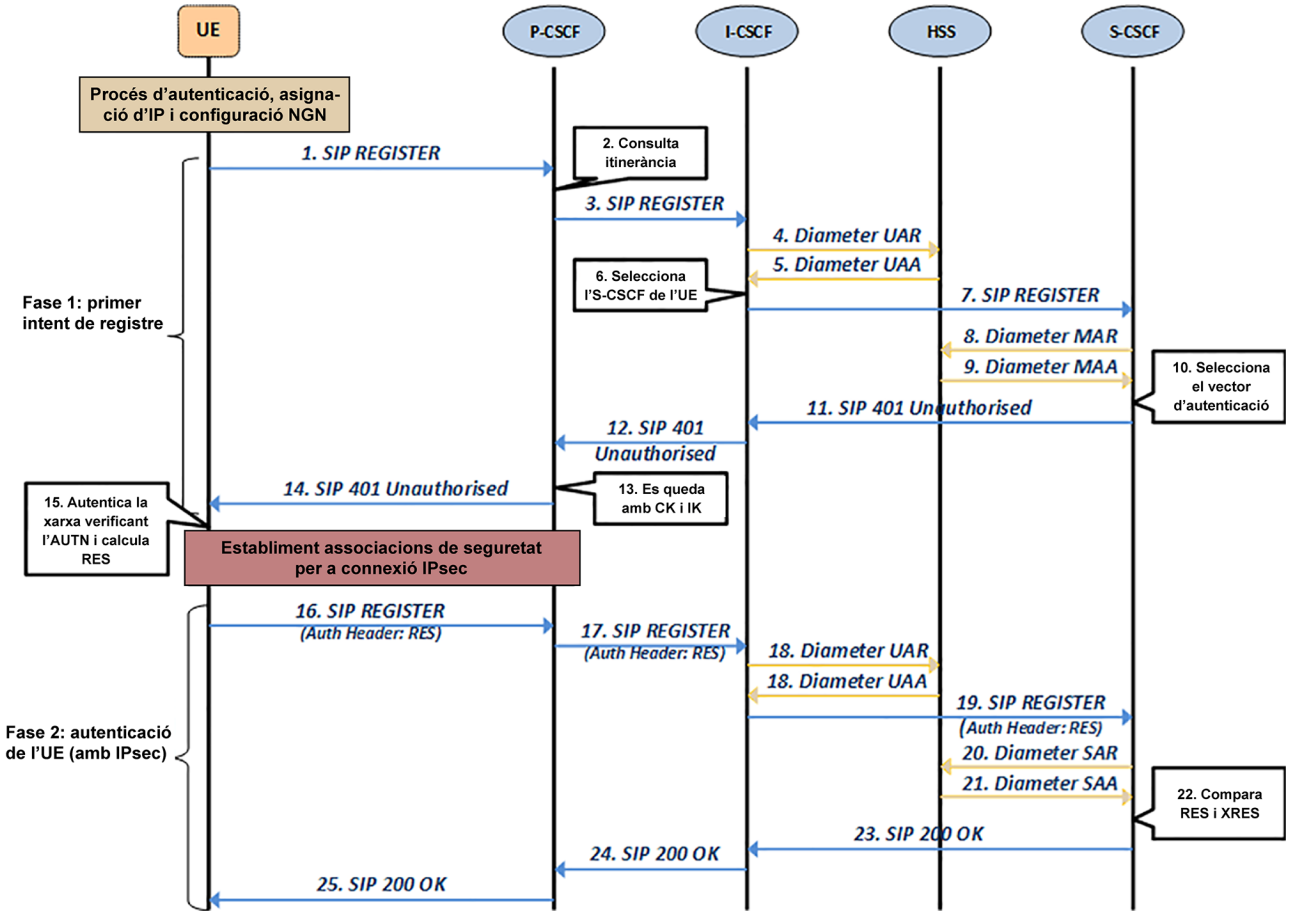
Els tres exemples que veurem són els descrits a continuació:

1) Registre en el nucli IMS.
2) Establiment d'una trucada de veu mitjançant dos nuclis IMS per a veure la interacció entre dos dominis.
3) Interacció amb un servidor d'aplicacions (AS), en aquest cas amb un servei de presència en IMS.

3.5.1. Registre en el nucli IMS

Seguidament veurem el procés de registre en el nucli IMS missatge a missatge.

Figura 14. Pas a pas del registre en el nucli IMS.



Pas 1. L'UE (client IMS) envia un missatge SIP REGISTER cap a la IP del P-CSCF, que el seu *hostname* ha rebut en la fase d'adhesió a la xarxa d'accés (per exemple, LTE). La IP el descobreix via consulta de DNS. Hi afegeix la capçalera Via: amb el seu *hostname* per dir que el missatge ha passat per ell.

Pas 2. El P-CSCF rep el SIP REGISTER i, gràcies a la capçalera Contact:, coneix l'adreça IP assignada a l'UE. També observa en el contingut el domini del SIP URI de l'usuari. Això li indica si l'usuari està en itinerància o no. Si ho està, redirigeix el missatge a l'IBCF (via interfície Mw) del seu domini, que el connecta amb el domini destinació o amb un altre domini que faci de trànsit al domini destinació. En aquest exemple, no fa itinerància, amb la qual cosa ha de redirigir el missatge a un I-CSCF (el P-CSCF no coneix l'S-CSCF associat a l'UE) descobrint la seva adreça IP via DNS.

Pas 3. El P-CSCF afegeix al SIP REGISTER algunes capçaleres (per exemple, afegeix al Via: el seu *hostname* per notificar que el missatge ha passat per ell.

Pas 4. L'I-CSCF rep el SIP REGISTER i la seva funció és saber a quin S-CSCF del seu domini ha de reexpedir-lo. Per a saber-ho, envia una petició Diameter amb l'ordre *user authorization request* a l'HSS (via interfície Cx), on li sol·licita la llista de S-CSCF.

Pas 5. L'HSS contesta amb una *user authorization answer* incloent la llista de S-CSCF candidats i les seves capacitats.

Pas 6. De la llista rebuda des de la interfície Cx, l'I-CSCF selecciona un S-CSCF basat en les seves capacitats. També afegeix una altra capçalera Via: amb el seu *hostname*.

Pas 7. L'I-CSCF fa el reenviament al S-CSCF seleccionant el SIP REGISTER.

Pas 8. L'S-CSCF s'adona que el missatge SIP REGISTER no inclou informació d'autenticació. Consulta l'HSS per la interfície Cx sobre informació per a l'autenticació de l'UE usant l'ordre *multimedia authentication request*.

Pas 9. L'HSS respon amb una *multimedia authentication answer* incloent *random number* (RAND), *authentication token* (AUT), *signed result* (XRES), *cipher key* (CK) i *integrity key* (IK).

Pas 10. L'S-CSCF selecciona l'*authentication vector* (format pels cinc paràmetres anteriors) a usar per a autenticar l'UE.

Pas 11. L'S-CSCF afegeix l'*authenticacion vector* al missatge de resposta al SIP REGISTER d'error d'autenticació (codi 401) incloent en la capçalera www-Authenticate: els paràmetres de l'*authentication vector*. El missatge de resposta viatjarà pels mateixos nodes que inclogui en totes les capçaleres Via: rebudes. Així, el missatge es reenvia a l'I-CSCF.

Pas 12. El missatge de resposta 401 passa al P-CSCF.

Pas 13. Aquí el P-CSCF extreu de la capçalera www-Authenticate: el CK i i IK que usarà per a dur a terme les associacions de seguretat amb UE i establir una connexió IPsec. Elimina aquests dos paràmetres d'aquesta capçalera abans d'enviar el missatge.

Pas 14. Envia el missatge *401 Unauthorized* a l'UE per reptar-lo en l'autenticació.

Pas 15. L'UE, usant l'*authentication token* (AUT), autentica la xarxa i calcula amb les seves claus el paràmetre RES (que haurà de coincidir amb el paràmetre XRES en poder de l'S-CSCF). Les seves pròpies claus CK i IK són calculades amb els paràmetres rebuts en l'*authentication vector* (haurien de concordar amb les que té el P-CSCF).

Pas 16. L'UE envia el SIP REGISTER de nou al P-CSCF, però aquesta vegada ja xifrat per IPsec i incloent el valor calculat RES en la capçalera *authorization*.

Pas 17. El P-CSCF reenvia el missatge a l'I-CSCF.

Pas 18. L'I-CSCF sol·licita de nou a l'HSS que li presenti la llista de S-CSCF amb un intercanvi UAR/UAA.

Pas 19. L'I-CSCF reenvia el SIP REGISTER a l'S-CSCF seleccionat.

Pas 20. Sol·licita a l'HSS informació de subscripció de l'usuari que vol autenticar-se amb una ordre *server assignment request*.

Pas 21. L'HSS respon amb una *server assignment answer*.

Pas 22. Compara el valor RES rebut des de l'usuari amb el valor XRES. Si coincideixen, l'autenticació de l'usuari és correcta.

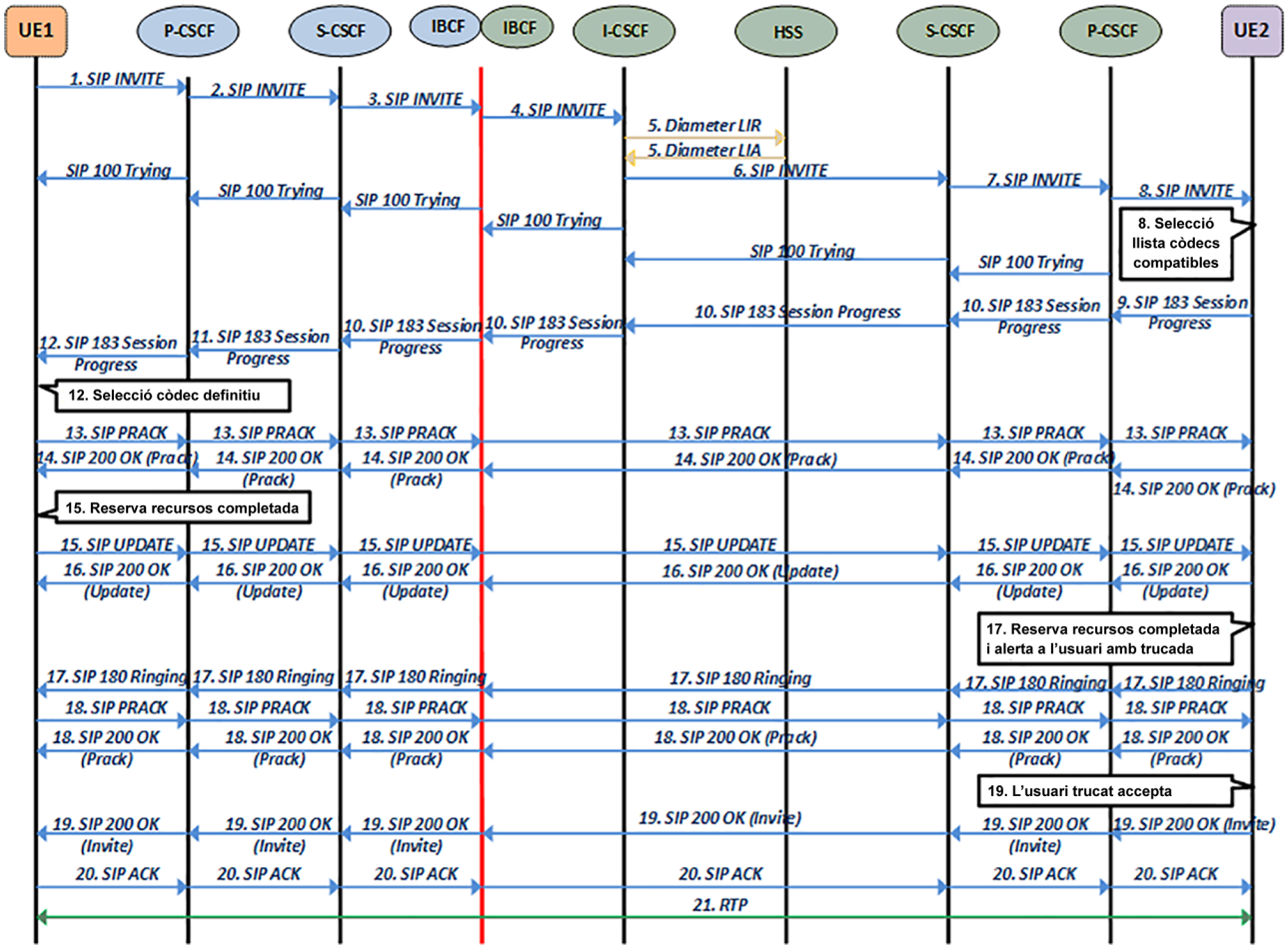
Pas 23 a 25. S'envia un missatge de resposta d'èxit (200 OK) indicant a l'UE una capçalera de tipus *service route:* amb el *hostname* de l'S-CSCF assignat en el registre (l'usarà l'UE per a establir sessions de servei). El P-CSCF aprofitarà per a registrar l'UE (i la seva adreça IP i identitats públiques registrades).

3.5.2. Establiment de sessions de servei

Seguidament veurem l'exemple de l'establiment d'una trucada de veu amb garantia de QoS d'extrem a extrem, en el qual tots dos interlocutors estan en dominis IMS diferents i s'ha implementat aquesta interconnexió amb els elements que especifica el model de 3GPP (l'IBCF).

La Figura 15 mostra els passos del flux de trucada d'establiment de sessió de veu entre dos clients SIP: l'UE 1 pertany a un domini IMS (blau) i l'UE 2 pertany a un altre domini IMS (verd).

Figura 15. Flux de trucada de veu en IMS.



Pas 1. L'UE1 (client IMS) inicia una sessió enviant un SIP INVITE cap al P-CSCF (és a dir, amb la IP de destinació del P-CSCF). Posa com a objectiu de la trucada la identitat pública de l'usuari després de l'UE 2 (del tipus SIP URI; usuari2@dominiverd.com). Afegeix al missatge SIP les capçaleres Contact: amb l'adreça IP i el port que usa l'UE 1 i Via: amb el seu *hostname*. També posa dues capçaleres Route:. La primera, potser no tan important, és per al *hostname* del P-CSCF (la posa per si de cas hi hagués un SIP proxy intermedi entre el P-CSCF i l'UE1) i la segona, per a indicar a quina S-CSCF ha d'anar el SIP INVITE (posa el *hostname* que ha obtingut del 200 OK en la fase de registre). També, i això és molt important, s'afegeix una capçalera SDP, en la qual l'UE1 proposa uns paràmetres de QoS inicials (*preconditions*) segons els còdecs que suporta per a veu. Recordem també que aquest missatge s'envia mitjançant la connexió IPsec entre l'UE 1 i el P-CSCF, establerta en la fase de registre.

Pas 2. El P-CSCF rep el SIP INVITE i comprova una de les capçaleres esteses per a IMS, incloses en el missatge (P-Preferred-Identity:), perquè coincideixi amb una de les identitats públiques registrades per l'usuari. Després llegeix la capçalera Route: i extreu el *hostname* de l'S-CSCF especificat. El resol via DNS i reenvia el SIP INVITE a l'S-CSCF. Abans d'enviar el missatge, el P-CSCF elimina la capçalera Route: que portava el seu mateix *hostname*, la capçalera P-Preferred-Identity: i afegeix una capçalera Via: amb el seu *hostname* per deixar mostra del camí recorregut pel missatge SIP fins ara. També afegeix una capçalera Record Route: per obligar que, si hi ha un missatge de tornada, aquesta passi pel P-CSCF.

Notificació enviament

En el pas 2, tan aviat com el P-CSCF reenvia el missatge SIP notifica a l'element adjacent (en aquest cas a l'UE) que el missatge ja s'ha tramitat, i ho fa amb una resposta del tipus 100 Trying. Això es repeteix per a tots els altres elements que processen la petició SIP INVITE en el camí.

Pas 3. L'S-CSCF rep el missatge i procedeix a encaminar el missatge SIP cap al domini destinació. És a dir, consulta la part de domini de la identitat pública de l'UE 2 i l'encamina cap a l'IBCF segons les seves rutes. L'S-CSCF elimina la capçalera Route: que conté el seu mateix *hostname*.

Domini IMS

Un domini IMS no cal que tingui un IBCF connectat amb tots els dominis existents. En el seu lloc, pot tenir un IBCF cap a un domini IMS «en trànsit» al domini destinació. Això és com una espècie de ruta per defecte, però en l'àmbit de dominis IMS destinació.

Pas 4. El missatge arriba a l'IBCF del domini blau, que s'encarrega d'eliminar del missatge totes les capçaleres que puguin donar pistes a altres dominis sobre la topologia del nucli IMS origen (capçaleres Via: sobretot). El SIP INVITE travessa la frontera entre dominis (possiblement amb una connexió IPsec entre IBCF) i arriba a l'IBCF del domini verd, el qual no sap en quina S-CSCF està registrat l'UE 2. Per això el reenvia a l'I-CSCF que tingui configurat perquè aquest se n'encarregui. Afegeix un Record Route: amb el seu *hostname* i el corresponent Via:.

Pas 5. L'I-CSCF del domini verd consulta al'HSS, via interfície Cx (Diameter; amb intercanvi d'ordres de tipus Location Information o LIR/LIA), a quina S-CSCF (*hostname*) cal enviar el SIP INVITE. Per això afegeix la capçalera Route: amb el *hostname* de l'S-CSCF destinació. També pot conèixer l'adreça IP de destinació mitjançant una consulta DNS i així pot reexpedir el missatge a la destinació.

Funcions de frontera entre dominis

En les versions de l'estàndard de 3GPP anteriors a la versió 7, era l'S-CSCF del domini origen (blau en el nostre exemple) el que s'encarregava de consultar el DNS per conèixer l'adreça IP de l'I-CSCF del domini destinació, que era qui feia les funcions de frontera entre dominis (verd, en el nostre exemple) i reexpedir així el SIP INVITE directament. Ara s'han inclòs els IBCF per fer aquesta funció (aportació de l'ETSI a l'estàndard de 3GPP).

Pas 6. L'S-CSCF del domini verd llegeix la identitat pública de l'UE 2 especificada per l'UE 1 en el missatge i comprova que està registrat. Si ho està, mapa aquesta identitat amb l'adreça IP i el port amb el qual l'UE 2 és registrat i la substitueix en el missatge. No obstant això, malgrat tenir la IP de l'usuari final, el missatge s'envia cap al P-CSCF corresponent (afegint la corresponent capçalera Route:). L'S-CSCF afegeix el Via: i un Record Route: amb el seu mateix *hostname*.

Pas 7. El P-CSCF del domini verd rep el missatge i aleshores poden succeir dues coses depenent dels mecanismes de reserva de recursos de la xarxa en què UE 2 és connectat: en mode *pull* el P-CSCF sol·licita al PCRF (en cas d'una xarxa d'accés LTE) un *authorization token* per incloure'l en el missatge a enviar a l'UE 2. En mode *push* el P-CSCF no sol·licita res al PCRF perquè solament

té la informació de QoS de l'UE i reenvia el missatge a l'UE 2. En tots dos casos, abans d'enviar el missatge (per la connexió IPsec corresponent) el P-CSCF inclou en la capçalera Via: el seu *hostname*.

Pas 8. L'UE 2 rep el SIP INVITE amb la proposta de còdec de l'UE 1. Llavors l'UE 2 selecciona d'aquesta llista els còdecs compatibles amb els suportats per ell, elabora una nova capçalera SDP amb aquests paràmetres i actualitza els paràmetres d'establiment de connexió RTP restants (IP i ports). Aquesta nova capçalera SDP amb els paràmetres preliminars acordats entre l'UE 1 i l'UE 2 s'inclou en un missatge de resposta provisional de tipus 183 Session Progress. Les capçaleres Via: i Record Route: són copiades del missatge SIP INVITE rebut. La capçalera Contact: es canvia amb la IP i el port usats per l'UE 2. En el missatge SIP s'indica també la capçalera Require:100rel, amb la qual s'indica a l'UE 1 que aquesta resposta provisional que li envia l'UE 2 ha de ser resposta amb un missatge PRACK per a saber així si el 183 Session Progress s'ha rebut.

Pas 9. La resposta 183 Session Progress arriba al P-CSCF, el qual, si la reserva de recursos és en mode *push*, podria iniciar una primera reserva de recursos abans de reexpedir el missatge de resposta (fins que no rep la resposta des del PCRF no reenvia el missatge SIP).

Pas 10. Aquesta resposta segueix el mateix camí de node a node que ha traçat el SIP INVITE, però al revés gràcies a la capçalera Via:. En cada node on recala, s'elimina el *hostname* corresponent del Via:, però el Record Route: no es modifica.

Record Route: i Via:

Fixeu-vos que les capçaleres Record Route: i el Via: es processen de manera diferent depenent de si el missatge és una petició o una resposta.

Pas 11. La resposta 183 Session Progress, amb una capçalera SDP que té una llista de paràmetres de QoS prenegociats entre UE 1 i UE 2, arriba al P-CSCF del domini blau. És en aquest punt que el P-CSCF extreu la informació de reserva de recursos per enviar-la al PCRF via interfície Rx (si s'usa el mode *push*). En cas d'usar-se el mode *pull*, el P-CSCF sol·licitaria al PCRF un *authorization token* per incloure'l en la resposta a enviar a l'UE 1. En tots dos casos el missatge de resposta no es reenvia a l'UE 1 fins que el P-CSCF no rep resposta a la sol·licitud cursada.

Pas 12. L'UE 1 selecciona els còdecs definitius de la llista rebuda en el SDP per usar-los en la conversa de veu. Com que en el missatge de resposta veu que hi ha la capçalera Require:100rel, prepara un missatge PRACK per a l'UE 2. Ara ja té el còdec definitiu i, depenent del model de reserva de recursos de la xarxa d'accés de l'UE 1, farà una acció o una altra. Si és en mode *pull*, l'UE 1 iniciarà els mateixos mecanismes que tingui la xarxa d'accés per a garantir la QoS negociada (en una xarxa LTE se sol·licitaria establir un túnel EPS dedicat). En aquesta petició de recursos l'UE 1 ha d'incloure l'*authorization token* si n'hi ha. Si és en mode *push*, l'UE1 no farà res, ja que l'establiment del túnel dedicat ja s'haurà iniciat en el pas anterior.

Pas 13. El PRACK recorre tot el camí fins a l'UE 2 del domini verd, que fa les accions següents depenent del model de reserva de recursos: si és en mode *pull*, des de l'UE se sol·licitarà l'establiment del túnel EPS dedicat. Si és en mode *push*, l'UE 2 no farà res, ja que l'establiment del túnel dedicat ja s'haurà iniciat des del PCRF.

Pas 14. La resposta al PRACK (200 OK) recorre tot el camí de tornada fins a l'UE 1. No obstant això, en passar pels P-CSCF respectius dels dominis blau i verd, poden fer sengles actualitzacions de la reserva de recursos amb la informació SDP del missatge de resposta (això solament es dona si tots dos estan en mode *push*).

Pas 15. L'UE 1 rep el 200 OK en resposta al PRACK enviat anteriorment i es prepara per a enviar el missatge d'UPDATE amb el qual notificarà a l'UE 2 l'estat definitiu de la reserva de recursos en la seva xarxa d'accés. Això es fa enviant la capçalera SDP en el missatge UPDATE amb el mateix format que el PRACK però incloent l'atribut a=curr: qos local sendrecv.

Pas 16. El missatge UPDATE viatja fins a l'UE 2. Aquest s'adonarà que els recursos ja estan disponibles en l'altre extrem de la trucada i respondrà amb un 200 OK a aquest missatge. El 200 OK en resposta a l'UPDATE viatja fins a l'UE 1 per notificar-li la recepció del missatge.

Pas 17. L'UE 2, com a resultat del final del procés de reserva de recursos a la seva xarxa d'accés, envia un 180 Ringing (amb la capçalera Require: 100rel que requereixi confirmació de recepció a l'UE 1) per notificar que l'UE 2 alerta a l'usuari trucat que es requereix una acció seva per a acceptar o rebutjar la trucada entrant. El 180 Ringing (sense informació de SDP) viatja fins a l'UE 1.

Nota

Fixeu-vos que, si l'usuari trucat accepta la trucada, els recursos ja estaran assignats i es podrà procedir a enviar fluxos de veu RTP sense dilació. Si la rebutja, provocarà l'enviament d'una resposta SIP 603 Decline cap a l'UE 1, que provocarà l'alliberament immediat de tots els recursos reservats en ambdues xarxes d'accés.

Pas 18. Es produeix un nou intercanvi de SIP PRACK i 200 OK (però aquesta vegada sense capçalera SDP). A partir d'aquí, l'usuari que trucat estarà a l'espera que l'usuari destinació decideixi acceptar o rebutjar la trucada.

Pas 19. L'usuari trucat (UE 2) decideix acceptar la trucada i provoca que s'enviï un 200 OK, però aquesta vegada serà la resposta definitiva al primer SIP INVITE enviat per l'UE 1.

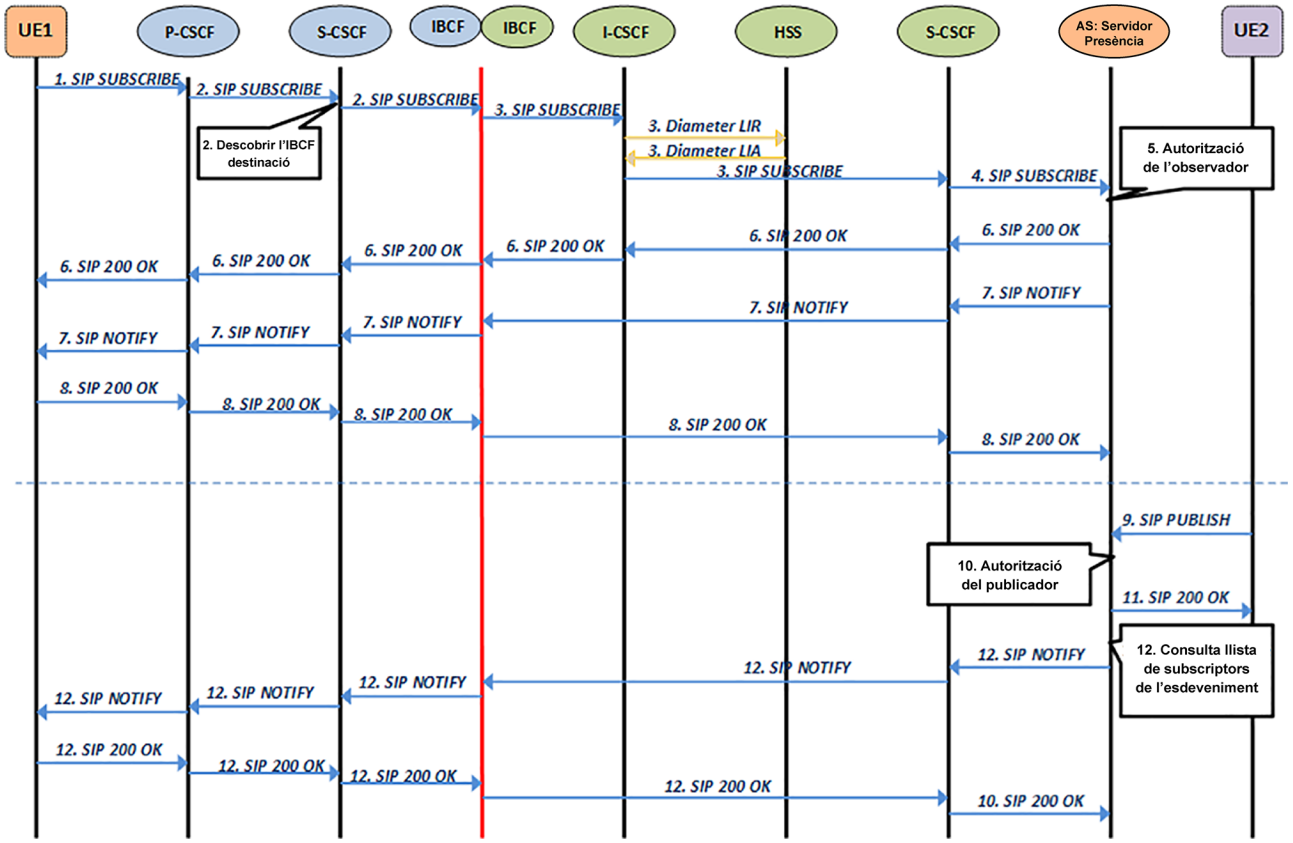
Pas 20. L'UE 1 contesta amb un SIP ACK final confirmant la recepció del 200 OK.

Pas 21. Arribats a aquest punt, tant l'UE 1 com l'UE 2 ja poden intercanviar els fluxos RTP.

3.5.3. Servei de presència

El servei de presència és un dels més importants que s'ofereixen en IMS, ja que és usat per moltes altres aplicacions i serveis. Vegem pas a pas els missatges involucrats en aquest servei a partir de la Figura 16.

Figura 16. Flux de missatges SIP en servei de presència.



Pas 1. L'UE envia un missatge SIP SUBSCRIBE en la capçalera SIP del qual inclou el camp Event: indicant l'esdeveniment al qual es vol subscriure. En aquest cas es tracta de l'esdeveniment *presence* (*Event: presence*). L'UE indica el seu propi URI en la capçalera From: i la ruta a seguir (Route:>) per al missatge SIP indicant el P-CSCF i S-CSCF assignats.

Pas 2, El missatge SIP SUBSCRIBE passa pel P-CSCF, que el fa arribar a l'S-CSCF assignat a l'UE dins del domini. Aquesta consulta el SIP URI de destinació (cap a l'AS que proporciona el servei de presència), que li indicarà a quina IBCF (del domini destinació) ha de reexpedir el SIP SUBSCRIBE.

Pas 3. El missatge arriba finalment a l'I-CSCF del domini que alberga l'AS i aquest li sol·licita a l'HSS (intercanvi de missatges Diameter LIR/LIA) el *host-name* de l'S-CSCF assignat a aquest AS.

Pas 4. L'S-CSCF reenvia el missatge SUBSCRIBE a l'AS corresponent.

Pas 5. L'AS de presència autoritza l'UE que vol subscriure's a l'esdeveniment (obté l'URI del camp From:). En cas d'autoritzar-lo, aquest contesta amb un 200 OK.

Pas 6. El 200 OK arriba a l'UE seguint el mateix camí de tornada que el SUBSCRIBE.

Pas 7. En el moment en què es dona l'esdeveniment al qual l'usuari s'ha subscrit, l'AS envia un missatge SIP NOTIFY cap a l'UE amb l'estat actual de presència. Aquest missatge segueix el mateix camí que el 200 OK excepte l'I-CSCF.

Pas 8. L'UE respon amb un 200 OK a aquest NOTIFY.

En cas que un usuari modifiqui la seva informació de presència, primer es publica el seu nou estat en l'AS de presència i aquest AS notifica el canvi a tots els UE subscrits a aquest esdeveniment. Seguidament, ho expliquem pas a pas amb un exemple:

Pas 9. Un UE extern canvia la seva informació de presència a «No disponible». Llavors aquest envia un missatge SIP PUBLISH cap a l'AS amb la nova informació de presència. En el missatge s'inclou la ruta a seguir amb la capçalera Route: fins al S-CSCF del domini de presència (com qualsevol altre missatge SIP vist fins ara).

Pas 10. L'AS rep el missatge i autoritza l'usuari que vol publicar aquesta informació sobre ell mateix per assegurar-se que pot publicar-la.

Pas 11. L'AS de presència contesta amb un 200 OK a aquesta publicació si l'usuari ha estat autoritzat.

Pas 12. L'AS genera el NOTIFY corresponent amb la nova informació d'estat de presència cap als UE que s'hagin subscrit a aquest esdeveniment (igual que en els passos 7 i 8).

4. Capa d'aplicació

En aquesta secció abordarem com es proveeixen i s'implementen els serveis en les xarxes NGN usant IMS com a capa de control de servei de base.

4.1. Què és un servei en un context NGN?

Abans de res, comencem per saber què és un servei. De manera estricta, i sense entrar en el món de les telecomunicacions i les tecnologies de la informació (IT), **un servei es pot definir en termes de negoci com qualsevol acció o activitat que té un valor afegit per a un consumidor**, el qual pot ser tant una persona com un sistema. Aquesta acció o activitat és oferta per **un proveïdor de serveis**, que pot ser una altra persona, entitat o sistema, el qual obté un benefici en proporcionar aquesta acció.

Els serveis en l'àmbit les telecomunicacions que s'oferien fins avui eren implementats de manera vertical en el sentit que cadascun disposava del seu propi sistema de gestió i operació dedicats. Eren serveis monolítics i incompatibles entre ells.

Les xarxes NGN donen un gir a aquest concepte de servei oferint serveis que no solament són **independents de la tecnologia de la xarxa de transport**, sinó que **es descomponen en elements reutilitzables denominats components de serveis o també habilitadors de serveis *(service enablers*)**.

Com a peces d'un puzle, uns serveis poden complementar-se i integrar-se amb uns altres amb l'única finalitat de produir un nou servei de valor afegit i emmascarar d'alguna manera la complexitat d'aquesta integració a l'usuari final.

Aquesta filosofia encaixa perfectament amb el concepte de les xarxes 5G en les quals la virtualització de xarxes i en concret el NFV-MANO (*network function virtualization management and orchestration*) són els conceptes més característics. Aquesta impulsa l'hiperfragmentació de funcions i/o serveis en microserveis completament independents entre ells i que s'executen en entorns virtualitzats.

Microserveis

El concepte de microserveis també s'estén als components del nucli IMS, en el qual les seves entitats funcionals (P-CSCF, I-CSCF, etc.) es consideren per si mateixes un servei que és consumit per altres entitats.

Per a poder aconseguir aquesta **integració de components de serveis** en altres serveis més complexos, anomenats components, **han de complir les característiques següents**:

- Han d'estar ben definits i diferenciats.
- Han de ser autocontinguts, és a dir, que sempre proporcionin la mateixa funcionalitat independentment dels altres serveis.
- No han de dependre del context o estat d'altres components o serveis.

La integració de serveis també comporta la definició d'interfícies estandarditzades que possibilitin la integració d'aquests components. És aquesta modularitat i interactivitat entre components la que possibilita la creació fàcil de nous serveis futurs, i això és una de les claus de les xarxes NGN.

Exemples d'aquests components són el servei de presència, el de gestió de grups, la missatgeria instantània, etc. Aquests serveis, a més, poden ser proveïts per tercers.

Amb vista a aconseguir la independència entre serveis i tecnologia de transport i possibilitar que tercers (desenvolupadors d'aplicacions) puguin desenvolupar ràpidament nous serveis, s'utilitzen API (*application programming interface*) obertes.

La indústria ha donat llum a diverses API obertes per a desenvolupar serveis com OSA/Parlay API, JAIN SIP, JAIN SLEE, SIP Servlet i, sobretot, API basades en HTTP REST.

En resum, aquest nou enfocament és definit per un nou paradigma en el món dels serveis anomenat SOA (*service oriented architecture*), el qual descriurem a continuació.

4.2. Introducció al paradigma SOA

El **paradigma SOA** (*service oriented architecture*) és un estil d'arquitectura l'objectiu del qual és aconseguir el desacoblament entre els components de programari que interactuen entre ells. El comportament d'aquests components és definit completament per API i interfícies contractuals, públiques i neutrals, tant en tecnologia com en plataforma.

Els principals objectius de SOA en comparació d'altres arquitectures de programari usades en el passat són els següents:

- Obtenir una major rapidesa d'adaptació del programari a les necessitats comercials canviants.
- Obtenir una reducció del cost d'integració de nous serveis i del manteniment de serveis ja existents.

SOA reorganitza les aplicacions de programari existents i els components en un conjunt de serveis autocontinguts i autodefinits definint interfícies estàndards i protocols de missatgeria entre aquest programari. Aquests serveis poden ser accedits sense que sigui necessària una connectivitat punt a punt tradicional, basada en diferents protocols. Qualsevol servei SOA pot tenir el paper de client o de servidor pel que fa a un altre servei, en funció de la situació.

Un exemple que l'arquitectura SOA s'ha implantat i s'usa de manera extensiva és la informàtica en núvol. Amazon ho implementa en el seu Amazon Web Services per als seus serveis web. Permet als usuaris construir les seves pròpies aplicacions web de manera escalable usant cadascun dels components de serveis que ofereix com un bloc estable i fàcil d'utilitzar. Aquests blocs poden ser usats per separat o enllaçats amb altres serveis d'AWS utilitzant comunicacions específiques i ben definides.

Arquitectura SOA

Heu de tenir en compte que SOA no és una tecnologia sinó un model arquitectural de programari distribuït. No obstant això, hi ha tecnologies per a crear programari amb arquitectura SOA, com per exemple BPEL d'Oracle o opcions de codi obert com Mule Studio de Mulesoft.

El paradigma SOA permet que processos i transaccions de negoci complexos puguin ser proporcionats com a serveis integrats de manera que les aplicacions puguin ser reutilitzades en qualsevol lloc i per qualsevol usuari.

Un SOA bàsic inclou tres procediments fonamentals:

- **Provisió de servei.** Els proveïdors desenvolupen aplicacions que proporcionen serveis als clients. En la provisió de serveis s'inclou també un pla de tarifes (si n'hi ha) o fins i tot la definició d'aspectes de seguretat i disponibilitat per a l'usuari.

- **Registre de servei.** És un directori anomenat Universal Description Discovery and Integration (UDDI), en el qual els proveïdors de serveis poden registrar informació sobre els serveis que ofereixen i el lloc on clients potencials poden descobrir-los i buscar-los.

- **Client de servei.** És l'eina que utilitza el consumidor del servei. Aquest no és conscient de la complexitat dels serveis ni tampoc de la seva descomposició en components. Tot el que sap, i pel que es preocupa, és el seu acord amb el proveïdor de serveis o SLA (*service level agreement*) i les aplicacions instal·lades o l'equip utilitzat per a poder disposar del servei.

Juntament amb aquests procediments, SOA també defineix tres funcions importants:

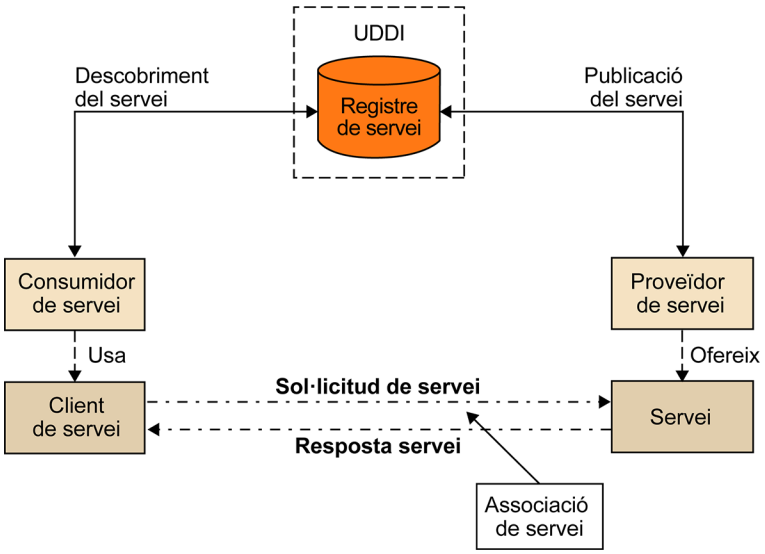
- **Publicació del servei.** El proveïdor publica en el registre de servei informació descriptiva sobre el seu servei perquè el client pugui saber quines capacitats té i com accedir-hi.
- **Descobriment de servei.** El client recorre al registre per conèixer d'una manera senzilla i intel·ligible tots els serveis disponibles.
- **Associació al servei.** Una vegada un client vol invocar un servei a un proveïdor concret, fa una sol·licitud (mitjançant la interfície corresponent) dirigida a aquest, el qual envia una resposta concorde a aquesta sol·licitud (provisió del servei).

SOA defineix una interacció entre els clients de servei i els proveïdors de servei. Aquests són responsables de publicar una descripció dels serveis en l'UDDI (vegeu la Figura 17). Per a publicar aquesta descripció dels serveis (interfícies de serveis web en aquest cas), l'UDDI se serveix del llenguatge WSDL (*web services description language*).

Com a exemple d'UDDI, hi ha el cas típic del servei de reserva de bitllets d'avió per internet. No solament es pot fer per la mateixa web de l'aerolínia sinó per una infinitat de cercadors web de bitllets d'avió i/o hotels. Les aerolínies poden registrar els seus serveis de reserva de vols en un directori d'UDDI. Les agències de viatges poden buscar les interfícies o els contractes dels serveis web de les aerolínies i, una vegada trobin el que necessiten, poden començar a usar-ho immediatament.

La publicació, no solament dels serveis sinó dels components de telecomunicació reutilitzables (anomenats habilitadors de serveis o *service enablers*) permet construir aplicacions amb la seva lògica de servei específica i l'ús d'aquests habilitadors. Aquesta reutilització permet reduir els costos d'introducció de serveis múltiples, de manera que és un dels principals avantatges finals de basar-se en SOA.

Figura 17. Arquitectura SOA.



Importància de l'orquestració dels serveis en SOA

Sabent que un servei pot estar format per diversos components de serveis, sembla obvi que s'hagi de desenvolupar alguna tasca de mediació o orquestració que proporcioni coordinació en l'ús dels components.

Els components dels serveis s'allotgen en una o més plataformes de subministrament de serveis anomenades SDP (*service delivery platforms*). Aquestes plataformes ofereixen un marc per a crear, orquestrar i executar serveis fàcilment, i gestionar aplicacions provinents de tercers. La integració de l'SDP amb les funcions de xarxa és única (la mateixa interfície amb la xarxa és utilitzada per tots els serveis).

Mitjançant orquestració, les capacitats dels diferents SDP es poden combinar per a crear nous serveis reutilitzant les seves capacitats. D'aquesta manera, es redueixen els esforços i els costos en el desenvolupament de serveis i el seu temps de llançament al mercat.

Si tinguéssim més d'un SDP a integrar entre ells, les seves interaccions s'extraurien cap a una capa externa d'orquestració, la qual cosa redueix les dependències i incrementa la flexibilitat dels serveis en un entorn de diversos proveïdors.

La capa d'orquestració no solament pren el rol de la integració de l'execució i de l'orientació de la gestió, sinó que també, i més important, té un paper essencial en definir i implementar la gestió i l'execució de la lògica del servei.

Com es comuniquen els serveis entre ells i què recomana la indústria per a implementar SOA en l'àmbit de protocols?

En el context d'implementació de serveis en el qual hi ha blocs de programari independents que interaccionen per formar un servei més complex és normal pensar en un esquema consumidor-productor. És a dir, un consumidor (que pot ser un component de programari o directament un usuari) consumeix uns serveis o recursos que un altre bloc produeix (aquesta arquitectura és quelcom molt típic en serveis web). I és en aquest context que s'utilitzen protocols que s'adapten a aquest intercanvi d'informació.

Hi ha principalment dues tecnologies per a implementar serveis que compleixin SOA: SOAP i REST. Encara que SOAP és uns dels protocols més usats per a implementar SOA, la tecnologia REST s'estén cada vegada més. La principal diferència entre SOAP i REST és la filosofia que segueixen per fer invocacions remotes.

REST

En anglès significa *representational state transfer.*

SOAP

En anglès significa *simple object access protocol.*

REST segueix un mètode basat en l'accés a recursos via interaccionis basades en web. Amb REST, es localitza un recurs en un servidor i es tria actualitzar aquest recurs, esborrar-lo o aconseguir alguna informació sobre ell.

Amb SOAP, el client no tria interactuar directament amb un recurs, sinó que crida un servei. Aquest servei mitiga l'accés a diversos objectes i recursos que hi ha al darrere.

SOAP ha construït un gran nombre d'entorns i API sobre HTTP, incloent el WSDL (*web services description language*), que defineix l'estructura de dades que s'intercanvien entre un client i un servidor.

SOAP (*simple object access protocol*) defineix una especificació o grup de regles d'un protocol estàndard de comunicació en el qual s'intercanvien missatges basats en XML. En l'àmbit de protocols de

transport suporta HTTP i SMTP. L'estàndard HTTP s'adapta millor, ja que pot traspassar tallafocs i *proxies* sense cap impacte en el protocol SOAP.

REST (*representational state transfer*) no és un protocol pròpiament dit, sinó que descriu un grup de principis d'arquitectura pels quals les dades poden ser transmeses sobre una interfície estandarditzada (com HTTP). REST no especifica una estructura de missatgeria pròpia i solament es focalitza en el disseny de regles per crear serveis sense estat. Conseqüentment, un enginyer de programari disposa de llibertat per a dissenyar l'estructura de la informació continguda en el cos dels missatges intercanviats. Un client REST pot accedir a un recurs usant l'URI únic, i una representació del recurs és retornada. Quan s'accedeix als recursos amb el protocol HTTP, l'URL del recurs serveix com un identificador del recurs i les operacions estàndard d'HTTP (com GET, PUT, DELETE, POST i HEAD) representen les operacions que es fan sobre aquest recurs. La informació intercanviada en el cos dels missatges HTTP sol ser codificada usant JSON o XML.

4.3. Integració dels serveis NGN en el paradigma SOA

URI

En anglès significa *unique resource identifier* i en HTTP REST és un URL com per a accedir a una pàgina web amb diverses carpetes, cadascuna de les quals alberga un recurs.

En aquest apartat ens endinsem en el camp de la integració dels serveis de comunicacions multimèdia (basats en SOA) en un entorn NGN en el qual hi ha el nucli IMS com a subsistema de control de sessió de servei.

A continuació descriurem el servidor d'aplicació (AS) com a entitat més representativa en la provisió de serveis en NGN/IMS.

Servidors d'aplicacions

Els **servidors d'aplicacions (*application servers*, AS)** són l'element central de l'arquitectura de serveis de NGN/IMS. La seva funció és albergar i executar els serveis de valor afegit de la plataforma i comunicar-se amb el nucli IMS (singularment amb l'S-CSCF) fent ús del protocol SIP. Els servidors d'aplicacions no són estrictament entitats d'IMS, sinó més aviat funcions que es construeixen per interactuar amb el nucli IMS a un nivell superior. No obstant això, hi recau la provisió de la majoria dels serveis que aporten valor a IMS.

Els atributs fonamentals d'un servidor d'aplicacions són:

- Possibilitat de rebre i processar una sessió SIP entrant procedent d'IMS.
- Capacitat per a fer peticions SIP.
- Capacitat per a enviar informació a les funcions de facturació.

Els servidors d'aplicacions poden operar com tres tipus d'entitats SIP: agent d'usuari (UA), servidor intermediari i agent d'usuari invers (B2BUA o *back-to-back user agent*). Aquests servidors poden estar situats dins de la xarxa local a la qual està connectat l'usuari o bé operar independentment des d'una xarxa externa. D'altra banda, un AS pot estar dedicat a proporcionar un únic servei, mentre que un usuari pot utilitzar més d'un servei simultàniament, i per això un mateix subscriptor pot fer ús d'un o més servidors d'aplicacions i fins i tot pot haver-hi sessions en les quals intervingui més d'un AS.

SIP, UA i B2BUA

En SIP, *user agent* (agent d'usuari o UA) representa un dels extrems de la comunicació SIP (per exemple, en un client SIP s'executa un UA de SIP). No obstant això, un SIP *proxy*, com que no és el destinatari final d'un missatge SIP, té la funció de reexpedir-lo a un altre servidor intermediari o a l'UA destinació. Finalment, un B2BUA són dos agents d'usuari en la mateixa màquina però interconnectats entre ells per algun tipus de lògica o funcionalitat. En aquest últim cas dues sessions SIP totalment independents s'interconnecten mitjançant aquesta lògica.

En la Figura 18 podem veure com la capa de control de servei (representada pel nucli IMS) es connecta amb el servidor d'aplicació (AS) per una interfície SIP (segons 3GPP, s'anomena ISC[4] o IMS *service control*), i aquesta amb l'aplicació mitjançant una API de programació oberta. És precisament aquesta API la que representa la interfície ANI del model de referència de l'ITU-T de NGN (vegeu la Figura 1).

[(4)]La interfície ISC també s'anomena SIP+.

En aquesta figura també veiem que l'S-CSCF no és l'únic element del nucli IMS connectat amb l'AS. L'I-CSCF també té una interfície dedicada d'interconnexió anomenada Dt. que està basada en SIP, com la interfície ISC. Aquesta interfície permet que l'I-CSCF rebi una petició SIP entrant dirigida a una PSI (*public service identity*), que la resol a un AS particular. L'I-CSCF encamina la petició directament a l'AS via interfície Dt. Aquesta interfície també és usada per l'AS quan necessita iniciar una sessió cap a un usuari o PSI i aquest AS no té coneixement previ de l'S-CSCF al qual és associat aquest usuari o PSI.

Tot i que l'I-CSCF té aquesta funcionalitat d'interacció amb els AS, a partir d'ara ens centrarem exclusivament en l'ús de la interfície ISC, ja que és el cas més comú.

Tornant a la Figura 18, podem veure també que tant l'AS com els CSCF del nucli IMS tenen accés a l'HSS per sengles interfícies basades en Diameter Sh i Cx respectivament. Aquestes interfícies són utilitzades per aquestes entitats per a descarregar informació de subscripció relacionada amb les aplicacions (*service profile*) a les qual l'usuari té permís d'accedir. En aquesta informació de subscripció hi ha l'iFC (*initial filter criteria*.

L'iFC (***initial filter criteria***) (3GPP TS 23.218) és una llista de paràmetres que componen el *service profile* i formen part de la informació de subscripció de l'usuari que ajuda l'S-CSCF a decidir a quin AS s'ha d'enviar una petició SIP determinada (que pot ser un REGISTER, INVITE, SUBSCRIBE, NOTIFY o MESSAGE). Aquesta informació, que té caràcter estàtic, la rep l'S-CSCF des de l'HSS via interfície Cx en forma de *trigger points*. Un iFC és format pels paràmetres següents:

- ***Priority level.*** És el nivell de prioritat amb el qual s'ha d'aplicar un iFC respecte a altres iFC en el mateix *service profile*. Aquest paràmetre indica l'ordre en què s'apliquen (com més baix és el nombre més prioritari és, i no cal que siguin nombres consecutius)

- ***Trigger points.*** És compost per un conjunt de *service point triggers* (que es descriuen més endavant).

- ***Application server.*** S'hi especifiquen les dades que defineixen el SIP AS al qual cal enviar el missatge SIP. Aquestes dades són:
  - SIP URI: és l'àlies (resoluble via DNS) que identifica el SIP AS de manera única (pot ser una adreça IP directament).
  - Default Handling: defineix l'acció a fer (avortar o continuar la sessió) si el *service broker* (que veurem més endavant) o l'S-CSCF no pot establir connexió amb l'AS pel motiu que sigui.
  - Service Information: són les dades addicionals que l'AS pot requerir per a processar la sol·licitud.

Priority level

Teniu un exemple de com s'aplica el *priority level* i els *trigger points* en l'orquestració de components de servei en el final de la secció 4.4.2.

Els *trigger points* estan formats per un conjunt de comparacions de camps del missatge SIP que, com ja s'ha comentat abans, s'anomenen *service point triggers*. La interrelació entre aquests SPT en un *trigger point* es defineix segons un altre paràmetre anomenat *condition type CNF*, que pot tenir dos valors:

- **Disjunctive Normal Format:** els SPT s'hi apliquen en AND acollits entre OR.
  (SPT1 **AND** SPT2 **AND**…) **OR** (SPTn **AND** SPTm **AND**...) **OR** (...).

- **Conjunctive Normal Format:** els SPT s'hi apliquen en OR acollits entre AND.
  (SPT1 **OR** SPT2 **OR**…) **AND** (SPTn **OR** SPTm **OR** …) **AND** (...).

En un acollit d'AND o d'OR pot ser que es tingui solament un SPT (vegeu l'exemple per a Disjunctive Normal Format a continuació).

(SPT1) **OR** (SPTn **AND** SPTm **AND**...) **OR** (SPT2)

Cada SPT es defineix pels camps següents per a fixar les condicions per a ferhi una coincidència:

- **Negació o «Not».** Farà coincidència sempre que no es compleixin les condicions que s'indiquen en l'SPT. Aquest camp es considera com una casella de selecció: «activat» [X] o «no activat«» [ ].

- **Tipus de camp.** Indica el tipus d'informació a consultar. Normalment és un entre els valors següents per cada SPT: Request URI, SIP Method, SIP Header, Session Case o SDP *line*.

a) **Valor de camp.** Depenent del tipus de camp que s'hagi seleccionat, el contingut pot canviar. A continuació es llista el tipus de contingut que s'espera segons cada tipus de camp:
   - **Request URI.** Text o part del text a comparar en aquest camp del missatge SIP. Normalment s'utilitza notació de Regular Expression (també anomenat Regex).

   Exemple que expressa un Request URI qualsevol que vagi al domini *home-domain.net*: «sip: *@home-domain.net».

   - **SIP Method.** Indica el missatge SIP a comparar (INVITE, REGISTER, SUBSCRIBE, ...).

   - **SIP Header.** Indica primer la capçalera dins del missatge i després el seu contingut amb notació Regex (*regular expression*).

   Exemple que expressa un SIP Header «From» qualsevol amb domini *home-domain.net*: header type: «From:» header value: «*@home-domain.net».

   - **Session Case.** Indica l'adreça del missatge SIP, de la qual hi ha dos tipus principals:
     - «*UE-originating*»: perfil per a peticions SIP sortints (generades per l'usuari subscriptor).
     - «*UE-terminating*»: perfil per a peticions SIP provinents d'un altre usuari i que van cap a l'usuari subscriptor en qüestió.

   - **SDP line.** En aquest cas solament s'aplica a línies que s'usen en la negociació de còdecs, que és de tipus SDP (*session description protocol*). S'indica primer el tipus de línia SDP (m, a, c, etc.) i després el seu contingut amb notació Regex.

   Exemple que expressa que en SDP hi ha un component de multimèdia de vídeo qualsevol: *SDP line: «m» SDP line value: «*video*»*.

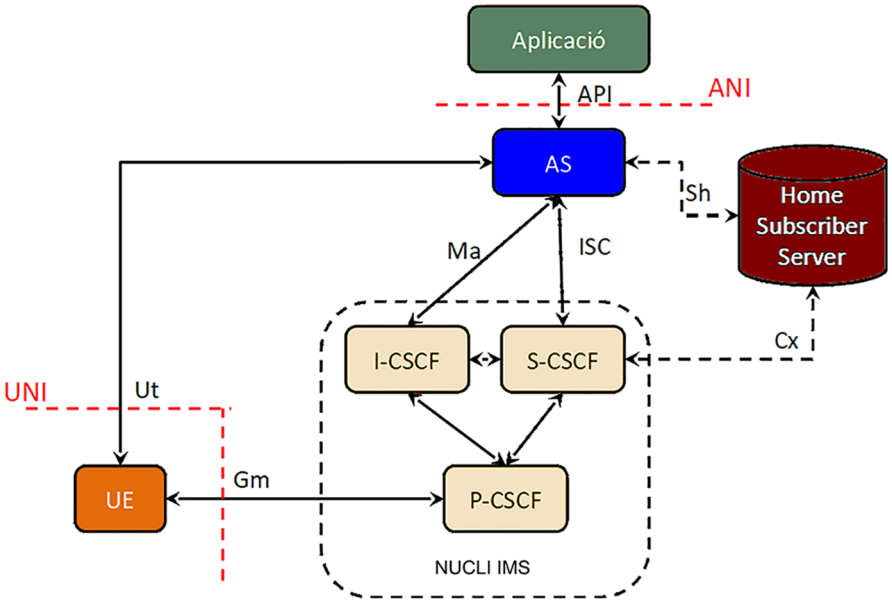
Precisament, pel que fa a l'usuari (representat com a UE en la Figura 18) podem remarcar una interfície anomenada Ut, definida per 3GPP, que interconnecta l'UE directament amb l'AS. Cal aclarir que aquesta interfície no s'utilitza per a invocar un servei. Per a això ja hi ha la interfície Gm, que està basada en SIP i interconnecta directament l'UE amb el P-CSCF del nucli IMS.

La interfície Ut proporciona a l'usuari un protocol per a configurar i gestionar aspectes relacionats directament amb el servei de l'AS (per exemple, grups o polítiques). El protocol proposat per 3GPP per a aquesta interfície és l'XCAP (*XML configuration access protocol*) en conjunció amb el protocol HTTP. Així, doncs, per a l'usuari, la interfície Ut es pot traduir en una pàgina web específicament dissenyada per a configurar el servei del qual l'usuari és subscriptor.

Protocol XCAP

El protocol XCAP, definit en l'RFC 4825, és un protocol que defineix com usar HTTP per a crear, modificar i eliminar un document XML incloent tots els seus elements, atributs i/o valors.

Figura 18. Interconnexió lògica entre el nucli IMS i els servidors d'aplicació (AS).



El cas exposat en la Figura 18 en relació amb la interconnexió entre l'S-CSCF i l'AS via interfície ISC, basada en SIP, és solament un cas genèric d'interconnexió. La realitat és que hi ha operadors que han apostat per una migració escalonada de la seva infraestructura a IMS per amortitzar així els servidors d'aplicacions ja existents, i per tant els serveis que ofereixen aquests servidors no estan basats en el protocol SIP. Els protocols usats en aquests casos són, per exemple, el CSE de CAMEL (*customized applications for mobile network enhanced logic*) o OSA (*open service architecture*).

Protocol OSA

La sigla OSA correspon a *open service access*. És un marc que habilita les aplicacions que implementen serveis per a usar funcionalitats de xarxa. Aquestes funcionalitats de xarxa es tradueixen en les SCF o *service capabilities features*, les quals són accessibles a les aplicacions mitjançant l'API estandarditzada d'OSA per al desenvolupament de serveis.

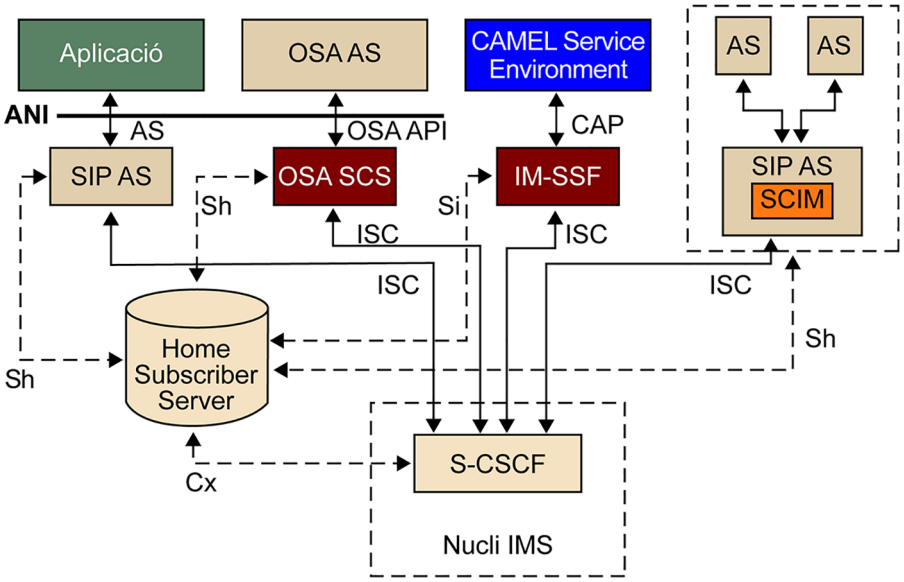
Davant aquest problema, 3GPP ha aportat la seva visió particular a la capa d'aplicació, tal com s'explica a continuació.

Proposta de 3GPP per a integrar AS en IMS

3GPP ha desenvolupat conjuntament una sèrie d'especificacions per a integrar els serveis en IMS.

En la Figura 19 es poden observar els elements definits per 3GPP per a poder connectar diversos tipus de servidors d'aplicació al nucli IMS, els quals descrivim breument a continuació.

Figura 19. Model d'arquitectura de servei NGN per 3GPP.



Per a proveir aquests serveis als subscriptors d'IMS, és necessària una adaptació dins del corresponent servidor d'aplicacions. D'aquesta manera, el terme *servidor d'aplicacions* s'empra genèricament per a englobar tant els servidors natius de SIP (SIP AS) com els que proporcionen aplicacions de CAMEL (*IP multimedia service switching function* o IM-SSF) per a serveis de telefonia mòbil (GSM o UMTS) o OSA (OSA *service capability server* o SCS) per a serveis de telefonia fixa. Per tant, hi ha tres tipus de funcions de servidor d'aplicacions:

1) SIP AS. Els servidors d'aplicacions basats en SIP (SIP AS) són natius d'IMS i, per tant, no requereixen cap tipus d'adaptació en la seva interfície amb l'S-CSCF del nucli IMS (vegeu la Figura 19). Es pot afirmar que aquestes aplicacions són les creades genuïnament per a interactuar amb la capa de control de servei de les xarxes NGN. Per això, tot servei nou que es creés s'emmarcaria en aquest tipus d'AS. Les atribucions principals d'un servidor d'aplicacions SIP són:

- Redirigir la sessió cap a xarxes o usuaris.
- Interactuar amb les plataformes de serveis per donar suport de serveis avançats.
- Comunicar-se amb l'HSS per obtenir informació relativa a subscripcions o serveis.

Si el SIP AS està en la xarxa local, la comunicació amb l'HSS es pot fer mitjançant Diameter mitjançant la interfície Sh, ja que es considera una interfície intradomini.

Exemples de SIP AS són habilitadors com els servidors de presència, de missatgeria, de conferència, d'aplicacions de trucada, i també aplicacions domèstiques, d'IPTV, de facturació, de descobriment d'altres serveis, etc.

2) OSA AS - OSA SCS. L'entorn OSA facilita diverses funcionalitats als operadors, com control de trucades, interacció de l'usuari, informació d'estat, informació de la capacitat del terminal, control de sessions de dades, gestió de comptes o facturació. Un altre avantatge de l'entorn OSA és que disposa de funcionalitats d'autenticació, autorització, registre i descobriment de servei, i per això és una manera eficaç d'introduir en el sistema servidors d'aplicacions externs a la xarxa IMS (el nucli IMS no ofereix solucions segures per a aquests casos).

Atès que aquests servidors d'aplicacions no suporten SIP, és necessària la intermediació de l'OSA SCS (OSA *service capability server*) amb l'objectiu que manegi la senyalització procedent de l'S-CSCF. De manera específica, l'OSA SCS és l'entitat que exerceix d'interconnexió entre els elements següents:

- funcions de les xarxes NGN
- tots els servidors d'aplicació externs pel que fa al domini local
- habilitadors de servei.

La comunicació entre l'OSA SCS i l'OSA AS es duu a terme mitjançant una API específica.

3) CAMEL CSE (SCP) - IM SSF. De la mateixa manera, per una xarxa IMS també es pot accedir a serveis CAMEL de xarxa intel·ligent (IN) i a les seves funcionalitats, com la màquina d'estats finits per a commutar serveis (CAMEL *service switching finite state machine*) o els punts de detecció d'activació de servei (*trigger detection points*). El suport d'aquest tipus d'aplicacions implementades en CSE (*CAMEL service environment*) i en un entorn SIP s'aconsegueix gràcies a la introducció de l'IM-SSF (*IP multimedia service switching function*), una passarel·la que permet als SCP (*service control points*) de CAMEL controlar una sessió IMS. En una xarxa interna, la comunicació segura entre l'AS i la HSS es faria mitjançant una interfície anomenada MAP (*mobile application part*).

Interfície MAP

El MAP (*mobile application part* és un protocol SS7 que proporciona una capa d'aplicació per als diferents nodes en les xarxes mòbils troncals de GSM i UMTS per comunicar-se mútuament amb l'objectiu de proporcionar serveis als usuaris de telèfons mòbils.

SCP

Un SCP (*service control point*) és un component de les anomenades xarxes intel·ligents (IN o *intelligent networks* en anglès) dels sistemes de telefonia tradicional (basats en SS7), el qual té com a funció controlar els serveis. Exemples d'aquests serveis són els anomenats prepagament, cobrament revertit, transferència de trucada o portabilitat del número telefònic. La capa d'aplicació de les xarxes intel·ligents s'anomena INAP (*intelligent network application part*).

4.4. Orquestració entre serveis i/o habilitadors

L'orquestració entre els serveis és crucial, no solament en la creació de nous serveis de valor afegit, sinó també per a permetre una migració progressiva dels serveis oferts avui dia pels proveïdors de serveis de comunicacions (no basats en xarxes NGN) cap a serveis basats en IMS.

Aquest últim factor és importantíssim, ja que les companyies que ja han invertit molts diners en la infraestructura de provisió de serveis actual (per exemple, en serveis basats en infraestructura heretada, com CAMEL o IN) necessiten amortitzar la inversió. Així, doncs, es preveu una coexistència llarga entre els nous serveis generats (basats en IMS) i els que ja hi ha per a anar migrant a poc a poc la infraestructura.

D'aquesta manera, aquesta companyia podrà continuar donant servei als usuaris que encara usen la infraestructura (telefonia mòbil 2G/3G, RTC, RDSI) i serveis antics mentre crea nous serveis emparats en el marc que ofereixen les xarxes NGN i IMS. Aquest és un factor clau que pot provocar que aquestes companyies proveïdores es decideixin a invertir en la migració progressiva cap a un sistema més eficient, atractiu i amb menors costos de manteniment i operació, com les NGN.

Fer l'orquestració de diversos serveis en un de sol no és una tasca fàcil. L'element que s'encarregui de fer aquesta funció rebrà una petició (per exemple, en forma de petició SIP des de l'S-CSCF via interfície ISC) i haurà de desencadenar i/o coordinar la comunicació entre components de serveis segons es requereixi. A més, té la dificultat afegida d'haver de fer a vegades traduccions de protocols, ja que els components o serveis que formen el servei final són de caràcter heterogeni i poden requerir utilitzar diferents protocols en una mateixa sessió de servei (en l'àmbit de comunicació entre components).

Així, doncs, l'orquestració de serveis es presenta com un dels aspectes clau en el futur de les xarxes NGN, i tots aquests requisits es concreten en un element que serà crucial en la integració de serveis: el *service broker*, que veurem en la secció 4.4.2.

El ***service broker (SB)*** és un element de xarxa que gestiona eficientment la interacció i la composició dels serveis. Està situat entre la capa de servei i la xarxa convergent, i desvinculat tradicionalment dels elements d'encaminament de trucades i dels entorns de creació i execució de serveis.

Abans de descriure amb més detalls el *service broker*, vegem una de les funcions que 3GPP ha definit junt amb les funcions que exerceix: la funcionalitat SCIM (*service capability interaction manager*).

4.4.1. Funcionalitat SCIM (*service capability interaction manager*)

l'SCIM (*service capability interaction manager*) gestiona la provisió de serveis entre diferents plataformes de servidors d'aplicacions dins de l'arquitectura IMS. El propòsit de l'SCIM és, doncs, coordinar les capacitats d'aquests serveis en l'àmbit de la capa d'aplicació. Es tracta d'una entitat independent que, en cas d'estar present en l'arquitectura, està situada entre l'S-CSCF del nucli IMS i els servidors d'aplicacions (AS).

L'SCIM està definit en el 3GPP TS 23.002. Al llarg del procés d'estandardització d'IMS, s'han identificat diferents possibles implementacions de SCIM, d'entre les quals descriurem només la més típica: SCIM com a *broker* SIP.

En aquest mode de funcionament l'SCIM gestiona la interacció entre diferents components de serveis basats essencialment en SIP i que implementen servidors intermediaris o agents d'usuari (*user agents*). Per a gestionar aquesta interacció, l'SCIM sol exercir funcions de B2BUA (agents d'usuaris interconnectats entre ells en una mateixa entitat) i aplicar seqüències de regles complexes i encaminament avançat.

Aquestes seqüències de regles són fixades pels iFC, que hem explicat anteriorment.

4.4.2. El *service broker*

Al principi d'aquest apartat hem vist una pinzellada de l'SB (*service broker*) i per tant ja podem veure que no és un element que faci una tasca que es pugui considerar senzilla tenint en compte els requeriments que necessiten les companyies proveïdores de servei. A manera d'evolució de l'SCIM, 3GPP també ha publicat un document d'especificació de definició de l'SB (TR 23.810), però l'última versió d'aquesta especificació (8) deixa en l'aire molts aspectes, tal com veurem més endavant. De totes maneres, sí que podem esmentar les dues funcions principals que un SB ha de fer:

1) Mediació entre serveis i la xarxa. L'SB proporciona tota la connectivitat de xarxa i la traducció de protocols necessària per a suportar la interoperabilitat entre qualsevol servei de comunicació i qualsevol xarxa (inclosos el *Mobile Switch Center* o MSC de telefonia mòbil, *switches* i *softswitches* de RTC, i S-CSCF del nucli IMS). En aquest sentit, l'SB va més enllà que la funcionalitat SCIM explicada en l'apartat anterior, la qual fa aquesta mateixa funció però solament interconnectant amb el nucli IMS en el costat de la xarxa.

Com a exemples, es pot esmentar el cas de mediació entre serveis de xarxes intel·ligents (IN) però de diferents variants de protocols. També es pot donar el cas de la mediació entre serveis d'IN i elements de control de sessió IMS (l'S-CSCF) o bé entre aplicacions de NGN i elements de control de trucada de xarxes tradicionals (l'MSC de la xarxa de telefonia mòbil).

2) Orquestració de servei en temps real. Permet que molts serveis interactuïn mútuament en una sola trucada o sessió amb l'objectiu de crear nous serveis o agrupacions de serveis combinant un nombre de serveis individuals (els quals poden estar associats amb xarxes heretades, xarxes NGN o una mescla d'ambdues). Per a això, usa les funcionalitats següents: SCIM, IM-SSF, gestió de *trigger* IN-IN, gestió de flux de trucada/protocol, facturació en temps real i interacció de dades de gestió de subscriptor (amb HSS).

Per a exercir aquestes funcions, l'SB té una arquitectura funcional interna que ajudarà a entendre com funciona aquest element. No obstant això, com hem dit abans, no hi ha una especificació clara de 3GPP sobre quins blocs funcionals conformen un SB. Aquest buit ha hagut de ser omplert per iniciatives d'empreses privades que ja han desenvolupat els seus propis SB propietaris. Per tant, vegem a continuació una proposta genèrica d'aquesta arquitectura, que pot donar una idea general de com podria ser implementat un SB.

Proposta d'arquitectura funcional

L'SB estaria compost pels components següents, els quals es poden veure en la Figura 20:

1) Motor d'orquestració. El MO està situat en el cor de l'arquitectura de l'SB. El MO encamina les peticions de serveis i tarifació des de la xarxa a una o més plataformes de serveis. A més, gestiona les interaccions entre plataformes de servei i l'encaminament de sessió mitjançant de les aplicacions.

2) Mòduls d'interacció (*interworking modules*). És un conjunt de mòduls configurables i intercanviables que habiliten el MO per a comunicar-se amb plataformes d'aplicacions i entitats de control de sessions en diverses xarxes. Cada IM proporciona interacció amb un element de xarxa específic mitjançant el protocol natiu d'aquest element. Hi ha tres tipus d'IM:

IM-SSF

L'IM-SSF, que interactua amb l'aplicació, té el seu element mirall que interactua amb la xarxa i que s'anomena IM-SSF invers. L'IM-SSF ja s'ha descrit anteriorment. L'IM-ASF invers és l'element mirall de l'IM-ASF (*application server function*) que implementa la interfície SIP per comunicar-se amb els SIP AS o habilitadors basats en aquest protocol SIP d'IMS.

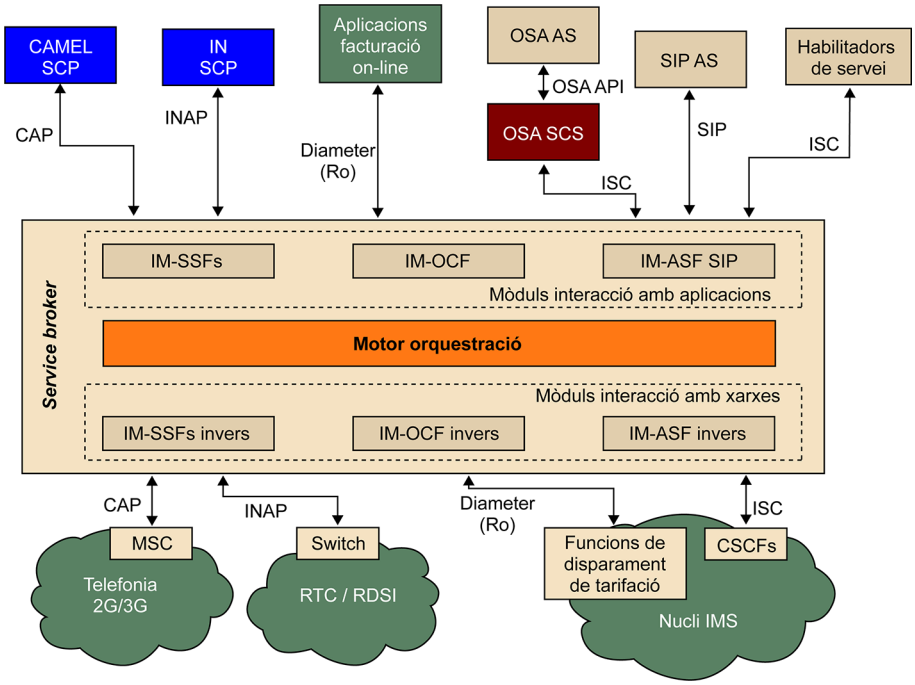
- **Mòduls d'interacció amb les xarxes.** Habiliten connectivitat entre l'SB i les entitats de control de sessió, com MSC de telefonia mòbil 2G/3G o l'S-CSCF del nucli IMS. Proporcionen una interfície intel·ligent a les entitats de control de sessió perquè interactuïn amb l'SB, de la mateixa manera que interactuen amb les plataformes d'aplicació, sense necessitat de fer canvis en configuració. Exemples d'aquests mòduls són els IM-SSF invers i els IM-ASF invers (mòduls d'interacció amb funcions d'AS).

- **Mòduls d'interacció amb les aplicacions.** Habiliten la connectivitat entre l'SB i plataformes d'aplicació, com els CAMEL IN, SIP AS i els servidors de tarifació en línia. Aquests mòduls proporcionen una interfície

intel·ligent a les aplicacions perquè interactuïn amb l'SB, de la mateixa manera que interactuen amb la xarxa, sense necessitat de fer canvis en la configuració. Exemples d'aquests mòduls són els IM-SSF, IM-OCF (mòdul per a la facturació en línia) i IM-ASF.

Mòduls suplementaris. Encara que no es mostrin en la Figura 20, són configurables i intercanviables de manera que faciliten i complementen les solucions de l'SB en certs casos particulars. Aquests mòduls són proporcionats per l'SB i poden ser utilitzats de manera opcional.

Figura 20. Arquitectura funcional d'un *service broker.*



En el nucli de l'SB, la interacció és normalitzada a un model comú de sessió i esdeveniment. Cada IM proporciona una conversió entre la representació de la sessió interna de l'SB i el protocol extern aplicable. Mitjançant un extens ventall d'IMS tant de xarxa com d'aplicació, l'MO estén el servei d'orquestració més enllà d'IMS cap a serveis anteriors a IMS, com per exemple IN, xarxes SS7 i altres dominis no-IMS com IPTV o SOA. Tot això fa possible l'orquestració i la mediació entre diverses plataformes d'aplicació i tarifació.

Interacció del *service broker* amb IMS

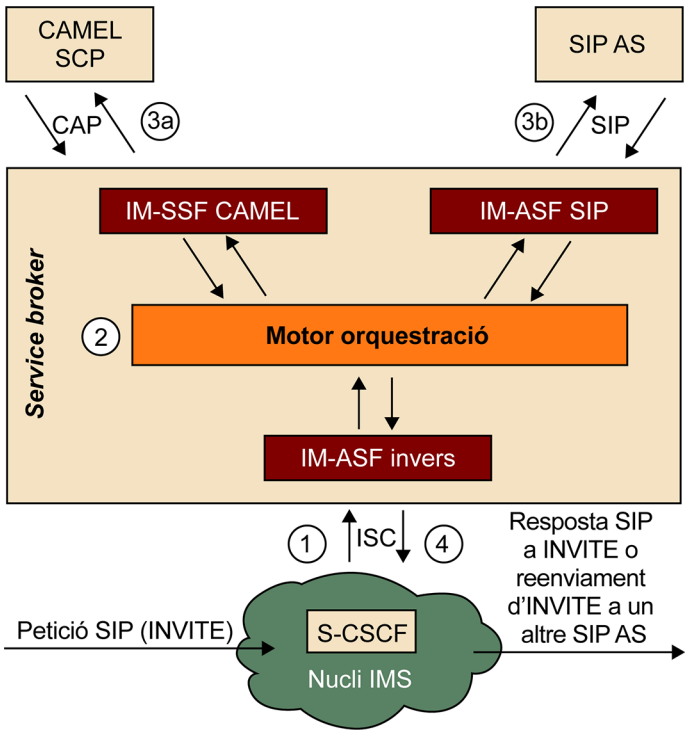
Tal com ja hem vist en l'anterior apartat, en el cas concret de xarxa IMS l'SB interactua amb l'S-CSCF via interfície ISC.

L'orquestració de servei dins del domini IMS està basada en un concepte d'agregació d'aplicacions. Aquest concepte habilita el lliurament de molts serveis en una sola sessió mitjançant l'encaminament de la sessió amb moltes

aplicacions. La cadena d'aplicacions per la qual passa una sessió habilita cada aplicació a complir el seu paper en el torn que li toqui. L'ordre en què es recorren les aplicacions depèn de la lògica de l'orquestració que veurem més tard.

En la Figura 21 podem veure un exemple d'aquesta orquestració entre el nucli IMS i l'SB, la qual és disparada per una petició de SIP rebuda des de l'S-CSCF. Dins de l'SB es produeix la traducció de protocols accedint primer al CAMEL SCP i després al SIP AS, abans d'enviar la resposta de retorn a l'S-CSCF.

Figura 21. Exemple d'orquestració mitjançant el *service broker*.



El MO gestiona la sessió tal com s'indica a continuació:

1) El MO és activat mitjançant l'IM-ASF invers per l'S-CSCF en enviar-li aquest una petició SIP per la interfície ISC (per exemple, un INVITE).

2) El MO encamina la sessió a moltes aplicacions mitjançant els mòduls d'interacció que hi són encarats. La ruta cap a múltiples aplicacions no és estàtica sinó determinada en temps real per lògica d'orquestració, la qual és seleccionada pel MO i descarregada dinàmicament (per exemple, des de la base de dades de subscripcions o HSS via interfície Sh, el MO es descarrega els iFC del perfil d'usuari per aplicar la lògica d'orquestració).

3) El MO reenvia la sessió a l'aplicació corresponent segons aquestes rutes configurades dinàmicament .

4) Una vegada la sessió ha passat per l'última aplicació en la cadena, el MO retorna la sessió a l'S-CSCF.

En aquest exemple (Figura 21), hem proposat un INVITE com a petició SIP, però no és necessàriament aquest missatge, ja que hi ha altres peticions SIP, com REGISTER, MESSAGE, SUBSCRIBE o NOTIFY.

Procés d'orquestració en el motor d'orquestració

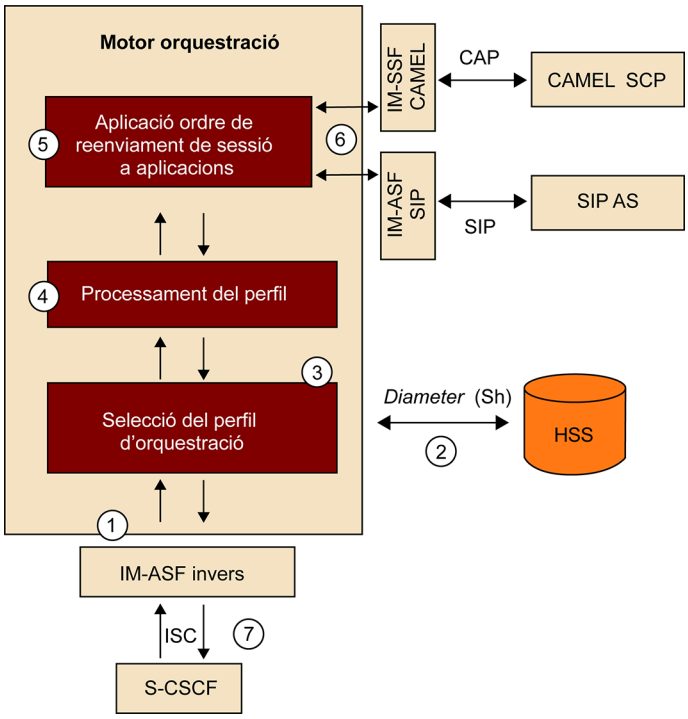
En la Figura 20 hem vist que el MO és el cor de l'SB. Però vegem com funciona exactament per dins i quins processos alberga per poder prendre les decisions d'orquestració quan arriba una petició de sessió.

Per a fer el servei d'orquestració, el MO requereix una lògica d'orquestració. Una lògica d'orquestració defineix les aplicacions per les quals el MO hauria de passar una sessió i l'ordre en què aquestes aplicacions han de ser invocades.

Volem reiterar que no hi ha una especificació estandarditzada sobre el diagrama de flux quant a funcions a exercir per l'SB a l'hora de fer el procés d'orquestració. Són les empreses privades les que han emplenat aquest buit amb propostes propietàries. Per això, el que mostrarem a continuació és una descripció genèrica de les fases per les quals passaria el MO a l'hora d'aplicar la lògica de l'orquestració.

El servei d'orquestració necessita fer principalment tres tasques, les quals es poden veure en la caixa del MO en la Figura 22. En aquesta figura també es pot veure pas a pas com s'apliquen els perfils d'orquestració des que una petició de sessió arriba de l'S-CSCF:

Figura 22. Aplicació en el MO de la lògica d'orquestració.



HSS

L'HSS conté informació de subscripció dels usuaris incloses les aplicacions a usar, i també els seu perfils d'orquestració (iFC emmagatzemats en el perfil de subscripció).

(5)Opcionalment, aquests perfils poden estar emmagatzemats localment en una base de dades en el mateix *service broker* en lloc d'estar en l'HSS (*home subscriber server*).

1) El servei d'orquestració rep una petició de sessió des de l'element de control de sessió corresponent (en aquest cas, de l'S-CSCF), que al seu torn és reexpedit al MO pel mòdul d'interacció.

2) El MO delega la funció de selecció del perfil al mòdul d'obtenció del perfil d'orquestració (iFC). Per a això, aquest es connecta via interfície Sh amb l'HSS[5].

3) Basant-se en la informació continguda en el mateix missatge de petició de sessió rebut, el mòdul d'obtenció del perfil selecciona el perfil d'orquestració a utilitzar per a aquesta sessió i el transfereix al MO per a usar-lo.

4) En el MO, el mòdul de processament elabora el pla de reexpedició de la sessió a les aplicacions que siguin necessàries i en l'ordre que sigui necessari.

5) El MO executa la lògica d'orquestració invocant la primera aplicació.

6) Quan la primera aplicació retorna el missatge de sessió, el MO invoca l'aplicació següent, i així fins que es compleixi tota la llista.

7) Quan aquest procés ha acabat es retorna el missatge de sessió a l'S-CSCF.

Exemple detallat d'aplicació dels iFC com a lògica d'orquestració en el cas particular de la funcionalitat SCIM (on solament es fa l'orquestració amb SIP AS)

Quan entra a l'SB (que té solament funcionalitat SCIM) una petició inicial de SIP reexpedit des de l'S-CSCF (per exemple, REGISTER, INVITE, SUBSCRIBE, MESSAGE, etc.), se segueixen els passos següents:

SCIM en l'S-CSCF

És relativament comú trobar la funcionalitat SCIM integrada en la mateixa plataforma on s'implementa l'S-CSCF.

Devolució de missatge

Si el *service broker* (SCIM) no troba un *service profile* per a un IMPU en concret, retorna el missatge SIP sense modificar a l'S-CSCF.

1) L'SB selecciona el *service profile* (llista d'IFC a aplicar) segons l'IMPU associat al subscriptor i si la trucada és entrant o sortint (*originating* o *terminating*). És a dir, si la trucada és de sentit entrant, l'IMPU associat al subscriptor s'agafa de la capçalera SIP From:, i si és de sentit sortint s'agafa de la capçalera SIP To:.

2) Començant per l'iFC de més alta prioritat (mirant el *priority level* de l'iFC) es comprova si el missatge SIP reexpedit des de l'S-CSCF compleix tots els *trigger points* que conformen aquest iFC.

3) Si no els compleix, l'SB consulta l'iFC següent per ordre de prioritat, i així fins que ja no quedin iFC per aplicar.

4) Si el missatge SIP compleix algun dels iFC, es reenvia al SIP AS associat (SIP URI). Si el SIP AS retorna el missatge SIP (que pot ser fins i tot modificat), l'SB continua aplicant la resta d'iFC de la llista des del punt en què s'havia quedat i per ordre de prioritat fins que ja no quedin iFC per aplicar.

Quan no queden iFC per aplicar, finalment reenvia la petició SIP de tornada a l'S-CSCF perquè l'encamini al destinatari final.

4.5. *Service enablers* o habilitadors de servei de VoLTE

A continuació descriurem els *service enablers* més comuns que podem trobar per a proveir el servei de VoLTE (almenys els oferts per les empreses especialitzades en provisió de programari per a aquest tipus de serveis IMS).

MMTel (*multimedia telephony*)

El servei de telefonia multimèdia de 3GPP/TISPAN (en anglès *multimedia telephony*) és un estàndard basat en IMS (utilitza el protocol IP per a transport i SIP per a senyalització de serveis) que permet als usuaris establir comunicacions multimèdia. Presta els serveis estandarditzats següents:

MMTel i els serveis suplementaris

El GSMA ha definit les especificacions IR.92 i IR.94 per definir les característiques del servei de telefonia en IMS per a trucades de veu i vídeo respectivament tant del costat de l'UE com del costat de l'*application server*. També ha definit l'IR.51 per especificar les característiques del servei de VoWiFi. Aquestes especificacions busquen maximitzar la interoperabilitat entre diferents fabricants.

- Conversa de veu bidireccional.
- Transmissió de vídeo unidireccional o bidireccional.
- Missatgeria en text
- Transferència de fitxers
- Compartició de fitxers d'àudio, vídeo i fotos.
- Capacitat d'afegir o eliminar components multimèdia (àudio o vídeo) segons es necessiti durant una sessió

Aquest habilitador de servei és usat típicament per a implementar servidors de telefonia (TAS o *telephony application server*) en els quals s'ofereixen els serveis d'emulació de xarxa GSM (és a dir, implementació de tots els serveis telefònics que ja venien) i serveis suplementaris per a trucades VoLTE i VoWiFi (especificats en els perfils del GSMA IR.92, IR.94 i IR.51). Com a serveis suplementaris, hi ha, entre d'altres: transferència de trucada automàtica, bloqueig de trucada, identificació del qui truca, trucada en espera, etc.

TAS virtualitzat

Molts fabricants de SIP AS ofereixen el seu servidor d'aplicacions en format VNF (*virtualized network function*), de manera que pot ser utilitzat en un entorn virtualitzat que compleixi l'especificació de l'ETSI de NFV-MANO, que veurem en el mòdul següent.

SCC (*service centralization & continuity*)

El servei de centralització i continuïtat utilitza mètodes definits per 3GPP com a part d'IMS Centralized Services (ICS) per a ancorar les trucades en aquest servidor assegurant coherència en la sessió tant si accedeixen des del domini de commutació de circuits (CS) com des de commutació de paquets (PS). Per a totes les trucades que estan ancorades, l'SCC-AS actua com un B2BUA establint els vessants de les trucades a tots els punts finals des del SIP INVITE fins al SIP BYE.

SCC

El GSMA va publicar l'especificació IR.64, on descriu com ha de ser el servei SCC.

Aquest habilitador està en la implementació de servidors d'aplicacions de continuïtat de trucada de veu (VCC o *voice call continuity*). El VCC permet la continuïtat d'una sessió de veu quan l'usuari es mou amb el seu telèfon entre LTE i xarxes no-LTE del tipus *circuit switched* (CS), en les quals s'utilitzen tecnologies com GSM (*global system for mobile communications*) i UMTS (*universal mobile telecommunication system*). Aquest servei també s'anomena comercialment SRVCC (*single radio voice call continuity*), encara que han aparegut noves versions millorades com l'eSRVCC (*enhanced single radio voice call continuity*).

SRVCC i eSRVCC

La diferència entre l'un i l'altre és que el primer solament ancora la trucada en l'àmbit de senyalització (solament missatges SIP), mentre que el segon implementa també un ancoratge en l'àmbit de fluxos multimèdia (fluxos de veu i/o vídeo).

CONF (*multiparty conference call*)

Aquest habilitador ofereix la capacitat d'establir i enllaçar múltiples sessions multimèdia. Normalment, hi ha la part que gestiona exclusivament la senyalització de les sessions, que és implementada en un SIP AS, i per al processament dels fluxos multimèdia s'utilitza l'element específic que dona aquesta funció en el nucli IMS, l'MRF. El servei de multiconferència per VoLTE és especificat a l'IR.92 del GSMA.

Normalment, aquest servei és inclòs en el TAS, encara que es pot implementar com un servidor per separat.

Group messaging

Aquest habilitador proporciona missatgeria instantània 1-a-1 o en grup i ha estat estandarditzat per diverses entitats, cadascuna de les quals li assigna un nom diferent: l'IETF l'anomena *instant messaging*, 3GPP, IMS *messaging*, i l'OMA SIMPLE, *instant messaging*. No obstant això, el més usat és el que li ha atorgat el GSMA: RCS (*rich communication service*).

Curiositat sobre RCS

El GSMA va batejar la primera versió de RCS (l'any 2012) amb el nom de *Joyn*.

L'RCS inclou, a més, altres serveis com agenda de contactes, trucades de veu i vídeo tant-com-puc, compartició de continguts i fitxers, etc.

L'RCS és l'equivalent de *Whatsapp*, però implementat per a IMS.

Resum

Les xarxes NGN ens mostren un nou paradigma de convergència de xarxes de transport i d'independència dels serveis pel que fa a aquestes xarxes, tot això amb el protocol IP com a pedra angular. Ofereixen un marc en el qual els proveïdors de serveis poden desenvolupar noves aplicacions i serveis sense preocupar-se de la tecnologia subjacent en l'equip d'usuari (UE). A més, les xarxes NGN garanteixen la qualitat de servei (QoS) d'extrem a extrem, oferint interoperabilitat amb xarxes i serveis existents avui dia (RTC / RDSI o telefonia mòbil).

Avui dia ja hi ha operadors que han invertit i implementat xarxes i serveis que compleixen amb NGN, com per exemple la xarxa de LTE Advanced i el servei de VoLTE. És precisament el mercat de la telefonia mòbil el que impulsa, sota el guiatge de 3GPP, noves especificacions i models de referència que abstreuen cada vegada més els serveis de la tecnologia de xarxa, tal com ja passa amb l'especificació de 5G.

Quant a la **capa de transport**, LTE és una xarxa d'accés especificada per 3GPP que ofereix les característiques de les NGN. La interacció d'aquesta capa amb el nucli IMS (capa de servei) és gràcies a la subcapa de processament de transport protagonitzat pel PCRF que controla la definició de les regles PCC. Aquestes regles marquen el comportament del trànsit IP en l'àmbit de QoS quan travessen l'EPC (*evolved packet core*).

Altres tecnologies sense fil, com Wi-Fi, han estat incorporades perquè puguin integrar-se amb l'EPC i oferir als operadors de telefonia mòbil una manera natural d'estendre la seva cobertura més enllà dels seus dominis administratius. 3GPP ha inclòs aquesta integració en els seus models de referència per donar forma al servei VoWiFi.

També cada vegada, més apareixen tecnologies que integren serveis web i comunicacions multimèdia, especialment webRTC. En aquest cas, 3GPP també ha fet un esforç per integrar-ho.

Respecte a la **capa de servei**, 3GPP ha definit el nucli IMS, que es basa en la definició, d'una banda, d'unes entitats funcionals (CSCF) que processen i encaminen els missatges d'establiment de sessió de serveis, i, d'una altra, d'elements de magatzematge d'informació de subscripció d'usuari en l'àmbit de servei (HSS). Aquests missatges estan basats en el protocol SIP (definit per l'IETF) però amb unes extensions en la seva definició per a adaptar-se a IMS. Amb el protocol SIP, un usuari pot invocar una sessió de qualsevol servei multimèdia (veu o vi-

deoconferència) servint-se d'altres protocols encapsulats en la mateixa senyalització SIP, com per exemple SDP, que s'usa per a negociar paràmetres de QoS d'extrem a extrem amb l'altre usuari o servidor d'aplicació o AS.

En l'àmbit de la **capa d'aplicació**, l'entitat que millor representa un servei NGN/IMS és el servidor d'aplicacions (AS), que s'interconnecta a l'element de control de sessió del nucli IMS (S-CSCF) amb una interfície basada en el protocol SIP anomenada ISC (*IMS service control*). Des del punt de vista del nucli IMS, la manera de saber cap a quin servidor d'aplicacions (AS) redirigir una petició SIP és accedir a la base de dades de subscripcions (HSS) i obtenir les iFC o *initialFilter Criteria* associades al perfil de servei de l'usuari. Els iFC contenen informació que diu a l'S-CSCF cap a quin AS cal enviar una petició SIP en funció dels valors de certs camps de la capçalera del mateix missatge.

Els serveis NGN s'adapten al paradigma SOA, el qual es basa en la integració de components de serveis més senzills, reutilitzables, independents entre ells i autocontinguts per a poder crear fàcilment nous serveis de valor afegit. Aquests components s'anomenen habilitadors de serveis (*service enablers*). Diversos exemples d'aquests habilitadors reutilitzables són els serveis de presència o gestió de llista de grups.

Quan parlem d'integració de servei, hem de parlar obligatòriament de la coordinació i orquestració de components de servei, i és aquí on sorgeix un element clau en la provisió de serveis NGN: el *service brokerx* (SB).

L'SB és un element de xarxa que gestiona eficientment la interacció i la composició dels serveis. Està situat entre la capa de servei (servidors d'aplicacions i habilitadors de servei) i la xarxa convergent (representada pel nucli IMS), i està desvinculat tradicionalment dels elements d'encaminament de trucades i dels entorns de creació i execució de serveis. La lògica d'orquestració és quelcom cosa que l'SB pot obtenir de l'HSS o de polítiques pròpies.

Exercicis d'autoavaluació

1. A continuació mostrem una llista de definicions de blocs funcionals que estan inclosos en el nucli IMS definit per 3GPP.

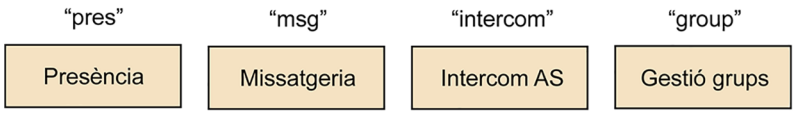
a) És l'element frontera del nucli IMS que es connecta directament amb l'usuari (client IMS) i, per tant, el primer SIP *proxy* que rep i processa les peticions SIP.
b) És l'element que fa frontera amb altres nuclis IMS d'altres operadors. Quan un missatge SIP ha d'encaminar-se cap a un altre domini, passa per aquest element just abans de sortir cap a l'element homòleg de l'altre domini administratiu.
c) És l'element central del nucli IMS on els clients es registren. A més, és on es mira per primera vegada el Request-URI (destinació final del missatge SIP) per prendre la decisió d'encaminament cap a un altre domini IMS, cap a un servidor d'aplicacions (AS) o cap a una altra xarxa heretada (RTC, per exemple).
d) És un SIP *proxy* que s'encarrega de trobar l'S-CSCF correcte d'un usuari en concret (consultant l'HSS) i encaminar el missatge SIP cap a ell. Un dels elements que més el consulta és el P-CSCF.
e) És l'element que fa de frontera amb xarxes RDSI o RTC. D'una banda, rep i processa les peticions de sessions SIP que rep des de la BGCF per convertir-les en peticions equivalents a les xarxes heretades. És com una VoIP en l'àmbit de senyalització.

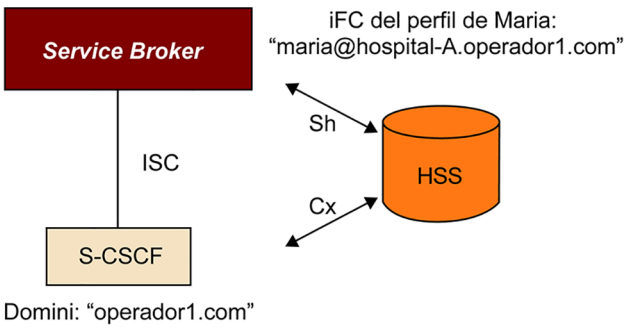
La llista d'elements és la següent:

1. I-CSCF
2. IBCF
3. P-CSCF
4. MGCF
5. S-CSCF
6. BGCF

Relaciona cadascuna de les definicions amb un dels elements. (NOTA: en la segona llista hi ha un element extra que no s'ha d'utilitzar.)

2. L'hospital A vol donar un servei d'atenció remota a persones de la tercera edat que estan a casa seva. Cada pacient disposa d'un dispositiu penjat del coll que té dos botons: un de vermell perquè en prémer-lo l'hospital s'adoni que el seu estat ha canviat a «no em trobo bé», i un de blau per a poder parlar directament amb una infermera (que escolta permanentment) sense necessitat de trucar per telèfon. L'hospital ha contractat l'operador1.com per disposar de tots els pacients registrats en el seu domini i tenir associat el seu servei d'atenció remota. En la figura següent es mostren els components que estan a disposició de l'hospital per a poder proporcionar qualsevol servei:





Contesteu les preguntes següents:

a) Quin paper té el *service broker*?
b) Segons la figura anterior, quins components creieu que s'usarien en aquest servei d'atenció a gent de la tercera edat?
c) Quins missatges SIP creieu que utilitzarà l'aparell d'avís segons el botó premut?

d) Segons la figura, quins components creieu que hauria d'integrar el *service broker* per a aquest cas?

e) Per a una pacient anomenada Maria, que té el perfil emmagatzemat en l'HSS, proposeu els iFC emmagatzemats per a ser consultats per l'S-CSCF de nucli IMS.

f) Feu el mateix en el cas del *service broker* per a l'orquestració del servei.

Solucionari

1.

a) P-CSCF
b) IBCF
c) S-CSCF
d) I-CSCF
e) MGCF

2.

a) El *service broker* integra i coordina diversos serveis elementals en un de sol de més valor afegit. Per a l'usuari, la complexitat del servei queda emmascarada, ja que solament existeix hi ha un servidor d'aplicació amb el qual interactuar, el representat pel *service broker*: PSI URI: servei-atenció-remota@hospital-A.operador1.com

b) Es detecten dos serveis que, conjuntament, poden formar aquest nou servei. El primer servei és el de presència, amb el qual en prémer el botó vermell l'estat d'aquests components canvia a «no em trobo bé» perquè el personal dedicat de l'hospital (un infermer o infermera) pugui veure'l. El segon servei és el d'Intercom (trucada que va sempre a la mateixa destinació), que s'activa amb el botó blau. Aquest servei estableix directament una connexió de veu amb un infermer o infermera sense necessitat de marcar cap número.

c) Per al servei de canvi d'estat, enviaria un missatge NOTIFY amb el nou estat al servidor d'aplicació (representat pel *service broker*). Per al servei de trucada estàtica, seria un missatge INVITE.

d) Solament es necessitarien dos components: el de presència, on s'enviarien els NOTIFY, i el servidor d'aplicació anomenat Intercom, que rebria l'INVITE d'inici de trucada.

e) L'iFC del perfil de Maria que necessita l'S-CSCF per a enviar els NOTIFY a *service broker* seria:

Mètode SIP	NOTIFY
OR	
Mètode SIP	INVITE
AND	
Capçalera SIP **Valor capçalera SIP**	To: .*hospital-A.operador1.com.*

f) Hi haurà dos iFC, un per cada tipus de mètode:

iFC de presència associat a l'AS pres@hospital-A.operador1.com

Mètode SIP	NOTIFY
AND	
Capçalera SIP **Valor capçalera SIP**	To: pres@hospital-A.operador1.com

iFC de presència associat a l'AS intercom@hospital-A.operador1.com

Mètode SIP	INVITE
AND	
Capçalera SIP **Valor capçalera SIP**	To: intercom@hospital-A.operador1.com

Glossari

3GPP Third Generation Partnership Project. Entitat d'estandardització de tecnologia mòbil, com UMTS, LTE i IMS, entre d'altres.

AF *Application function*. Des del punt de vista de la xarxa de transport, l'AF simbolitza l'element de la capa de servei que té contacte directe amb els elements de la subcapa de control de transport.

ARP *Allocation and retention priority*. Paràmetre que indica la importància o nivell de prioritat d'un IP-CAN *bearer*.

AS *Application server*. Element que presta un servei a les xarxes NGN.

AVP *Attribute value pair*. En el protocol Diameter i en un context de xarxes NGN, paràmetres que contenen informació sobre una sessió de reserva de recursos.

B2BUA *Back-to-back user agent*. Dos agents d'usuari SIP en una mateixa màquina però interconnectats entre ells per algun tipus de lògica o funcionalitat.

BBERF *Bearer binding and event reporting function*. Funció d'associació de túnels i reportament d'esdeveniments en el model de referència PCC de 3GPP.

BGCF *Breakout gateway control function*. Element definit en el nucli IMS 3GPP que s'encarrega de seleccionar el següent salt d'una petició SIP quan l'adreça de destinació de la trucada no és un identificador típic SIP URI.

CAMEL *Customized applications for mobile networks enhanced logic*. Conjunt d'estàndards definits per l'ETSI i 3GPP, dissenyats per a permetre a l'operador definir serveis sobre l'estàndard de serveis GSM i serveis UMTS.

CSE *CAMEL service environment*. Entorn de servei que descriu CAMEL per a l'entorn de creació de serveis i per als nodes de la xarxa que interactuen per entregar serveis al subscriptor.

DIAMETER Protocol per al desenvolupament d'aplicacions d'AAA evolució del RADIUS.

DNS *Domain name server*. Servidor de resolució de noms d'amfitrió a adreça IP.

I-CSCF *Emergency call session control function*. Component del nucli IMS que exerceix d'element que processa una trucada d'emergència IMS. És un element definit per 3GPP.

EPC *Evolved Packet Core*. Xarxa troncal de la xarxa LTE segons 3GPP.

EPS *Evolved Packet System*. Model de referència de 3GPP per a la capa de transport tant en la part de xarxa troncal (EPC) com de xarxa d'accés ràdio (E-UTRAN).

EPS *bearer* *Evolved packet system bearer*. Canal virtual amb unes característiques de QoS i amplada de banda particulars des de la PDN-GW fins al terminal d'usuari (model de referència del PCC de 3GPP).

ETSI European Telecommunications Standards Institute. Organització d'estandardització de la indústria de les telecomunicacions (fabricants d'equips i operadors de xarxes) d'Europa amb projecció mundial.

E-UTRAN *Evolved UMTS Terrestrial Radio Access Network*. Xarxa d'accés ràdio de LTE segons 3GPP.

GBR *Guaranteed bit rate*. Taxa garantida de bit. És usada com a paràmetre de caracterització dels IP-CAN *bearers*.

GERAN GSM Edge Radio Access Network. Xarxa d'accés ràdio de GPRS segons 3GPP.

GPRS General Packet Radio Service. Extensió del GSM per a transmetre paquets que permet velocitats de transferència de 56 a 144 kb/s.

GSM *Global system for mobile communications*. Estàndard de telefonia mòbil de segona generació.

GTP *GPRS tunneling protocol*. Protocol de tunelització usat en GPRS per a transportar paquets IP.

HLR *Home Location Register*. En el món de la telefonia mòbil, base de dades que emmagatzema informació de subscripció i de localització d'usuaris.

HSS *Home Subscriber Server*. Base de dades que emmagatzema la informació de subscripció d'un usuari juntament amb informació d'autenticació i autorització en l'àmbit de servei. És un model de referència de 3GPP.

HTTP *Hypertext transfer protocol*. Protocol usat en les transaccions de la WWW.

HTTP Digest Mecanisme d'autenticació que utilitza MD5 com coixinet. És usat en serveis web.

IBCF *Interconnection border control function*. Funció de control de passarel·la fronterera amb una altra xarxa troncal en el model de referència de 3GPP i de l'ETSI-TISPAN en el nucli IMS.

I-CSCF *Interrogating call session control function*. Component del nucli IMS que exerceix d'element encaminador de la senyalització SIP cap a l'S-CSCF correcte dins del seu mateix domini. És un element definit per 3GPP.

IETF Internet Engineering Task Force. Entitat d'estandardització oberta responsable de millorar els protocols i els estàndards que defineixen la tecnologia d'internet.

IMPI *IP multimedia private identity*. Identitat privada d'un usuari.

IMPU *IP multimedia public identity*. Identitat pública d'un usuari.

IMS *IP Multimedia Subsystem*. Estàndard definit per 3GPP per proveir serveis multimèdia en telefonia mòbil basats en protocols definits per IETF (SIP, RTP o Diameter).

IMS AKA IMS Authentication and Key Agreement. Protocol basat en una clau secreta de llarga durada compartida entre la ISIM i el centre d'autenticació de la xarxa d'accés.

IN Intelligent Networks. Plataforma basada en la interconnexió de nodes de xarxes de commutació de circuits on hi ha aplicacions informàtiques, centrals de commutació i sistemes de bases de dades en temps real, enllaçats mitjançant sistemes de senyalització avançats, per a proveir la nova generació de serveis.

IP *Internet Protocol*.

IP-CAN Internet Protocol Connectivity Access Network. Xarxa d'accés que proporciona connectivitat IP.

IP-CA *bearer* Canal virtual d'un IP-CA.

IPTV *IP television*. Servei de televisió basat en el protocol IP. Pot estar basat en IMS o definir la seva pròpia plataforma de gestió i control del servei.

ISIM IMS Subscriber Identity Module. Targeta intel·ligent amb informació sobre la identitat d'un usuari IMS.

ITU-T International Telecommunications Union - Telecommunication. Sector de normalització de les telecomunicacions de l'ITU en què s'estableixen normes que comprenen des de la funcionalitat bàsica de la xarxa i la banda ampla fins als serveis de les xarxes de propera generació.

LTE Long Term Evolution. Estàndard definit per 3GPP per a l'evolució de la telefonia mòbil.

MBR *Maximum bit rate*. Taxa de bit màxima. És usada com a paràmetre de caracterització dels IP-CAN *bearers*.

MGCF *Media gateway control function*. Funció de control de passarel·la de mitjans en el model de referència de 3GPP per al nucli IMS.

MME Mobility Management Entity. Entitat que gestiona la mobilitat dels terminals d'usuari a la xarxa d'accés ràdio del model EPS. És un model de referència de 3GPP.

MO Motor d'orquestració en el *Service Broker*.

MRB Multimedia Resource Broker. Funció de gestió de recursos de mitjans en el model de 3GPP per al nucli IMS.

MRFC *Media resource function control*. Funció de control de recursos de mitjans en el model de referència de 3GPP i ETSI-TIPAN per al nucli IMS.

MRFP *Media resource function processor*. Funció de processament de recursos de mitjans en el model de referència de l'ETSI-TISPAN i de 3GPP per al processament de transport.

NAPT *Network address and port translation*. Traducció de ports i encaminament IP.

NAT *Network address translation*. Traducció d'encaminament IP entre un encaminament privat i un altre de públic.

NGN *Next generation network*. Xarxa de propera generació.

NNI *Network-network interface*. Frontera entre dues xarxes diferents (dues xarxes troncals o una xarxa troncal i una xarxa d'accés).

NSWO Non-Seamless WLAN Offload. Prestació definida per 3GPP que indica al terminal mòbil que usi la interfície SWu (túnel IPsec) per a trucades IMS però que usi la Wi-Fi directament i de manera transparent per a trànsit no-IMS.

OCS Online Charging System. Sistema de control de facturació en línia per a controlar en temps real la despesa en un servei. Element del model de referència PCC de 3GPP.

OFCS Offline Charging System. Sistema de control de facturació diferit per a generar posteriorment les factures d'ús d'un servei. Element del model de referència PCC de 3GPP.

OFDMA Orthogonal Frequency-Division Multiple Access. Versió multiusuari de la multiplexació per divisió de freqüències ortogonals.

OMA Open Mobile Alliance. Organització que desenvolupa estàndards oberts per a la indústria de la telefonia mòbil.

OSA/Parlay Open Service Access / Parlay. API per a l'accés d'aplicacions als recursos de les xarxes de telecomunicacions.

PCC *Policy control and charging*. Control de les polítiques de QoS i facturació, definides en el model de referència de 3GPP per a controlar la xarxa de transport.

PCEF *Policy and charging enforcement function*. Funció d'aplicació de polítiques i facturació en el model de referència PCC de 3GPP.

PCRF *Policy charging and rules function*. Grups de funcions que conformen el control d'admissió i recursos del model de referència PCC de 3GPP.

P-CSCF *Proxy call session control function*. Component del nucli IMS que exerceix d'element fronterer amb l'equip d'usuari en l'àmbit de senyalització SIP, definit per 3GPP.

PDN-GW *Packet data network gateway.* Element de l'EPC frontera que interconnecta amb la xarxa troncal d'un altre operador.

PSI *Public service identifier*. Identificador de servei públic que identifica qualsevol element de destinació d'una trucada SIP i que no és un usuari.

QCI *QoS class identifier*. Paràmetres que defineixen el comportament de QoS del trànsit associat a un túnel d'EPS.

QoS *Quality of service*. Qualitat de servei.

RADIUS Remote Authentication Dial-In User Server. Protocol d'autenticació i autorització definit per IETF per a aplicacions d'accés a la xarxa o mobilitat IP.

RDSI Xarxa Digital de Serveis Integrats.

REST *Representational State Transfer*. Conjunt de principis d'arquitectura per a descriure qualsevol interfície entre sistemes que utilitzi directament HTTP per a obtenir dades o indicar l'execució d'operacions sobre les dades, en qualsevol format (XML, JSON, etc.) sense les abstraccions addicionals dels protocols basats en patrons d'intercanvi de missatges.

RFC *Request For Comment*. Publicacions on es plasmen els estàndards que defineix IETF.

RTC Xarxa telefònica commutada.

RTP *Real time protocol*. Protocol basat en UDP per a transmetre fluxos multimèdia (àudio, vídeo) en temps real.

SAE System Architecture Evolution. Vegeu **EPS**.

SBC *Session border controller*. Element col·locat a les fronteres administratives d'una xarxa gestionada o domini (per ex., SBC: P-CSCF o IBCF).

SCIM Service Capability Interaction Manager. Funcionalitat proposada per 3GPP per a orquestrar serveis i habilitadors quan el servei s'invoca des del nucli IMS, en concret des de l'S-CSCF.

S-CSCF Serving call session control function. Component del nucli IMS que exerceix de registrador de l'usuari en l'àmbit de capa de control de servei, i d'encaminador de la senyalització cap a altres elements que finalitzin la trucada dins del mateix domini o d'un altre diferent. És un element definit per 3GPP.

SDP *Session description protocol*. Protocol adherit a la senyalització SIP per a negociar paràmetres multimèdia d'establiment de sessió, és a dir, còdecs o ports UDP on enviar els fluxos RTP.

SGSN/GGSN Serving GPRS Support Node / Gateway GPRS Support Node. Xarxa troncal GPRS. L'SGSN s'encarrega de la mobilitat del mòbil a més de donar-li accés a la xarxa de dades mòbils, d'autenticar i assignar la qualitat del servei a utilitzar per cada terminal. El GGSN és la porta d'enllaç o punt central de connexió cap a l'exterior o la PDN d'una xarxa mòbil. Les xarxes externes poden ser internet o una xarxa corporativa.

SGW *Serving gateway*. Component de l'EPC de 3GPP que fa d'ancoratge de les connexions IP per garantir el servei de mobilitat en terminals mòbils.

SIP *Session initiation protocol*. Protocol definit per IETF per a establir i negociar sessions de serveis multimèdia.

SLA *Service level agreement*. Acord que defineix les característiques del servei per a un subscriptor.

SLF *Subscriber location function*. Element del model de referència d'IMS de 3GPP que s'encarrega de trobar l'HSS correcta on se situa un perfil d'usuari buscat.

SOA *Service object architecture*. Estil d'arquitectura l'objectiu de la qual és aconseguir el desacoblament entre els components de programari que interactuen entre ells.

SOAP *Simple object access protocol*. Protocol simple basat en XML per a intercanviar informació en un entorn distribuït i descentralitzat.

SPR Subscription Profile Repository. Funció d'emmagatzematge de perfils d'usuari en l'àmbit de capa de transport en el model PCC de 3GPP.

SS7 *Signalling system number 7*. Sistema de senyalització número 7 usat en els enllaços troncals de telefonia.

TCP *Transport control protocol*. Protocol de capa 4 per a enviar paquets amb confirmació.

THIG *Topology hiding inter-network gateway*. Funcionalitat d'emmascarament de topologia de xarxa que elimina de les capçaleres SIP qualsevol informació que pugui revelar la topologia de la xarxa.

UA *User agent*. En el protocol SIP, punt inicial o de terminació d'un missatge SIP. Normalment, és implementat per un client o un servidor d'aplicacions SIP (SIP AS).

UDDI Universal Description Discovery and Integration. Element de l'arquitectura SOA que s'usa perquè proveïdors de servei puguin registrar informació sobre els serveis que ofereixen i fer-los públics.

UDP User Datagram Protocol. Protocol de capa 4 per a enviar paquets sense confirmació.

UE *User equipment*. Equip d'usuari. Pot contenir un o més terminals.

UMTS *Universal mobile telecommunications system*. Sistema universal de telecomunicacions mòbils de tercera generació de l'ITU, successor del sistema GSM.

UNI *User-network interface*. Frontera de l'àmbit estrictament d'usuari i de l'àmbit de la xarxa d'accés o servei.

URI *Uniform resource identifier*. Identificador uniforme de recursos.

UTRAN UMTS Terrestrial Radio Access. Xarxa d'accés ràdio d'UMTS segons 3GPP.

VCC Voice Call Continuity. Habilitador de servei definit per 3GPP que permet la continuïtat d'una sessió de veu mentre l'usuari es mou d'una xarxa d'accés a una altra de tecnologia diferent.

WSDL *Web services description language*. Llenguatge basat en XML usat per a descriure els serveis web que ofereix un negoci.

XCAP XML Configuration Access Protocol. Protocol que permet a un client llegir, escriure i modificar dades de configuració d'una aplicació emmagatzemades en un servidor en format XML.

XML *Extensible markup language*. Llenguatge de marques desenvolupat per W3C que permet definir la gramàtica de llenguatges específics per a estructurar documents grans.

Bibliografia

3GPP (juny de 2018). *Recomanació TS 23.203 v15.3.0: Policy and charging control architecture*

3GPP (març de 2018). *Recomanació TS 23.228 v15.2.0: IP multimedia subsystem (IMS)*

3GPP (juny de 2018). *Recomanació TS 29.214 v15.4.0: Policy and charging control over Rx reference point*

3GPP (juny de 2018). *TS 23.141 v15.0.0: Presence service; architecture and functional description*

3GPP*TS 23.198 V9.0.0. Open Service Access (OSA). Stage 2.*

3GPP (juny de 2018). *TS 23.216 v15.2.0 (2018-06): Single radio voice call continuity (SRVCC)*

3GPP (juny de 2018). *TS 24.173 v15.1.0: IMS Multimèdia Telephony Communication Service and Supplementary Services*

Hurwitz, J.; Bloor, R.; Kaufman, M.; Halper, F. (2009). *SOA for dummies*(2a. ed.).

ITU-T Recomanació Y.2012 (abril de 2010). *Functional requirements and architecture of next generation networks*

ITU-T Recomanació Y.2018 (setembre de 2009). *Mobility management and control framework and architecture within the NGN transport stratum*

ITU-T Recomanació Y.2111 (novembre de 2011). *Resource and admission control functions in next generation networks*

Poikselka M.; Mayer G. (2009). *The IMS: IP multimedia concepts and services*(3a. ed.)

Enllaços d'interès:

Exemples de fluxos de trucades IMS:http://www.eventhelix.com/realtimemantra/telecom/

OMA Presence Simple: http://www.openmobilealliance.org/technical/release_program/presence_simple_v1_1.aspx

SOAP: http://www.w3schools.com/soap/soap_intro.asp

WDSL: http://www.w3.org/tr/wsdl