NGN/IMS a fons

Víctor Huertas García

PID_00175627

Universitat Oberta de Catalunya

Índex

Introducció..... 5

Objectius..... 6

1. Arquitectura funcional d'NGN/IMS..... 7
1.1. Elements que defineixen l'arquitectura 8
1.1.1. Entitat funcional 8
1.1.2. Punt de referència 8
1.2. Capa de Transport 8
1.2.1. Arquitectura de referència de la ITU-T 9
1.2.2. Arquitectura de referència de l'ETSI-TISPAN 30
1.2.3. Arquitectura de referència del 3GPP 41
1.3. Capa de Servei 51
1.3.1. Components del nucli IMS 53
1.3.2. Components de magatzematge d'informació de subscripció 65
1.3.3. Altres components del model de l'ETSI-TISPAN de control de Servei 68
1.3.4. Altres components del model de la ITU-T de control de Servei 69
1.3.5. Components de la subcapa de Distribució de Contingut 70
1.3.6. Subcapa de Suport a Serveis i Suport a Aplicacions 72

2. Mecanismes de garantia de recursos i QoS en xarxa de transport..... 73
2.1. Mode *push*..... 73
2.2. Mode *pull*..... 76

3. Protocols bàsics emprats en les xarxes NGN i IMS..... 78
3.1. Protocol SIP 78
3.1.1. Entitats SIP 79
3.1.2. Missatges SIP 79
3.1.3. Extensions per a IMS 82
3.2. Protocol DIAMETER 84
3.2.1. Nodes i agents Diameter 85
3.2.2. Missatges Diameter 86
3.3. Protocol H.248 / MEGACO 87

4. Exemples de fluxos de trucades en NGN IMS..... 88
4.1. Adhesió a la xarxa 88

4.1.1. Fase d'autenticació de l'equip d'usuari i assignació d'IP 88
4.1.2. Fase de registre en el nucli IMS 90
4.2. Establiment de sessions de serveis 93
4.2.1. Sessió IMS de servei de veu 93
4.2.2. Servei de Presència 99

Resum 102

Exercicis d'autoavaluació 105

Solucionari 107

Glossari 111

Bibliografia 120

Annex 121

Introducció

Un nou paradigma ha sorgit en el món de les xarxes de telecomunicacions i els seus serveis: les xarxes de propera generació o xarxes NGN, que fan que qualsevol xarxa que pugui transmetre paquets IP es converteixi en una xarxa multiservei amb garantia de qualitat de servei i no monoservei, com succeeix ara amb les xarxes existents de telefonia fixa/mòbil. A partir d'ara els serveis oferts als usuaris i les xarxes de transport ja no estaran íntimament vinculats.

Hi ha moltes entitats d'estandardització i especificació de tot el món (governamentals o no) que estan actualment involucrades a definir les xarxes NGN. Però entre aquestes hi ha un grup especialment actiu en la generació de documentació, com per exemple la ITU-T, l'ETSI-TISPAN i sobretot el 3GPP (entitat que ha especificat IMS).

Cadascuna d'aquestes entitats dóna la seva pròpia versió de com es defineixen les xarxes NGN i genera la seva documentació pròpia. Encara que en termes generals són models de referència molt similars, les diferències més importants entre uns i altres es troben en la distribució de les funcionalitats en blocs adaptant-se a una tipologia de xarxa en concret. Per exemple, el model ETSI-TISPAN es focalitza en xarxes fixes (xDSL) i la del 3GPP en xarxes mòbils. La ITU-T segueix un model més genèric sense cap especialització. Hi ha altres entitats, potser no tan actives en generació de documentació, que també han aportat el seu granet de sorra com, per exemple, CableLabs amb el seu model de referència PacketCable 2.0, especialitzat en integració en NGN de xarxes de cable (híbrid fibra i coaxial).

Web recomanat

Més informació sobre PacketCable 2.0 a: http://cablelabs.com/packetcable/specifications/specifications20.html

És important que tingueu en compte que, malgrat que són molt similars, aquests models de referència de les diferents entitats d'estandardització poden aparèixer indistintament esmentats en multitud d'articles i documentació diversa sobre les xarxes NGN.

És per això que val la pena que seleccionem tres models representatius (ITU-T, ETSI-TISPAN i 3GPP) i vegem les característiques més importants de cadascun.

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 la ITU-T, l'ETSI-TISPAN i el 3GPP per a les subcapes següents de la capa de transport.
- Subcapa de processament de transport.
- Subcapa de control de transport: adhesió a la xarxa i control d'admissió i recursos.

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

3. Per a la capa de servei, conèixer els components del nucli IMS del 3GPP i les diferències amb els models equivalents de l'ETSI-TISPAN i la ITU-T.

4. Identificar els punts de referència (o interfícies) entre blocs funcionals del nucli IMS.

5. Identificar i conèixer els punts de referència (o interfícies) entre el nucli IMS i la capa de transport.

6. Identificar altres blocs funcionals en la capa de servei que les entitats d'estandardització ETSI-TISPAN i ITU-T afegeixen als estrictament definits en el nucli IMS i que complementen altres funcionalitats de provisió de servei.

7. Conèixer els dos mecanismes que les xarxes NGN defineixen en el procés de reserva de recursos i garantia de QoS en la xarxa de transport durant l'establiment de la sessió de servei: mode *push* i mode *pull*.

8. 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.

9. Conèixer els passos que un terminal ha de fer per a accedir a la xarxa d'accés i posteriorment poder accedir als serveis IMS.

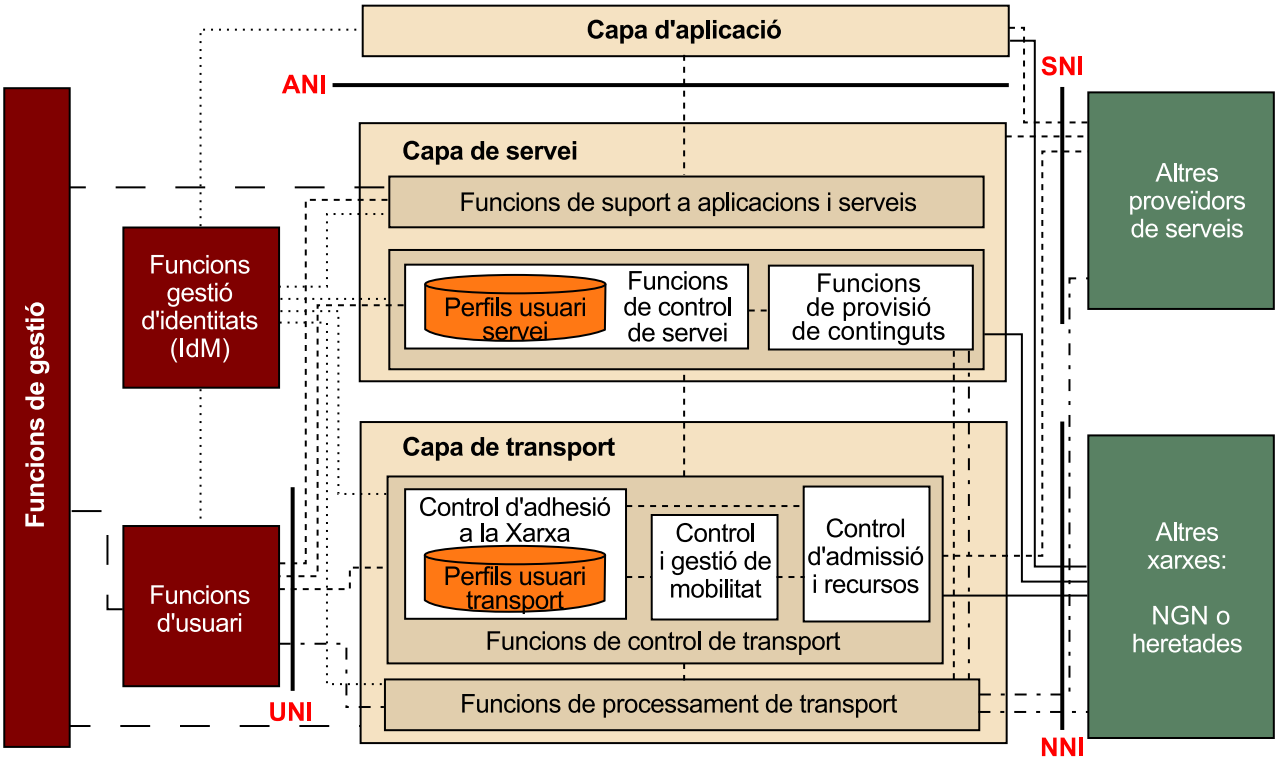
10. Conèixer el flux de trucada IMS, i identificar els missatges SIP que s'intercanvien per als serveis més representatius.

1. Arquitectura funcional d'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).

Aquestes característiques defineixen una arquitectura de referència horitzontal separada en capes de transport i servei. En la figura següent la ITU-T ens mostra la seva visió d'aquesta arquitectura.

Figura 1. Arquitectura de referència segons el Release 2 de xarxes NGN de la ITU-T



La figura 1 correspon al Release 2 de l'arquitectura, en la qual s'han introduït alguns blocs nous pel que fa al Release 1 enfocats bàsicament a serveis com IPTV, gestió d'identitats i mobilitat en la capa de transport.

A continuació veurem cadascuna de les parts i capes que conformen l'arquitectura ITU-T de referència començant per la capa de transport i les seves funcions, i pujant fins a la capa de servei. A més, per a cadascuna de les parts també veurem el model que defineixen dues organitzacions més de les més actives en la tasca de generació de documentació d'especificació sobre les xarxes NGN: l'ETSI-TISPAN i el 3GPP.

Encara que el model de referència de la ITU-T és el que es considera com a global i harmonitzador d'altres estàndards, val molt la pena veure aquestes altres dues especificacions, ja que és molt normal llegir publicacions amb aquests dos models. Veurem també les diferències i similituds entre aquests.

1.1. Elements que defineixen l'arquitectura

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 independentment del model que descriguem.

1.1.1. Entitat funcional

L'entitat funcional es defineix com el concepte lògic que especifica una sèrie de funcions úniques que no són fetes per altres entitats funcionals. Les entitats funcionals es poden agrupar per a descriure implementacions físiques i pràctiques d'aquestes.

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, que es podria donar el cas que una instància d'una entitat funcional tingui un comportament lleugerament diferent depenent d'aquest context.

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

1.1.2. Punt de referència

El punt de referència o interfície és un punt d'unió entre dues entitats funcionals ben diferenciades. Els punts de referències poden ser usats per a identificar el tipus d'informació que s'intercanvia entre aquestes entitats funcionals. A escala d'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 pot ser el cas de DIAMETER o H.248.

1.2. Capa de Transport

A continuació farem un escombratge per tres especificacions de les entitats estanderditzadores més actives en especificació de xarxes NGN. Començarem per la ITU-T i després mirarem les de l'ETSI-TISPAN i 3GPP a manera de comparació amb la primera.

1.2.1. Arquitectura de referència de la ITU-T

La definició de l'arquitectura de referència de la capa de Transport de la ITU-T està dividida en dues subcapes: la de processament i la de control. Al seu torn, cada subcapa està desglossada i atomitzada en funcions i subfuncions. Això és molt normal, ja que la ITU-T exerceix d'entitat d'estandardització global, la qual s'encarrega d'harmonitzar les aportacions d'altres estàndards com l'ETSI o el 3GPP, que estan focalitzades a un tipus concret de tecnologia de xarxa d'accés.

Així doncs, veurem definicions de funcionalitats genèriques que intenten fugir de qualsevol especificació que es decanti per un tipus de tecnologia de xarxa d'accés en concret i alhora intenten no descartar cap tipus de tecnologia que hi pugui haver en aquest àmbit.

Subcapa de processament de transport

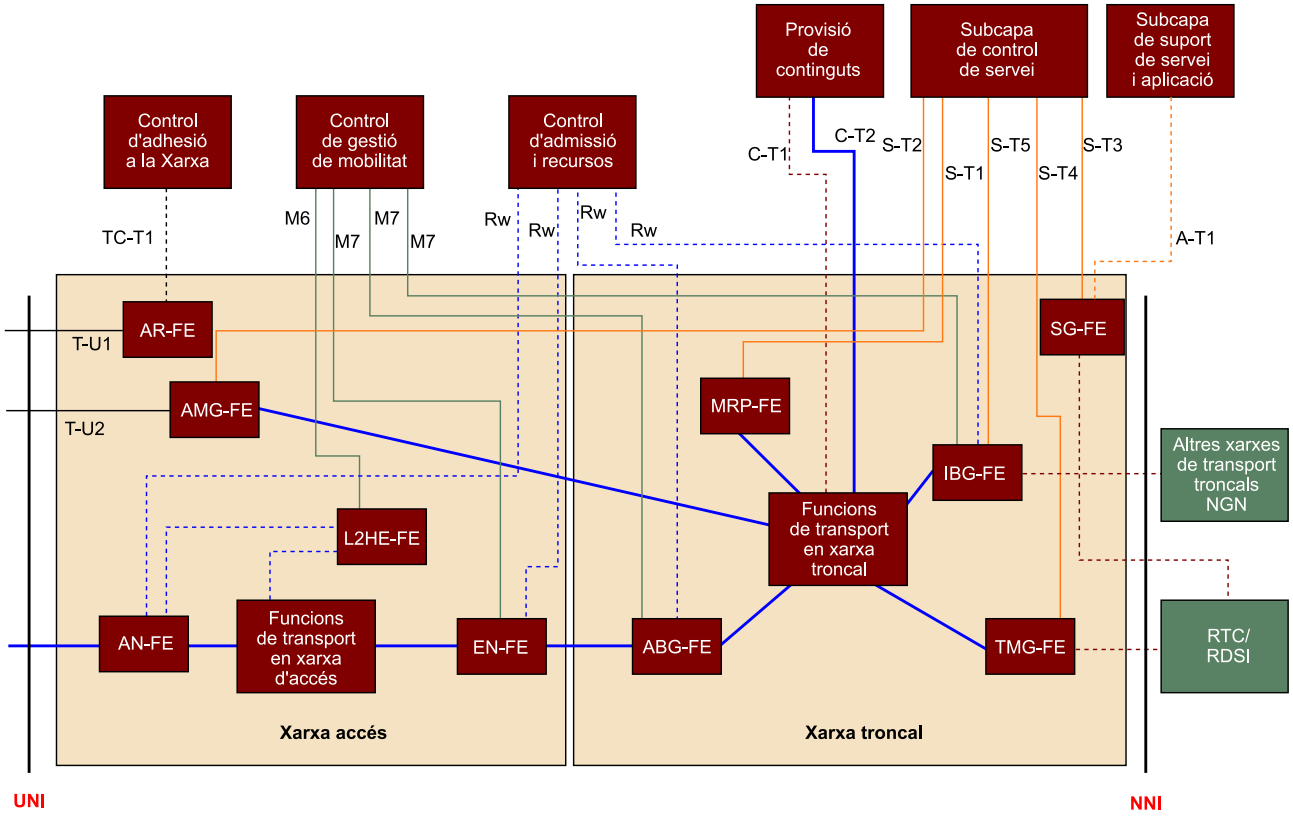
L'arquitectura que la ITU-T proposa d'entitats funcionals per a la subcapa de processament de trànsit en la capa de transport es pot apreciar en la figura 2. Les entitats funcionals d'aquesta subcapa estan classificades en dues seccions:

- xarxa d'accés i
- xarxa troncal.

Xarxa d'accés i xarxa troncal

Dins de les xarxes de transport, la xarxa d'accés es considera l'última milla abans d'arribar al terminal d'usuari i la xarxa troncal és la xarxa d'alta capacitat que interconnecta diverses xarxes d'accés entre si.

Figura 2. Entitats funcionals i punts de referència per a la capa de Processament de Transport



A continuació veurem quines funcionalitats té cada entitat i els punts de referència que les uneixen. Començarem definint algunes entitats funcionals elementals que poden estar presents en una o més entitats que apareixen en la figura 2, i seguidament abordarem les entitats pròpies de la xarxa d'accés i de la xarxa troncal.

1) Entitats elementals de processament de transport

Les entitats elementals no prenen decisions per si soles sinó que són controlades per altres entitats de control (localitzades en la subcapa de Control de Transport o de Control de Servei) amb l'objectiu de garantir la QoS dels serveis.

a) Entitat Funcional d'Aplicació de Polítiques (PE-FE): aquesta entitat s'anomena en anglès *Policy Enforcement Functional Entity* i posseeix els mecanismes necessaris per a aplicar polítiques concretes de processament de paquets IP. Entre aquests mecanismes hi ha filtratge, classificació i marcatge de paquets, conformació de trànsit a escala de flux o d'usuari i també gestió de cues, i priorització.

Aquestes polítiques per executar són decidides i especificades per una altra entitat anomenada *PD-FE* (Policy Decision Functional Entity) localitzada en la subcapa de Control de Transport, com veureu més endavant.

Veureu posteriorment que el lloc típic on s'integra aquesta entitat funcional és on hi ha potencialitat de produir-se un coll d'ampolla en termes de capacitat o també on es requereix fer un control dels recursos de transport.

Un exemple d'aquests llocs són les passarel·les a escala de paquet IP, que estan en els límits de la xarxa d'accés o en les Funcions d'Usuari.

Recurs de transport

El concepte de *recurs de transport* no solament inclou el concepte d'amplada de banda o capacitat en bits per segon sinó també l'àmbit de la traducció d'adreces IP o ports. En IPv4 la quantitat d'adreces IP públiques és un recurs finit i, per tant, s'ha de controlar.

b) Entitat Funcional d'Aplicació de Recursos de Transport (TRE-FE): aquesta entitat, que en anglès es tradueix com a Transport Resource Enforcement Functional Entity, depèn de la tecnologia associada al segment de la xarxa d'accés que controla i aplica polítiques de recursos de transport especificades per l'entitat de control respectiva (TRC-FE, en la subcapa de Control de Transport).

En una xarxa TDMA, la TRE-FE seria el bloc que assigna dinàmicament les ranures a cada terminal d'usuari per a complir una capacitat de transmissió determinada pel gestor de recursos (TRF-FE).

c) Entitat Funcional de Transferència Elemental (EF-FE): en anglès es tradueix com a *Elementary Forwarding Functional Entity* i es pot definir com un element físic que transfereix un paquet de dades des d'una interfície d'entrada a una altra interfície de sortida. La ITU-T anomena aquesta interfície *Flow Point* (FP).

Unicast* i *multicast

Si el paquet es transmet en unidestinació (*unicast*), aquest entra per un sol FP i surt per un altre de sortida (diferent del d'entrada). Si la transferència és multidestinació (*multicast*), el paquet entra per un sol FP d'entrada i surt per cap o diversos FP de sortida (mai pel mateix FP d'entrada).

L'entitat EF-FE és controlada per la seva entitat corresponent de control (EC-FE), que és la que li indica per quin FP ha de treure els paquets en funció de paràmetres del paquet rebut.

Un exemple clar d'aquesta funcionalitat és la que conté un encaminador (capa 3) quan aplica rutes IP configurades, o un commutador (capa 2) quan consulta la taula MAC.

d) Entitat Funcional de Control Elemental (EC-FE): en anglès es diu Elementary Control Functional Entity i s'encarrega de processar dades de control de protocols tant per a unidestinació com per a multidestinació amb vista a configurar el comportament de l'EF-FE. També pot rebre peticions des de la TRE-FE i la PE-FE per a l'aplicació de polítiques i respondre'ls sobre el resultat d'aquesta operació.

Exemples d'aquesta entitat funcional són la capacitat de processament de paquets d'encaminament dinàmic (RIP, OSPF, etc.) d'un encaminador (capa 3) o de Spanning Tree en el cas d'un commutador (capa 2). Un altre exemple seria que l'EC-FE fos una aplicació externa que configurés de manera estàtica les rutes IP en funció de criteris arbitraris d'operador.

2) Entitats funcionals de processament de transport a la xarxa d'accés

Recordem que la xarxa d'accés la formen entitats funcionals que interactuen directament amb el terminal d'usuari. S'assumeix que la xarxa d'accés NGN és una xarxa que és capaç de transmetre paquets IP. La ITU-T intenta copar amb qualsevol terminal amb tecnologia de xarxa existent incloent-hi les de xarxes heretades que no estan dissenyades per a la transmissió de paquets IP. Com veurem a continuació, hi haurà entitats funcionals que hauran de suportar interconnexió amb aquest tipus de tecnologies.

Vegem, doncs, les cinc entitats funcionals de processament de transport a la xarxa d'accés. Són les següents:

a) Passarel·la de Mitjans de xarxa d'Accés (AMG-FE): en anglès respon a les sigles d'*Access Media Gateway Functional Entity* i bàsicament s'encarrega d'interconnectar la xarxa d'accés per a transport de paquets IP amb terminals d'usuari basats en línies telefòniques analògiques o d'XDSI. Aquesta entitat està controlada per una altra entitat funcional situada en la subcapa de Control de Servei, anomenada *Passarel·la de Control de Senyalització* (AGC-FE, amb les seves sigles en anglès). Aquest control s'estableix per mitjà d'un punt de referència anomenat *T-U2*.

XTC /XDSI (commutació de circuits) i IP són tecnologies radicalment diferents i d'aquí s'extreuen les subfuncions següents:

Nota

La recomanació ITU-T Y.1453 especifica la interconnexió entre interfícies XDSI i IP.

- Processament bidireccional de mitjans en el pla d'usuari (fluxos de trànsit de veu, bàsicament) entre la tecnologia XTC/XDSI i la xarxa NGN. Opcionalment s'inclouen funcions com la transcodificació i la cancel·lació d'eco (el cas d'un terminal d'usuari amb línia analògica). També pot fer funcions d'interactivitat entre el sistema TDM i IP per a suportar serveis d'emulació XDSI en casos en què es necessiti un enllaç XDSI sense restriccions.

- Reenviament de la senyalització de control de trucada d'un usuari de la tecnologia XTC/XDSI cap a l'AGC-FE. Implica una traducció dels missatges de senyalització al seu equivalent en IP (normalment a SIP).

  Un exemple clar d'implementació en la vida real d'aquesta entitat funcional és una passarel·la de VoIP, que té una o diverses interfícies XDSI, i d'altra banda una interfície IP, per la qual processa la senyalització SIP o H.323 i els fluxos RTP on va la càrrega útil.

b) Node d'Accés (AN-FE): en anglès *Access Node Functional Entity*, és el punt de terminació o inici de l'últim tram de la xarxa d'accés abans d'arribar just a les entitats funcionals de les funcions d'usuari (vegeu la figura 1). Depenent de l'arquitectura i la tecnologia de la xarxa d'accés aquest bloc pot ser que no estigui present. Però, si ho està, per norma general es tracta d'un element de capa 2 (enllaç) i que opcionalment pot suportar capa 3 (IP). Així, l'AN-FE és un element amb potencialitat de coll d'ampolla i, per tant, ha de suportar les funcions de control dinàmic de qualitat de servei executades per les entitats EC-FE, EF-FE, PE-FE i TRE-FE, i definides per les entitats funcionals de la subcapa de Control de Transport per a tal funció com del bloc de Control d'Admissió i Recursos (RACF). La comunicació entre tots dos grups de blocs es fa via una interfície anomenada *Rw*.

Nota

Aquestes funcions de control de QoS són realment necessàries quan aquesta entitat funcional suporta la capa IP.

c) Node Fronterer (EN-FE): anomenat en anglès *Edge Node Funcional Entity*, fa les funcions de node frontera entre l'àmbit de la xarxa d'accés i la xarxa troncal de transport. Com que la xarxa troncal de transport suporta obligatòriament la capa 3 (IP), aquesta entitat funcional es pot considerar com el node en què acaba la sessió de capa 2 (enllaç entre el terminal d'usuari i la xarxa d'accés) i on comença la xarxa purament IP (sempre que el node d'accés no suporti capa IP). Això comporta la possibilitat de ser coll d'ampolla, amb la qual cosa, a part de les funcionalitats de transferència de paquets descrites ja com l'EF-FE i l'EC-FE, pot allotjar també les funcions de priorització i control de recursos descrites en les entitats elementals d'aplicació de recursos de transport i de polítiques (TRE-FE i PE-FE). Aquestes funcions també serien controlades pel RACF via la interfície Rw.

Nota

En xarxes d'accés mòbils, l'EN-FE pot incloure funcionalitats d'execució de transferència (*handover*) en capa 3. La transferència en capa 3 es dispara quan el terminal d'usuari surt de l'àmbit de la subxarxa d'accés en la qual es troba i es desplaça a una altra subxarxa que requereix el canvi d'assignació d'adreça IP. Amb la definició d'un node fronterer amb capacitat opcional d'execució de transferència en capa 3, la ITU-T deixa la porta oberta a les xarxes d'accés mòbils. Les funcions de mobilitat descrites per la ITU-T es descriuen amb més detall en el document ITU-T I.2018.

d) Entitat Funcional de Retransmissió d'Accés (AR-FE): en anglès es tradueix com a *Access Relay Functional Entity*. Aquesta entitat no processa paquets de trànsit de l'usuari sinó que s'involucra en processos d'ingrés a la xarxa dels terminals d'usuari rebent sol·licituds d'aquests (per mitjà d'una interfície ano-

menada *T-U1*) i transferint-los directament al bloc AM-FE (Access Management Funcional Entity) dins del Control d'Adhesió a la Xarxa (NACF), via un punt de referència anomenat *TC-T1*. En aquesta transferència, l'AR-FE pot afegir informació de configuració local que pugui creure convenient per al NACF.

Ingrés a la xarxa d'accés

Ingrés a la xarxa d'accés s'entén com a autenticació mútua entre el terminal d'usuari i la xarxa i l'assignació posterior d'adreça IP dins de l'àmbit de la xarxa d'accés. És el primer pas que tot terminal d'usuari ha de fer abans de poder accedir a cap servei contractat per mitjà d'una xarxa d'accés.

Per exemple, imaginem que en un cas real la sessió de capa 2 entre el terminal d'usuari i la xarxa d'accés està basada en el protocol PPP. Amb l'establiment de connexió que defineix aquest protocol es pot autenticar el terminal d'usuari i assignar dinàmicament una adreça IP. Llavors l'AR-FE actuaria com un reenviador de PPPoE (encapsulació de trames PPP en una trama Ethernet) cap al NACF.

En canvi, si s'usa DHCP, l'AR-FE actuaria a manera de reenviament dels paquets DHCP al NACF. A més podria afegir informació a aquest missatge DHCP abans de reenviar-lo informant sobre l'identificador de canal virtual associat (en el cas que fos una xarxa ATM).

e) Entitat Funcional d'Execució de transferència en Capa 2 (L2HE-FE): la Layer 2 Handover Execution Functional Entity està clarament orientada a xarxes amb mobilitat (sense fils) en les quals el terminal d'usuari es desplaça d'una cel·la de cobertura a una altra. Bàsicament aplica mecanismes associats a la mobilitat en la capa d'enllaç (no en capa IP) per preservar la continuïtat del flux de dades en el procés de transferència. Aquests mecanismes estan controlats pel bloc de control de mobilitat anomenat *MMCF* (Mobility Management Control Function) en la subcapa de Control de Transport. Dins d'aquest bloc és l'entitat HDC-FE (Handover Decision Control Functional Entity), via una interfície anomenada *M6*, la que pren les decisions del procés de transferència d'un equip d'usuari a la xarxa d'accés. L'L2HE-FE intercanvia amb aquesta entitat esdeveniments i accions per garantir la continuïtat del flux de dades. Com cal suposar, aquest procés està molt lligat a la tecnologia i la tipologia de la xarxa d'accés.

Nota

La ITU-T no ha definit una entitat funcional separada a l'equivalent en capa 3. Directament està integrada en altres entitats, com ja hem vist. Per a una informació més detallada sobre els mecanismes que la ITU-T defineix per a transferència de capa 2 i capa 3, consulteu la recomanació Y2018.

3) Entitats funcionals de processament de transport en la xarxa troncal

A continuació passem la frontera de la xarxa d'accés (considerada com l'última milla abans del terminal d'usuari) i ens passem a una xarxa aglutinadora de trànsit que ve des de les xarxes d'accés, o va cap a aquestes. Aquí les xarxes troncals ja es consideren purament NGN i, per tant, totes les entitats suporten la transferència de paquets IP. En aquest àmbit, es presenten les cinc entitats funcionals que conformen el processament de transport en la xarxa troncal:

a) Passarel·la Fronterera de la xarxa d'Accés (ABG-FE): l'Access Border Gateway Funcional Entity és l'element "mirall" del node fronterer EN-FE en la xarxa d'accés, ja que simplement fa transferències de paquets IP entre els segments de xarxa d'accés i troncal (això és el mateix que dir que inclouen les funcionalitats elementals de transferència de paquets com EF-FE i EC-FE). Com la xarxa troncal i la d'accés poden pertànyer a dominis administratius dife-

rents (operadors diferents) aquesta entitat pot fer altres funcions frontereres (protecció mútua mitjançant ocultació o emmascarament de la tipologia de xarxa).

És important esmentar que, en ser un element fronterer de transferència de paquets IP entre dos àmbits diferents de la xarxa de transport, opcionalment l'ABG-FE pot suportar la traducció d'adreces IPv4 a IPv6.

Emmascarament

Quan diem *emmascarament* volem dir que, per exemple, s'inclouen funcionalitats com obertura o tancament de portes d'accés a escala de flux IP o filtratge de paquets a manera de tallafoc. També seria capaç de fer traducció d'adreçament tant a escala de direcció IP com a escala de port (NAPT) aplicada a fluxos multimèdia (anomenat *media latching*). La configuració d'aquestes traduccions pot ser controlada remotament per entitats en la subcapa de Control de Transport (el RACF via la interfície Rw) i perquè tal control es dugui a terme l'ABG-FE ha d'implementar part de les funcions elementals d'aplicació polítiques descrites anteriorment en la PE-FE, en concret, la conformació de trànsit i el remarcatge de paquets.

Pot semblar absurd tenir dues entitats adjacents que fan pràcticament la mateixa funció, però és molt important amb vista a delimitar dos dominis administratius diferents, que són operats per dues organitzacions completament diferents. És, doncs, desitjable i lògic que tots dos operadors es protegeixin d'alguna manera fent que l'única entitat visible de cada xarxa operada per entitats externes sigui un únic element. Així poden controlar molt millor el trànsit que entra des d'altres xarxes externes.

Igual que en l'element EN-FE, aquesta entitat podria tenir opcionalment integrada la funcionalitat d'execució de transferència en capa 3 (L3HEF). Per aquest motiu s'ha dibuixat la interfície M7 en la figura 2.

b) Passarel·la d'Interconnexió Fronterera (IBG-FE): en anglès es defineix com a *Interconnection Border Gateway Functional Entity* i és l'element que marca la frontera entre la xarxa troncal NGN (xarxa de paquets d'alta capacitat) amb una altra xarxa troncal NGN de les mateixes característiques però d'un altre operador. Seria l'equivalent en funcions a la passarel·la ABG-FE (control dinàmic de QoS, traducció d'adreçament i tallafoc) però en l'altre extrem de la xarxa troncal.

Com a opció, aquesta entitat fronterera preveu també altres funcions més complexes que dependran del servei, com per exemple la transcodificació de mitjans per al servei de VoIP, la traducció d'adreces IPv4 a IPv6 o el xifratge de mitjans, entre altres funcions.

Igual que amb l'ABG-FE, es preveu la possibilitat d'integrar funcionalitats de mobilitat en capa 3 en aquesta entitat (L3HEF). Per aquest motiu s'ha inclòs la interfície M7.

IBG-FE

En ser la IBG -FE una entitat fronterera entre dos dominis administratius independents sorgeix de nou la necessitat de protegir-se, que ja hem comentat en el cas de la passarel·la fronterera de la xarxa d'accés. Controlat per un RACF via la interfície Rw, la passarel·la IBG-FE implementaria les funcions bàsiques d'aplicació de polítiques de l'entitat elemental PE-FE (amb excepció de les funcions per a travessar la traducció d'adreça IP privada a pública i ports, ja que no existeixen en l'IBG-FE) i les d'aplicació de recursos de transport de la TRE-FE. Es recomana a més suportar les funcions elementals de transmissió de paquets EC-FE i EF-FE.

Nota

La ITU-T ja preveu que un RACF estigui dedicat exclusivament a controlar l'IBG-FE dins d'una xarxa troncal. No obstant això, també preveu que una altra entitat funcional diferent controli l'IBG-FE: l'IBC-FE o Interconnection Border Control Functional Entity, però l'especificació de la seva integració està sota estudi de la ITU-T.

Ens hem d'imaginar que hi haurà tantes instàncies de l'IBG-FE com el nombre d'interconnexions que hi hagi amb altres xarxes troncals operades per tercers.

c) Passarel·la de Mitjans cap a Xarxes de Circuits (TMG-FE): en anglès es tradueix com a *Trunking Media Gateway Functional Entity*. Així com la passarel·la fronterera de la xarxa d'accés (AMG-FE) que hem vist abans exercia la funció de passarel·la entre la tecnologia XTC/XDSI i la xarxa IP amb vista a terminals d'usuari telefònics, aquesta entitat fa la mateixa funció però en la xarxa troncal (incloent-hi funcions de transcodificació, cancel·lació d'eco i punt de conferència). És a dir, que proporciona a les xarxes NGN (basades en paquets IP) la interconnexió amb les xarxes tradicionals de telefonia XTC o XDSI. Aquesta entitat, com l'AMG-FE, té la seva entitat homòloga a escala de control, i es tracta de l'MGC-FE (Media Gateway Control Functional Entity), localitzada en la subcapa de Control de Servei. Per aquest motiu s'ha inclòs la interfície anomenada *S-T4*.

Nota

Aquesta entitat proporciona la interconnexió de les xarxes NGN amb tercers operadors de xarxes tradicionals. La ITU-T preveu, com és lògic, interconnectar els serveis de veu d'NGN amb aquestes xarxes per a garantir la màxima interoperabilitat i interconnectivitat de totes les tecnologies.

d) Entitat Funcional de Processament de Recursos de Mitjans (MRP-FE): també anomenada en anglès Media Resource Processing Functional Entity, aquesta entitat funcional proporciona processament de la càrrega útil de paquets usats en la xarxa troncal NGN. Aquesta entitat apareix com una font de recursos addicionals que enriqueixen el servei de trucada de veu. Per *enriquiment* ens referim a totes aquelles funcions que fan que el servei de veu vagi més enllà d'una mera trucada entre dos terminals. Per exemple, generació de tons (d'espera, comunicant, etc.), generació i recepció de tons DTMF, generació de locucions o avisos de veu automàtica, transcodificació (descodificar i codificar de nou amb un altre codificador de veu), reconeixement de veu i barreja de vídeo o altres mitjans entre si. Totes aquestes funcionalitats són decidides i

Reflexió

Penseu que tota la senyalització acústica en el món de la telefonia que nosaltres com a usuaris reconeixem de seguida (com, per exemple, el to de comunicant o els missatges de l'operadora que indiquen que el número no està accessible), han de ser traslladats al món IP i això comporta que alguna entitat s'encarregui de generar els fluxos RTP d'àudio que un terminal de VoIP suporti i converteixi a senyal acústic. La ITU-T ha volgut separar tots aquests serveis en un element independent com l'MRP-FE.

controlades per una altra entitat de la capa de Control de Servei anomenada Media Resource Control Functional Entity per via d'una interfície anomenada S-T1.

e) Passarel·la de Senyalització (SG-FE): en anglès l'entitat es diu *Signalling Gateway Functional Entity* i s'encarrega simplement de traduir els missatges de senyalització entre la xarxa NGN i les xarxes heretades, com l'XTC, XDSI i les xarxes basades en SS7. Aquesta senyalització en el costat NGN es reenvia a la mateixa entitat de control associada a la passarel·la de mitjans TMG-FE (l'entitat de control de passarel·les de mitjans o MGC-FE, que està localitzada en la capa de Control de Servei). L'MGC-FE s'encarrega d'encaminar aquesta senyalització cap a les funcions d'encaminament de senyalització NGN adequades dins de la capa de Control de Servei (la senyalització en NGN en aquest cas seria SIP).

Reflexió

Tal com està formada una passarel·la de VoIP, no seria desgavellat pensar que l'SG-FE estigués integrada amb la TMG-FE en un mateix equip físic. De fet, es podria dir que la suma d'SG-FE i TMG-FE seria l'equivalent a l'AMG-FE però a la xarxa troncal. La possible raó per la qual la ITU-T ha separat la senyalització i el processament dels mitjans en dues entitats independents és la complexitat i variació més grans en la senyalització de la xarxa troncal de telefonia en comparació de l'AMG-FE.

Subcapa de Control de Transport

En la subcapa de control de transport hi ha la intel·ligència de gestió de recursos tant de la xarxa d'accés com de la xarxa troncal. A més, aquesta subcapa és de summa importància ja que, gràcies als punts de referència oberts que els connecten amb la capa de Servei, proporcionen en certa manera la independència entre la tecnologia de la xarxa de transport i els serveis i garanteixen, si és necessari, la QoS d'extrem a extrem. Aquesta subcapa està formada per tres blocs principals: el de Control d'Adhesió a la Xarxa (NACF en les seves sigles en anglès), el de Control d'Admissió i Recursos (RACF) i finalment el de Control de Gestió de Mobilitat (MMCF). Per a cadascun d'aquests blocs en descriurem l'arquitectura i funcions.

1) Control d'Adhesió a la Xarxa (NACF)

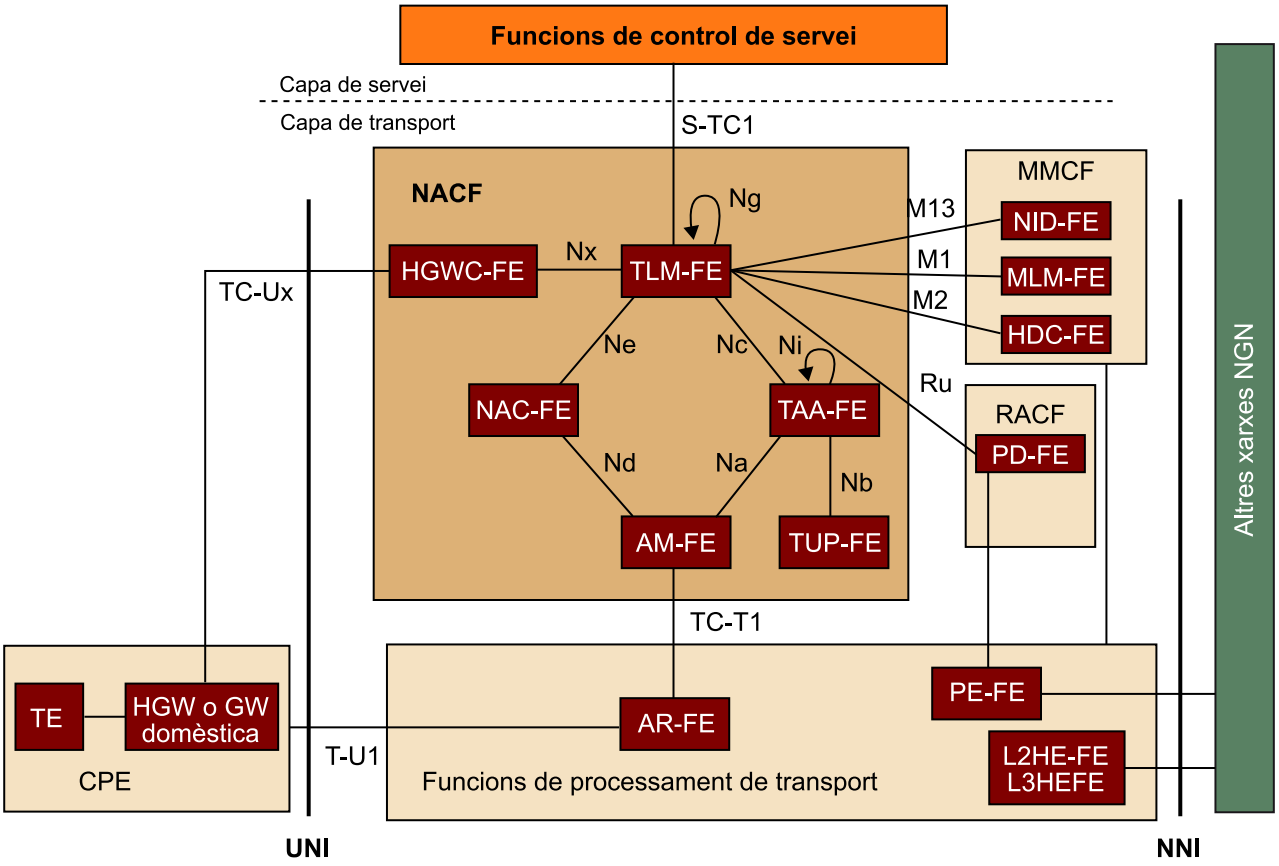
A continuació veurem les recomanacions de la ITU-T per a fer un ingrés correcte d'un terminal o equip d'usuari a la xarxa d'accés. Aquest procés és sempre el preludi a poder accedir als serveis que ofereix una xarxa NGN.

A continuació veurem una descripció de cada entitat funcional i com està relacionada amb els seus adjacents.

Vegeu també

En la taula 4 de l'annex podem veure els punts de referència que afecten el NACF.

Figura 3. Arquitectura de referència del NACF per a la ITU-T



a) Entitat Funcional de Configuració d'Accés a la Xarxa (NAC-FE): la Network Access Configuration Functional Entity, en anglès, es responsabilitza de l'assignació de l'adreça IP a l'equip d'usuari (l'equip d'usuari en anglès també s'anomena *Customer Premises Equipment* o CPE) una vegada aquest s'ha autenticat contra l'entitat encarregada de l'autenticació i autorització a escala de transport (TAA-FE).

El NAC-FE pot assignar dues IP a un equip per a suportar mobilitat IP: una IP persistent, que mai no varia, i una IP temporal que va canviant cada vegada que l'usuari canvia de subxarxa.

A part d'assignar l'adreça IP, la NAC-FE pot aprofitar aquesta transacció per a distribuir altres paràmetres de configuració de xarxa com les adreces de servidors DNS o les de servidors intermediaris (*proxies*) de senyalització per a alguns components de la capa de servei (com per exemple el P-CSC-FE del punt de presència del nucli IMS per a l'usuari en la capa de Control de Servei).

Situant-nos en un escenari d'itinerància de l'equip d'usuari (és a dir, que ingressa en una xarxa d'accés d'un altre operador), aquesta entitat funcional pot estar localitzada en una xarxa visitada o en una xarxa local, depenent del domini administratiu i de l'escenari de negoci.

Nota

No hi ha una única manera d'implementar aquesta entitat funcional. Recordeu que les entitats funcionals descriuen meres funcionalitats però no maneres de dur-les a terme. Per a implementar la NAC-FE potser la primera idea que us ve és utilitzar un servidor DHCP, però també es podria implementar amb un servidor PPP que faci la mateixa funció. En definitiva, com qualsevol altra entitat funcional descrita en aquest document, hi ha total llibertat en la implementació de la NAC-FE sempre que compleixi cadascuna de les funcionalitats descrites.

b) Entitat Funcional d'Autenticació i Autorització a Escala de Transport (TAA-FE): la Transport Authentication and Authorization Functional Entity fa l'autenticació de l'usuari i també el control d'autorització basada en perfils de subscriptor a escala de transport, amb vista a l'accés a la xarxa. Aquesta funcionalitat és sempre prèvia a l'assignació de l'adreça IP de la NAC-FE.

Nota

També es pot preveure la possibilitat que aquesta informació addicional de configuració de xarxa (*DNS*, servidors intermediaris) estigui estàticament configurada en l'equip d'usuari, incloent-hi l'assignació estàtica de l'adreça IP (si el perfil d'usuari a escala de transport així ho indica).

Per a poder autenticar i autoritzar l'usuari, la TAA-FE necessita informació sobre les credencials i del perfil de subscripció d'aquest. Aquesta informació la proporciona una altra entitat funcional dins del NACF anomenada *TUP-FE*, i que més tard es detallarà.

En un escenari d'itinerància d'ingrés a la xarxa, la TAA-FE pot fer el paper de servidor intermediari per a connectar-se a una altra entitat TAA-FE remota on es troba la informació d'autenticació emmagatzemada de l'usuari en qüestió (en la TUP-FE corresponent). Per a això es requereix el punt de referència Ni.

En el procés d'adhesió a les xarxes NGN, es preveuen dos mètodes d'autenticació:

- L'autenticació **implícita**, en el qual simplement amb la consulta d'un paràmetre que identifiqui unívocament l'equip d'usuari (per exemple, una adreça MAC en una llista d'admesos) pugui ser suficient.

- L'autenticació **explícita**, en el qual llança un repte a l'equip d'usuari i es desencadena el procediment d'autenticació per mecanismes i protocols de comprovació de credencials.

c) Entitat Funcional de Perfil d'Usuari a Escala de Transport (TUP-FE): la Transport User Profile Functional Entity és l'entitat funcional a manera de base de dades que emmagatzema en un mateix perfil el següent:

- **Dades d'autenticació**, entre les quals s'inclouen: 1) l'identificador de subscriptor a escala de capa de transport, 2) la llista de mètodes d'autenticació suportats o 3) les claus per a usar.

- **El perfil de subscripció de transport**. Aquest conté la informació relacionada amb la configuració requerida per a l'accés a la xarxa, i també la informació de perfil de QoS contractat per l'usuari en l'àmbit de la xarxa d'accés.

Igual que en el cas de l'entitat que assigna l'adreçament IP (NAC-FE) per a l'escenari d'itinerància, la informació pot ser transferida a un TUP-FE d'una xarxa visitada, però sempre per mitjà de l'entitat TAA-FE. És a dir, que la capacitat de transferència de perfils la té realment la TAA-FE, el qual té un punt de referència específic (anomenat *Nb*) per a aquesta funció.

Informació TUP-FE

És possible que us feu la pregunta sobre quin format o informació exacta contenen aquests perfils. La ITU-T ja especifica en la seva recomanació Y.2014, en què descriu amb detall el bloc NACF d'adhesió a la xarxa de transport i tots els seus blocs funcionals, una taula en el qual indica quins paràmetres defineixen aquest perfil. A manera de resum, cada perfil de transport té el seu identificador únic que conté informació d'accés a la xarxa. Però associat a aquest, hi ha diversos subperfils, cadascun amb el seu propi identificador, tots amb informació d'autenticació i perfil de recursos de transport propis. Aquest identificador de subperfil és l'identificador que es correspon amb un altre identificador de connexió lògica a la xarxa d'accés (equivalent, per exemple, a ID de canal virtual en ATM o a l'etiqueta assignada en una xarxa MPLS).

d) Entitat Funcional de Gestió de Localització a Escala de Transport (TLM-FE): la Transport Location Management Functional Entity registra l'associació entre l'adreça IP assignada a un equip d'usuari i la informació de localització en xarxa relacionada amb aquest, la qual és proporcionada per l'entitat NAC-FE via la interfície Ne.

Exemple

Aquesta informació de localització en xarxa inclou, per exemple, característiques de l'equip a la xarxa d'accés, un identificador de connexió lògica (és un identificador que defineix la connexió o canal virtual que porta a l'accés directe de l'equip d'usuari) o la identificació de l'equip limítrof en la central que tanca el bucle d'abonat (una cosa típica en xarxes ADSL).

El TLM-FE registra també l'associació entre la informació de localització a escala de transport rebuda des de l'entitat funcional NAC-FE i la informació de localització geogràfica (en forma de coordenades o fins i tot la seva adreça postal). A més, afegeix a aquesta associació el perfil de QoS de l'usuari rebut des de TAA-FE via la interfície anomenada Nc i després el passa al RACF (Control d'Admissió i Recursos) via la interfície anomenada Ru. Més tard es veurà per a què usa el RACF aquesta informació.

Informació geogràfica

La capa de Control de Servei sol·licita la informació geogràfica (coordenades de localització) per mitjà d'un punt de referència anomenat *S-TC1*. No obstant això, l'estàndard de la ITU-T no especifica com el TLM-FE obté aquesta informació geogràfica. Aquesta informació, com que en determinats casos és delicada per a l'usuari, es pot restringir o no mostrar-se deliberadament si aquest així ho acorda amb l'operador de xarxa d'accés.

e) Entitat Funcional de Gestió a Escala d'Accés (AM-FE): l'Access Management Functional Entity, com es diu en anglès, és l'entitat funcional que està directament connectada a l'entitat funcional de Retransmissió d'Accés (AR-FE) en la subcapa de processament de transport via la interfície TC-T1. La seva funció és acabar a escala de capa 2 (els missatges de la qual són rebuts des de l'AR-FE) la connexió entre l'equip d'usuari i el NACF amb vista al registre i la inicialització de l'equip d'usuari. Aquesta connexió de capa 2 pot ser utilitzada per a detectar intents d'adhesió a la xarxa d'un equip d'usuari. En aquest cas, la connexió de capa 2 entre l'equip d'usuari i l'AM-FE pot constituir un marc unificat per a les entitats de capes superiors per mitjà d'entorns amb xarxes heterogènies per a facilitar la selecció i el descobriment de múltiples tipus de xarxes d'accés existents dins d'una àrea geogràfica. Gràcies a aquesta connexió, l'AM-FE pot descobrir els identificadors d'enllaç (de la connexió lògica i física).

Connexió lògica i física

Com a connexió lògica el considerem com un identificador de canal virtual i com a connexió física algun paràmetre que identifiqui el terminal d'usuari en la xarxa d'accés (per exemple una adreça MAC, l'adreça IP de l'element PE-FE associat o un identificador de port físic).

Cal aclarir que cada relació a escala de comunicació entre l'equip d'usuari i l'AM-FE no implica cap mecanisme de transport en particular.

Exemple

Per a entendre exactament quin paper pot tenir l'AM-FE posem-ne un exemple. Imagineu-vos que el protocol de capa 2 a la xarxa d'accés és el PPP. Així doncs, l'AM-FE faria la funció de servidor PPP i traduiria les peticions d'aquest protocol a escala d'autenticació i sol·licitud d'adreça IP a un altre protocol (RADIUS en mode client) per mitjà del punt de referència que el connecta amb les entitats del NACF corresponents (TAA-FE per a autenticació i NAC-FE per a assignació d'adreça IP).

Un altre exemple seria la utilització del protocol 802.1X, en el qual l'AM-FE faria d'autenticador implementant un client RADIUS cap al TAA-FE i el NAC-FE.

f) Entitat Funcional de Configuració de Passarel·la Domèstica (HGWC-FE): la Home Gateway Configuration Functional Entity s'usa en la inicialització i actualització remota de la passarel·la domèstica (per exemple, instal·lació remota de nova versió del microprogramari). Proporciona a aquesta passarel·la informació de configuració addicional a escala de tallafoc local o marcatge de paquets per a QoS (aquesta informació pot estar emmagatzemada en forma de perfils de configuració en la passarel·la domèstica mateixa) que pot ser usada en processos posteriors de garantia de QoS (proporcionats per interaccions amb el RACF per mitjà d'altres entitats funcionals). Cal aclarir que aquestes dades de configuració de xarxa no tenen res a veure amb la configuració de xarxa proporcionada pel NAC-FE (informació de servidors intermediaris, servidors DNS, etc).

Nota

La definició de l'equip d'usuari de la ITU-T (o CPE, en anglès) no se cenyeix solament a un terminal únic (un sol dispositiu físic) com seria el cas d'un terminal de telefonia mòbil, sinó que l'estàndard també considera que el CPE pugui ser una xarxa sencera amb una passarel·la residencial encapçalant-la com, per exemple, l'encaminador ADSL en una llar que dóna servei a tota una xarxa al darrere.

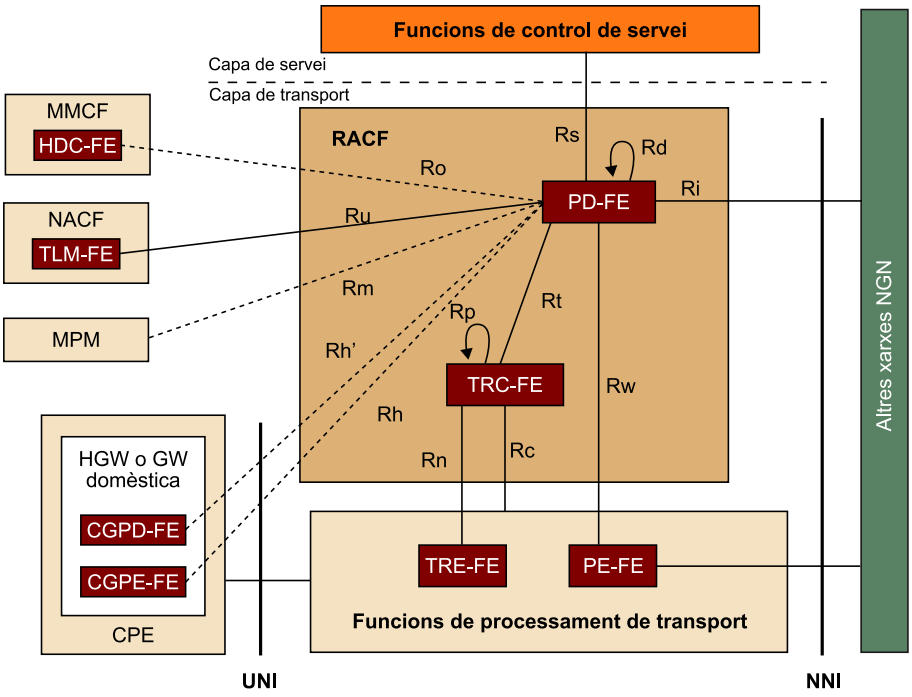
L'HGWC-FE també pot gestionar informació de monitoratge que la passarel·la domestica pugui generar sobre els terminals o dispositius que es connecten després d'aquesta (per exemple, sobre la disponibilitat dels equips terminals o TE en anglès).

Aquesta entitat pot estar interconnectada amb l'entitat TLM-FE per a obtenir informació sobre el tipus de connexió o els identificadors d'enllaç que li puguin ajudar a seleccionar la configuració més adequada.

2) Control d'Admissió i Recursos (RACF)

En la figura 4 podeu apreciar l'arquitectura de referència que la ITU-T presenta per al RACF. Com veureu a continuació, aquesta entitat és clau, ja que garanteix la gestió de recursos i la QoS dels serveis en la xarxa de transport (d'accés i troncal). Per això donarem una explicació una mica més detallada.

Figura 4. Arquitectura de referència del RACF per a la ITU-T



Abans d'abordar cadascun dels blocs funcionals i interfícies que componen el RACF, definirem les fases que es preveuen en el procés de control d'admissió i recursos, ja que és una cosa comuna a les xarxes NGN.

Vegeu també

Sobre els blocs funcionals i interfícies del RACF, vegeu el resum en la taula 5 en l'annex.

Hi ha tres passos principals en la garantia de QoS en el moment en què el RACF rep una sol·licitud sobre aquest tema:

- **Autoritzar** (*Authorization*). La sol·licitud de QoS aplicant polítiques de xarxa definides per l'operador.

- **Reservar** (*Reserve*). Els recursos a la xarxa de transport. En aquest cas es fa una comprovació de compliment de perfil d'usuari (solament en cas de xarxa d'accés) i posteriorment una comprovació de disponibilitat de recursos en el sistema abans de fer la reserva. Si els controls es passen satisfactòriament s'actualitza l'estat dels recursos com a reservats (però l'usuari encara no els pot usar).

- **Assignar** (*Commit*). Els recursos ja prèviament reservats a l'usuari perquè en faci ús (no requereix actualització d'estat dels recursos sinó una assignació d'aquests al terminal rere el qual hi ha l'usuari).

Aquests tres passos es poden fer en una sola fase (sota una sola sol·licitud), en una fase separada per a cada pas (amb tres sol·licituds separades) o en dues fases, i llavors l'autorització i la reserva de recursos es fa en una sola fase i l'assignació es fa *a posteriori*, sota sengles sol·licituds de recursos des de la capa de control de servei.

Reserva en dues fases

Per què s'habilita la possibilitat de fer la reserva en dues fases? Es fa així per a evitar que s'assignin recursos en ple establiment de la sessió de servei i per algun motiu es cancel·li aquest establiment sense arribar a usar el servei. Solament s'assignaran els recursos quan l'establiment de la sessió estigui totalment assegurat i confirmat pels usuaris. A més, penseu que quan es reserven els recursos, mentre no s'assignin, aquests estan disponibles per a trànsit *Best Effort* de la xarxa (que no requereix sol·licitud expressa de garantia de recursos).

a) Entitat Funcional de Decisió de Polítiques (PD-FE): la Policy Decision Functional Entity representa per a la capa de Control de Servei un únic punt de contacte amb la capa de Transport a l'hora d'autoritzar i aplicar reserves de recursos de transport i QoS. Gràcies a aquest únic punt de contacte, s'emmascara o amaga la tipologia de la xarxa de transport a un operador de la subcapa de Control de Servei.

Les sol·licituds d'autorització de QoS i reserva de recursos es reben per mitjà de la capa de Control de Servei (per mitjà d'una interfície anomenada *Rs*), des d'un altre PD-FE pertanyent a un altre operador NGN en un escenari de nomadisme o itinerància (per mitjà d'una interfície anomenada *Ri*), o bé des d'un altre PD-FE pertanyent al mateix domini (per mitjà d'una interfície anomenada interfície *Rd*).

Quan la petició de recursos de QoS es rep des de les funcions de la subcapa de Control de Servei es diu que la reserva es fa en mode *push*, perquè al final es tradueix en un control d'admissió i una instal·lació de polítiques de QoS sobre la subcapa de Processament de Transport.

En un mode diferent, la PD-FE també pot rebre aquesta sol·licitud de reserva de recursos des d'aquelles entitats funcionals de la subcapa de processament de transport que posseeixin l'entitat elemental d'aplicació de polítiques (PE-FE) via la interfície Rw.

Quan la petició de recursos de QoS es rep des de les funcions de la subcapa de Processament de Transport es diu que la reserva es fa en mode *pull*. Aquest mode pretén respectar i aprofitar els mecanismes inherents de sol·licitud de recursos (en capa 2) que hi podria haver en algunes xarxes d'accés. Al final es tradueix en un control d'admissió i una instal·lació de polítiques de QoS sobre la mateixa subcapa de Processament de Transport.

Nota

Es preveu la possibilitat que la capa de Control de Servei i el RACF (o també dos RACF) puguin ser entitats gestionades per operadors diferents, i de nou s'inclou aquesta funció de frontera administrativa i d'accés per mitjà d'un únic punt de contacte com a mètode de protecció.

El resultat de l'autorització en la sol·licitud de recursos, ja sigui positiva o negativa, és sempre comunicant a l'entitat que ha fet la sol·licitud. A més, la PD-FE ha de suportar la sol·licitud de modificació d'una petició ja autoritzada (cosa que comporta també el procés d'autorització corresponent) o també la sol·licitud de terminació de la sessió de reserva de recursos (cosa que significa que haurà d'alliberar els recursos assignats i també desinstal·lar qualsevol política de QoS associada).

Però què ha de fer exactament la PD-FE per a prendre la decisió final sobre si ha d'autoritzar o no una nova (o modificada) sol·licitud de recursos en la xarxa de transport (ja sigui d'accés o troncal)?

Per a la PD-FE prendre aquesta decisió comporta fer una llista de control d'admissions a diferents nivells:

- El PD-FE, per començar, ha d'**autoritzar la sol·licitud de recursos mateixa i QoS en si**, aplicant:
  - Regles de polítiques de xarxa arbitràries (per exemple, no admetre cap sol·licitud que contingui informació de vídeo de cap operador), les quals són a escala del servei que se sol·licita i són proporcionades directament pels operadors NGN.

  - SLA particulars entre l'operador de la xarxa d'accés (emmagatzemats en el RACF) i l'operador de la subcapa de Control de Servei. És com

un altre tipus de regles arbitràries però aplicades exclusivament a un operador de subcapa de Control de Servei en particular.

Un SLA (Service Level Agreement) es defineix com un acord de provisió de serveis entre dues entitats (per exemple, subscriptor i proveïdor de servei) en què es comprometen certs aspectes de la qualitat dels serveis.

- Posteriorment ha de **fer el control d'admissió** a escala de subscripció de transport (solament aplicable al cas de xarxa d'accés) per a l'usuari que sol·licita el servei (perfil de QoS proporcionat pel NACF, per mitjà del punt de referència Ru).

- Finalment ha de **consultar** (via el punt de referència anomenat *Rt*) **a l'entitat funcional que controla els recursos de transport (TRC-FE) sobre la disponibilitat dels recursos** per a aquesta sol·licitud. La resposta d'aquest haurà de ser tinguda en compte (el nombre de TRC-FE connectats a la PD-FE dependrà de la tipologia de la xarxa d'accés o troncal).

Nota

El PD-FE no fa el control dels recursos de la xarxa. Per a això hi ha la TRC-FE, al qual sol·licita que autoritzi la reserva de recursos (reserva de capacitat) segons la informació actualitzada de l'estat dels recursos de la xarxa que posseeix aquest.

Llavors si la sol·licitud passa l'autorització i tots aquests controls d'admissió, què ha de fer la PD-FE?

Si el resultat d'aquesta autorització de recursos és positiva, la PD-FE pot decidir instal·lar polítiques de QoS (amb **paràmetres QoS que no depenen de la tecnologia** de la xarxa de transport) sobre els elements corresponents per a l'aplicació de polítiques en la subcapa de Processament de Transport (les entitats funcionals que continguin la PE-FE, bàsicament). De fet, pot controlar diverses instàncies de PE-FE via la interfície Rw sempre que estiguin dins del mateix domini administratiu.

Nota

Aquests paràmetres de QoS utilitzats en les polítiques estan especificats per la ITU-T en la seva recomanació Y.1514.

El PD-FE a més pot interactuar amb entitats localitzades dins dels equips d'usuari mateixos i més concretament en el cas que l'usuari tingui una passarel·la residencial amb dispositius connectats al darrere. Estem parlant de l'entitat funcional d'aplicació de polítiques localitzada en la passarel·la residencial (CGPE-FE en la figura 4). S'ha de tenir en compte que més enllà de la passarel·la residencial hi ha l'enllaç amb la xarxa d'accés, de manera que és molt probable que en aquesta entitat funcional es produeixi un coll d'ampolla en sentit d'enllaç de pujada i, per tant, cal aplicar algun mecanisme d'aplicació de polítiques de QoS. Així doncs, la PD-FE utilitza el punt de referència Rh per a instal·lar regles de polítiques directament en la passarel·la residencial per a garantir la QoS segons el control d'admissió que es faci.

La interfície Rh'

La interfície Rh' s'usa per al cas d'un control més complex dels recursos en el costat de l'usuari en què una altra entitat anomenada CGPD-FE seria capaç de fer funcions de control d'admissió a escala de recursos però en l'àmbit de la xarxa local de l'usuari.

Quan la PD-FE ha d'interactuar amb un element PE-FE (via Rw) per a instal·lar una política de QoS, aquesta pot incloure informació sobre **control d'accés a manera de tallafoc** (*Gate Control*) si l'entitat PE-FE en qüestió ho requereix. Aquestes regles de pas són en forma de tuple de 5 paràmetres: IP origen i destinació, port origen i destinació i protocol, o si s'escau, identificador de transport en capa 2 com VLAN ID. Amb això es permet o denega el pas dels fluxos IP que caracteritzen la sessió del servei.

Reflexió

Una vegada vistes les entitats en la subcapa de Processament de Transport, quines entitats funcionals creieu que poden ser triades per l'entitat PD-FE per a fer el control d'accés?

També pot incloure informació perquè les entitats de la subcapa de processament de transport que apliquin puguin fer el **marcatge (o remarcatge) dels paquets IP** si així es requereix per tal de garantir certa QoS al llarg de la xarxa d'accés o troncal.

Nota

Hi ha mètodes de marcatge de paquets que obeeixen a un mecanisme estandarditzat de garantia de QoS, com DiffServ. Però dins d'un domini l'operador pot adoptar qualsevol patró de marcatge (estàndard o no) per tal que es garanteixi la mateixa QoS.

Si l'element d'aplicació de polítiques PE-FE amb el qual interactua és algun tipus d'element limítrof amb un altre domini administratiu, les polítiques de QoS poden incloure informació d'**encreuament de NAT (traducció d'IP privada a IP pública) o ports** per als fluxos IP. Aquesta funcionalitat obliga la PD-FE a interactuar amb la capa de Control de Servei i la PE-FE de la subcapa de Processament de Transport per a fer les assignacions d'adreçament IP o ports en el costat global i local de la PE-FE que fa aquesta traducció.

Reflexió

Tindria sentit una funcionalitat així en una xarxa de transport que únicament usés adreçament basat en IPv6?

En alguns casos la PD-FE pot decidir **limitar la velocitat en bits per segon**[1] dels fluxos IP del servei (per exemple, en un servei de vídeo sota demanda hi pot haver un flux IP per a vídeo i un altre per a àudio per separat que segons el codificador que usin no haurien de sobrepassar certa taxa). Aquesta informació també s'inclou en l'especificació de la política QoS per a aplicar en les entitats que apliquen aquestes polítiques de QoS en la subcapa de processament de transport.

(1)Aquesta funció és molt recomanada per a trànsits inelàstics, és a dir, basats en UDP, i més concretament està recomanada per a trànsits multimèdia de transmissió de continguts basats en el protocol RTP.

Si la PD-FE controla una xarxa troncal, ha de poder **controlar el camí que recorren els fluxos IP** i també les entrades i sortides d'aquests fluxos en l'àmbit que controla. També ha de poder localitzar les entitats PE-FE dins de les xarxes troncals que s'han d'involucrar en la garantia de QoS d'extrem a extrem. Tot això es fa indicant rutes en la xarxa troncal, les quals estan condicionades per la informació rebuda des de Rs i les polítiques (independents de la tecnologia subjacent).

Fa alguna cosa més la PD-FE?

Doncs la PD-FE pot notificar a les entitats de la subcapa de Control de Servei (via el punt de referència Rs) sobre esdeveniments ocorreguts en la xarxa de transport si així ho ha requerit l'entitat que ha sol·licitat els recursos de QoS. Aquests esdeveniments poden haver estat reportats per entitats a càrrec seu (PE-FE via Rw o TRC-FE via Rt).

Per exemple, reportar la pèrdua de connectivitat de transport de qualsevol usuari que tingui una sessió de reserva de recursos activa. D'aquesta manera deixa a la capa de servei que ordeni al RACF d'alliberar tots els recursos reservats per a tal usuari.

Fixeu-vos en la figura 4 que la PD-FE pot tenir interconnexió amb altres entitats externes com les de gestió de mobilitat (MMFC) via una interfície anomenada *Ro* i la de processament de paràmetres de gestió (MPM) via una interfície anomenada *Rm*. El primer s'utilitza per a preguntar al RACF sobre la disponibilitat de recursos per a un usuari en concret en la xarxa d'accés abans de fer la transferència (*handover*). El segon és per a reportar informació d'utilització de la xarxa d'accés o troncal i també informació de monitoratge útil.

b) Entitat Funcional de Control de Recursos de Transport (TRC-FE): la Transport Resource Control Functional Entity du a terme decisions d'admissió de sol·licituds de recursos remeses des de la PD-FE per mitjà del punt de referència Rt. El TRC-FE és una entitat independent del servei per a la qual es fa la sol·licitud de recursos però alhora està adaptada a la tecnologia específica i a la tipologia de la xarxa de transport de què controla els recursos.

Sobre la base d'això últim pren una decisió sobre l'admissió o no dels recursos sol·licitats. Aquesta decisió s'envia en resposta a la PD-FE com un més dels paràmetres que usa aquest per a prendre la decisió final de control d'admissió.

Hi ha la possibilitat que la PD-FE faci aquesta sol·licitud a un sol TRC-FE prefixat i aquest distribueixi la sol·licitud degudament desglossada a altres instàncies de TRC-FE (a manera de jerarquia) distribuïdes al llarg dels segments que formen la xarxa (tots dins d'un mateix domini) i amb gestió de recursos independent. Aquesta comunicació entre TRC-FE es fa per mitjà d'un punt de referència anomenat *Rp*.

Nota

Tingueu en compte que la comunicació entre TRC-FE adjacents és sempre intradomini. L'estàndard de la ITU-T no admet que dues TRC-FE de diferent domini interactuïn. Per a això ja s'ha definit la interacció entre entitats PD-FE pel punt de referència Ri.

Un TRC-FE pot interactuar amb més d'un PD-FE o amb un altre TRC-FE adjacent, sempre dins del seu mateix domini.

El TRC-FE, a més, ha de suportar la modificació de la reserva de recursos i també l'alliberament dels recursos si així ho indica la PD-FE.

Però com pren la TRC-FE la decisió sobre la disponibilitat o no dels recursos sol·licitats?

El TRC-FE és l'element que realment s'adapta a la tecnologia concreta de la xarxa d'accés o troncal, i coneix exactament els mecanismes i els paràmetres de QoS relacionats amb la tecnologia en cada segment. I per a poder fer un control exhaustiu dels recursos es val d'una interfície anomenada *Rc* per a sol·licitar i captar tot tipus d'informació que li ajudi a tenir actualitzada la tipologia i estat dels recursos. Aquesta interfície Rc, la qual és totalment dependent de la tecnologia subjacent de la xarxa de transport, connecta la TRC-FE amb totes

aquelles entitats de la subcapa de Processament de Transport que li puguin proporcionar aquesta informació (no es tanca la porta al fet que la TRC-FE sigui completament autònom sense necessitar aquesta interfície Rc).

A més, sobre la base del resultat d'aquest control d'admissió és capaç d'actualitzar i assignar els recursos en el segment agregat de la xarxa per a complir la QoS sol·licitada des de la PD-FE. Per a això utilitza la interfície Rn, que el comunica amb l'entitat que assigna els recursos en la subcapa de processament de transport (TRE-FE).

Com sol·licita els recursos la PD-FE a la TRC-FE?

Dependrà de si la reserva de recursos de QoS en la PD-FE es fa en mode *push* o mode *pull*. Si és en mode *push*, la PD-FE pot rebre la sol·licitud de nova reserva de recursos de QoS en dues fases (reserva en la primera fase i assignació en la segona) o en una sola (reserva + assignació en una de sola). El procediment de reserva (*Reserve*) i assignació (*Commit*) de recursos en dues fases respon a la PD-FE mateixa, que ho especifica així perquè també així li ho han especificat via Rs.

Diguem que si la PD-FE, una vegada ha autoritzat la petició de QoS, li indica que vol solament "reservar" els recursos, la TRC-FE fa el control d'admissió de capacitat global del sistema, actualitza l'estat d'aquests recursos i dóna resposta a la PD-FE, però no executa l'assignació de recursos ni una instal·lació de polítiques de QoS sobre la TRE-FE (ni tampoc ho farà la PD-FE sobre el/els PE-FE). És quan la PD-FE rep una modificació de la sessió de sol·licitud de recursos quan s'indica que en aquest moment es vol fer ús dels recursos reservats i sol·licita l'assignació.

3) Control de Gestió de la Mobilitat (MMCF)

La ITU-T ha definit aquest conjunt de funcions clarament per copar amb aquelles xarxes els equips d'usuari de les quals ja no estan basats en una passarel·la residencial, sinó que són un sol dispositiu i a més tenen la capacitat de la mobilitat: les xarxes mòbils (LTE), Wi-Fi o WiMAX.

Nota

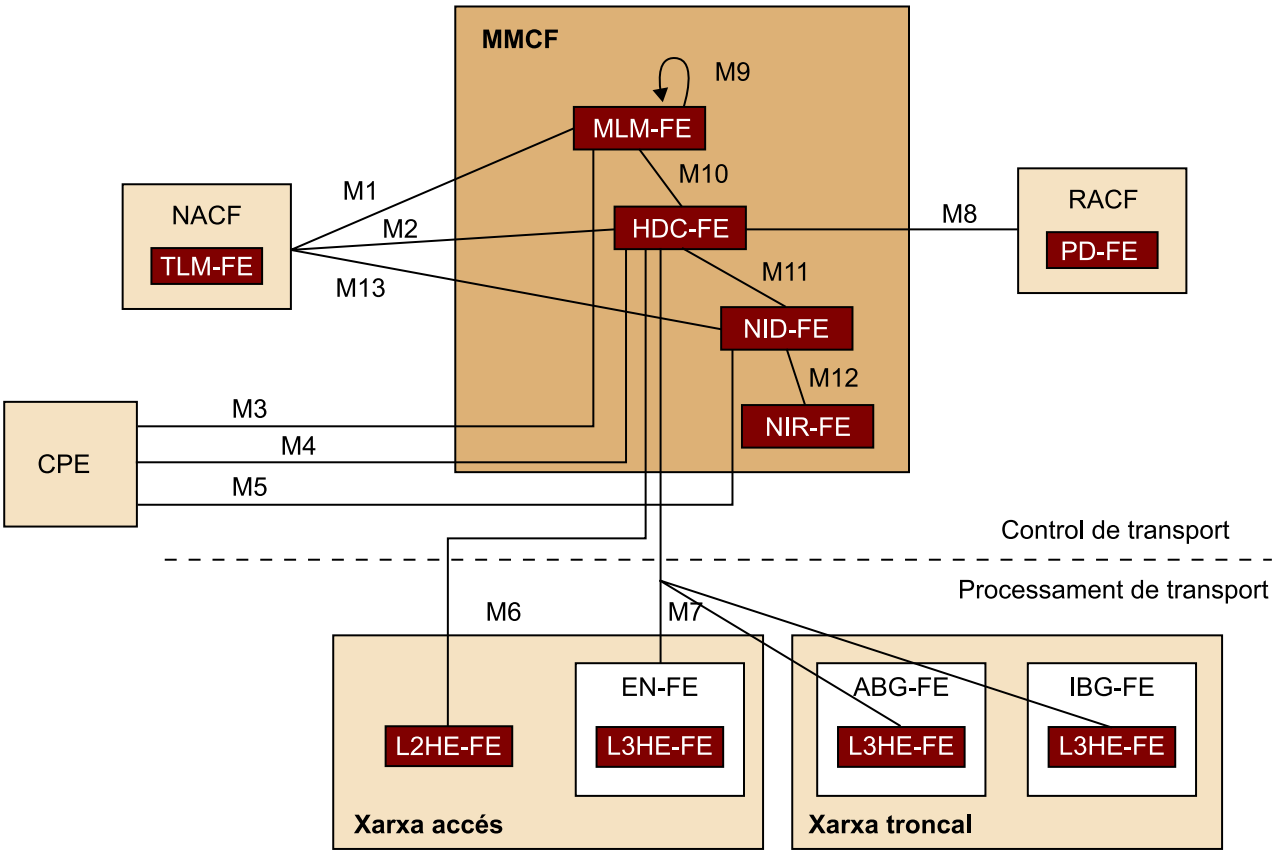
El terminal d'usuari pot suportar més d'una tecnologia sense fil simultània (els telèfons intel·ligents suporten LTE i Wi-Fi), amb la qual cosa es converteixen en el que podem anomenar un *terminal híbrid*.

I és en aquests casos quan la capacitat de mobilitat cobra una gran importància a escala de control de transport. Les xarxes fixes (ADSL, cable, fibra, etc.) no tindrien necessitat d'haver de suportar o implementar aquests blocs de mobilitat.

L'MMCF s'encarrega bàsicament de possibilitar a un usuari que posseeix un terminal mòbil fer una transferència a escala de xarxa de transport de manera transparent per a l'usuari copant fins i tot amb el mecanisme a escala de subcapa de Control de Transport per a la transferència de sessions de reserves de recursos que aquest terminal pugui tenir actives.

Depenent de la tecnologia de la xarxa aquest procés de transferència pot ser liderat pel terminal d'usuari mateix (amb suport de la xarxa) o per la xarxa.

Figura 5. Arquitectura de referència de l'MMCF



Dins de la mobilitat es poden descriure dos modes d'operació:

- **Mobilitat controlada per l'equip d'usuari**: és un mode d'operació en què l'equip d'usuari pren un paper actiu en la provisió del servei de mobilitat en capa 3, concretament contactant amb el proveïdor de servei de mobilitat per a invocar aquest servei tan aviat com aconsegueix l'ingrés a la xarxa.

- **Mobilitat controlada per la xarxa**: és el mode d'operació en què l'equip d'usuari no pren un paper actiu en la provisió del servei de mobilitat. Tota la iniciativa la porta la xarxa.

A continuació veurem una descripció entitat per entitat de l'MMFC i la relació entre cadascuna.

Vegeu també

Un resum dels punts de referència involucrats amb aquest bloc funcional es pot trobar en la taula 6 en l'annex.

a) Entitat Funcional de Gestió de Localització Mòbil (MLM-FE). La Mobile Location Management Functional Entity té una sèrie de responsabilitats relacionades amb la mobilitat, les quals es resumeixen en la llista següent:

- Si la mobilitat està controlada i liderada íntegrament per la xarxa, l'MLM-FE s'encarregaria de registrar la localització inicial en el nom de l'equip d'usuari.

- Processa missatges de registre de localització enviats des de (via M3) o en el nom de l'equip d'usuari (via M1).

- Opcionalment, manté l'associació entre l'identificador d'usuari en el servei de mobilitat i l'adreça IP assignada de manera persistent a l'usuari.

- Gestiona l'associació entre l'adreça IP persistent assignada a un equip d'usuari i l'adreça temporal, si es tracta de mobilitat controlada i liderada pel *host*, o l'adreça de l'extrem del túnel més proper a l'equip d'usuari, si es tracta de mobilitat basada en xarxa (aquesta tecnologia basada en túnels o *bearers* és molt utilitzada en tecnologia LTE i WiMAX).

- De manera opcional, manté dues associacions de localització per a l'equip d'usuari mòbil marcant l'associació per a la xarxa present com a "activa" i marcant l'associació per a la xarxa objectiu com a "*standby*".

- Suporta la separació del pla de control i de dades i permet que l'adreça de l'MLM-FE i l'adreça del terminal per al traspàs de dades (l'adreça del túnel del terminal) siguin diferents.

- Indica una nova associació de mobilitat i distribueix la informació de l'associació a l'HDC-FE (via M10).

b) Entitat Funcional de Control i Decisió de Transferència (HDC-FE). La Handover Decision and Control Functional Entity té tres subfuncions:

- Decisió de transferència (HDF): rep des de l'equip d'usuari una llista d'enllaços d'accés candidats per a fer una transferència i invoca el o els RACF per a verificar la disponibilitat dels recursos de QoS per a cadascun dels enllaços. També sol·licita al RACF reassignació de recursos i QoS en el nou camí de dades (allibera els recursos de l'antic camí alhora que configura els recursos en el nou). A més, pot disparar la transferència sota la petició de l'equip d'usuari (en el cas de lideratge de la mobilitat des de la xarxa). En aquest cas pot comunicar l'acció de transferència a l'element d'execució en capa 2 L2HCF (si la transferència és dins de la subxarxa) i a l'L3HCF (si la transferència és entre subxarxes).

- Control de transferència en capa 2 (L2HCF): es comunica amb l'entitat L2HE-FE en la subcapa de Processament de Transport per a transferir esdeveniments de la capa d'enllaç cap a l'HDF i, sota petició d'aquest, invocar la transferència a la instància apropiada de l'L2HE-FE.

- Control de transferència en capa 3 (L3HCF): es comunica amb l'entitat L3HE-FE en la subcapa de Processament de Transport per a invocar i coordinar, sota petició d'aquest, la transferència a les instàncies apropiades de l'L3HE-FE.

c) Entitat Funcional de Distribució d'Informació de Xarxa (NID-FE). La Network Information Distribution Functional Entity es responsabilitza del següent:

- Distribueix les polítiques de transferència, que són un grup de regles i preferències definides pels operadors NGN que afecten les decisions preses per l'equip d'usuari o l'HDC-FE. Es distribueixen a l'equip d'usuari via la interfície M4 i a l'HDC-FE via la interfície M11.

  Per exemple, una política de transferència pot indicar que una transferència vertical des d'una xarxa d'accés E-UTRAN (LTE) a una xarxa d'accés Wi-Fi no està permès. Podria indicar a més que la xarxa d'accés WiMAX és preferible a Wi-Fi.

- Distribueix una altra informació proporcionada pel NIR-FE (rebuda des de la interfície M12).

d) Entitat Funcional de Repositori d'Informació de Xarxa (NIR-FE). La Network Information Repository Functional Entity proporciona informació estàtica sobre xarxes veïnes a la NID-FE per donar-li suport en el descobriment de les xarxes d'accés i en la presa de decisió de la selecció de la xarxa següent.

1.2.2. Arquitectura de referència de l'ETSI-TISPAN

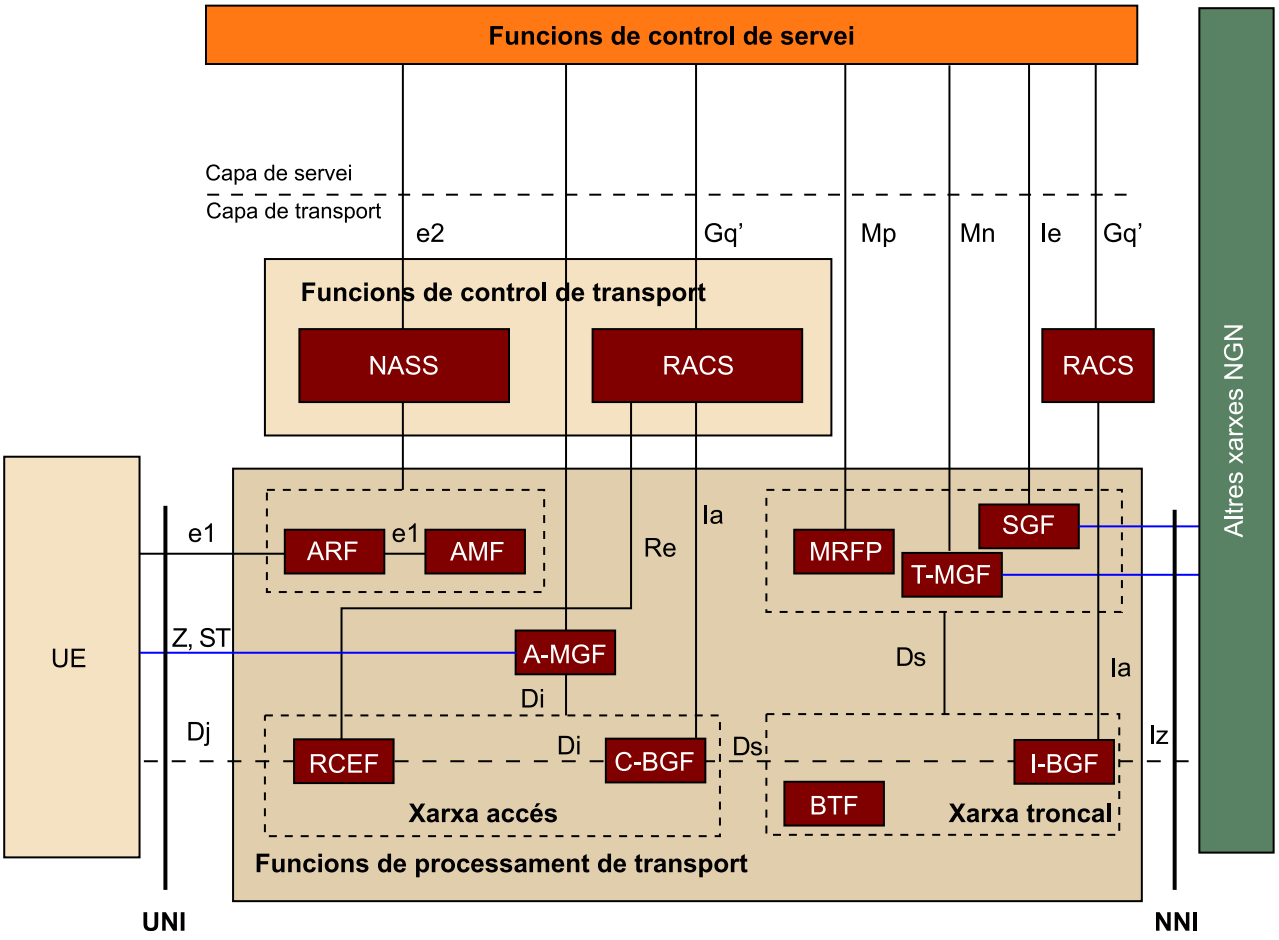
L'ETSI-TISPAN també defineix la capa de transport de les xarxes NGN. La descripció d'alguns blocs és calcada als descrits en la ITU-T, solament que canviant noms de les entitats funcionals i els interfícies. Altres vegades sí que es produeix alguna variació pel que fa a la ITU-T.

Veurem que l'ETSI-TISPAN ha triat el camí de la integració en xarxes NGN de les xarxes d'accés fixes. Ho notareu en el tipus d'equip d'usuari que preveu i en el fet que hi ha funcionalitats que no especifica, com la gestió de la mobilitat.

Subcapa de Processament de Transport

En aquest apartat veurem una descripció funcional de les entitats que conformen la subcapa de Processament de Transport segons el model de l'ETSI-TISPAN subdividides en xarxa d'accés i xarxa troncal. L'arquitectura de referència de l'ETSI-TISPAN es mostra en la figura 6.

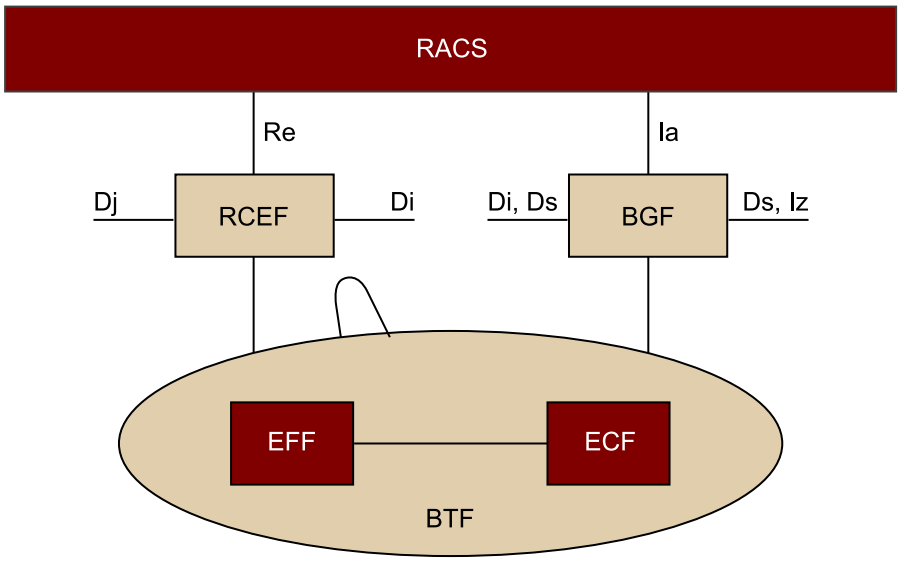
Figura 6. Arquitectura de referència de la subcapa de processament de transport per a l'ETSI-TISPAN



1) Funcionalitat Bàsica de Transport (BTF)

Com en el model de referència de la ITU-T, l'ETSI-TISPAN també defineix entitats funcionals elementals que afecten la simple transferència de paquets IP. En aquest cas es tracta del Basic Transport Function (BTF), la qual se subdivideix en dos elements més senzills: l'entitat elemental de transferència de paquets (EFF) i la de control (ECF).

Figura 7. Components del BTF



Com podem veure en la figura 7, el BTF té la capacitat d'interactuar amb dos elements que processen el trànsit d'usuari:

- l'RCEF, que és l'entitat que aplica polítiques de QoS dictades des del bloc que controla els recursos de la xarxa de transport (RACS) i
- l'entitat fronterera amb altres xarxes de transport de diferent domini administratiu (BGF).

Un exemple d'aquesta interactuació entre el BTF i l'RCEF o el BGF és el mode *pull*, en què els notifiquen sobre esdeveniments relacionats amb la tecnologia de la xarxa de transport i que poden desencadenar una reserva de recursos. La interfície entre l'RCEF o el BGF i aquest element està fora de l'àmbit de l'especificació, ja que depèn molt de la tecnologia de la xarxa.

Vegem la descripció d'aquestes dues entitats elementals segons l'ETSI-TISPAN:

- **Funcionalitat Elemental de Transferència (EFF)**: correspon exactament en funcions amb l'entitat elemental definida per la ITU-T, EF-FE, descrita anteriorment.
- **Funcionalitat Elemental de Control (ECF)**: correspon exactament en funcions amb l'entitat elemental definida per la ITU-T, EC-FE, descrita anteriorment.

2) Entitats funcionals de Processament de transport en la xarxa d'accés

Continuant la mateixa classificació d'entitats funcionals de la subcapa de processament de transport seguida en l'especificació de la ITU-T, explicarem quines entitats correspondrien a la xarxa d'accés i quins paral·lelismes tenen amb les entitats equivalents de la ITU-T. Si mirem l'arquitectura de referència de la figura 6 podem veure un total de 4 entitats funcionals.

a) Funcionalitat de Passarel·la de Mitjans d'Accés (A-MGF): l'Access Media Gateway Function interconnecta la xarxa d'accés NGN amb terminals d'usuari amb tecnologia de xarxes tradicionals de telefonia (XTC i XDSI). Així doncs, equival a l'entitat funcional AMG-FE de la ITU-T[2].

[(2)]Vegeu el subapartat "Subcapa de control de transport".

b) Funcionalitat d'Aplicació de Control de Recursos (RCEF): la Resource Control Enforcement Function és una entitat funcional que s'encarrega primordialment d'aplicar les polítiques de QoS que el RACS li indica via un punt de referència anomenat *Re*. Aquestes polítiques, anomenades *Policy Rules*, poden estar predefinides en el bloc mateix i el RACS simplement hi ha de fer referència per a activar-les o desactivar-les. O bé el RACS les pot definir per complet indicant paràmetres de classificació de trànsit (fluxos IP), nivell de prioritat (marcatge de ToS) i identificadors de classificació de transport.

Nota

L'ETSI també defineix un subtipus de l'A-MGF: l'R-MGF (Residential) que és com el mateix que l'A-MGF però integrat en la passarel·la residencial (localitzades en instal·lacions de l'usuari).

Classificadors de transport

Els anomenats *classificadors de transport*, que l'ETSI-TISPAN indica, són molt útils per a relacionar les polítiques de QoS per a aplicar a la connectivitat amb l'equip d'usuari en qüestió, com per exemple un identificador de canal virtual en ATM.

L'RCEF pot actuar en mode *push* en l'assignació de recursos, en què rep aquestes polítiques des del RACS i les aplica **mapant els paràmetres de QoS de la política** (independents de la tecnologia subjacent) amb paràmetres específics de la tecnologia de la xarxa d'accés.

L'RCEF pot actuar també en mode *pull*, en el qual rep una notificació des de l'entitat elemental BTF (dependent de la tecnologia de la xarxa d'accés) dient que un equip d'usuari sol·licita recursos. El RCEF reformata el missatge segons l'especificació de la interfície Re per a notificar-ho al RACS i esperar una presa de decisió d'aquest (en forma d'instal·lació de noves polítiques).

Independentment del mode com treballem, l'RCEF pot **reportar esdeveniments** a escala de capa de transport que puguin provocar una presa de decisió del RACS sobre les polítiques de QoS actives (les pot eliminar o modificar, depenent de les polítiques de l'operador).

Traçant un paral·lelisme amb el model de referència de la ITU-T, l'RCEF es correspon amb les entitats funcionals equivalents de la ITU-T en processament de Transport com l'AN-FE o CGPE-FE, aquest en el costat de l'equip d'usuari. És a dir, se situa en aquell lloc on hi ha potencialitat de coll d'ampolla o on s'ha de fer assignació directa de recursos a la xarxa d'accés.

c) Funcionalitat de Passarel·la Fronterera (C-BGF): sobre la Core Border Gateway Function, com es diu en anglès, es pot dir que equival a l'entitat funcional de la ITU-T anomenada *EN-FE*, entitat funcional fronterera entre la xarxa d'accés i la xarxa troncal de diferent domini administratiu[3], exceptuant les funcions que afecten la mobilitat en 3, les quals no són implementades en el model de l'ETSI-TISPAN. El C-BGF és controlat pel bloc de Control Admissió i Recursos (RACS) en la subcapa de Control de Transport per mitjà d'un punt de referència anomenat *Ia*, que equival en funcions a la interfície Rw de la ITU-T.

[(3)]Vegeu el subapartat "Subcapa de control de transport".

d) Funcionalitat de Retransmissió de Xarxa d'Accés (ARF): l'Access Relay Function equival exactament a l'entitat funcional del model de la ITU-T anomenat *AR-FE*[4]. S'interconnecta amb el NASS, el bloc de funcions equivalent al NACF de la ITU-T per a l'adhesió a la xarxa d'accés.

(4)Vegeu el subapartat "Subcapa de control de transport".

3) Entitats funcionals de Processament de transport a la xarxa troncal

Passem la frontera de la xarxa d'accés per a passar-nos a l'àmbit de la xarxa troncal d'alta capacitat. En aquest àmbit identifiquem un total de quatre entitats. Veurem com hi ha un paral·lelisme molt clar amb les entitats de processament de transport de la xarxa troncal en el model de referència de la ITU-T.

a) Funcionalitat de Passarel·la Fronterera (I-BGF): sobre la Interconnection Border Gateway Function, com es diu en anglès, es pot dir que equival a l'entitat funcional de la ITU-T anomenada *IBG-FE*, entitat funcional fronterera entre dues xarxes troncals de diferent domini administratiu[5], exceptuant les funcions que afecten la mobilitat en 3, les quals no són implementades en el model de l'ETSI-TISPAN. L'I-BGF és controlat pel bloc de Control d'Admissió i Recursos (RACS) en la subcapa de Control de Transport per mitjà d'un punt de referència anomenat *Ia*, que equival en funcions a la interfície Rw de la ITU-T.

(5)Vegeu el subapartat "Entitats funcionals de processament de transport en la xarxa troncal".

b) Funcionalitat de Passarel·la cap a Xarxes de Circuits (T-MGF): equival a l'entitat funcional TMG-FE de la ITU-T[6]. La interfície que la connecta amb l'element de la capa de Control de Servei és l'anomenada *Mn* (equivalent a la interfície S-T4 definida per la ITU-T).

(6)Vegeu el subapartat "Entitats funcionals de processament de transport en la xarxa troncal".

c) Processament de Funcionalitats de Recursos Multimèdia (MRFP): el Media Resource Function Processor equival exactament a l'entitat funcional MRP-FE del model de la ITU-T[7]. La interfície que el connecta amb l'element de la capa de Control de Servei és l'anomenada *Mp* (equivalent a la interfície S-T1 definida per la ITU-T).

(7)Vegeu el subapartat "Entitats funcionals de processament de transport a la xarxa troncal".

d) Funcionalitat de Passarel·la de Senyalització (SGF): la Signalling Gateway Function equival exactament a l'entitat funcional SG-FE del model de la ITU-T[8]. La interfície que la connecta amb l'element de la capa de Control de Servei és l'anomenada *Ie* (equivalent a la interfície S-T3 definida per la ITU-T).

(8)Vegeu el subapartat "Entitats funcionals de processament de transport a la xarxa troncal".

Subcapa de Control de Transport

De la mateixa manera que en el model de la ITU-T, en la subcapa de control de transport hi ha la intel·ligència de gestió de recursos tant de la xarxa d'accés com de la xarxa troncal. Defineix els mateixos punts de referència oberts que els connecten amb la capa de Servei i que proporcionen la independència entre la tecnologia de la xarxa de transport i els serveis amb garantia de QoS d'extrem a extrem. Aquesta subcapa està formada per dos blocs principals: el de Control d'Adhesió a la xarxa (NASS en les seves sigles en anglès), el de Con-

trol d'Admissió i Recursos (RACS). A diferència del model de la ITU-T, el de l'ETSI-TISPAN no preveu cap bloc de funcions que gestionin la mobilitat ja que se centra en la integració de xarxes fixes en les xarxes NGN.

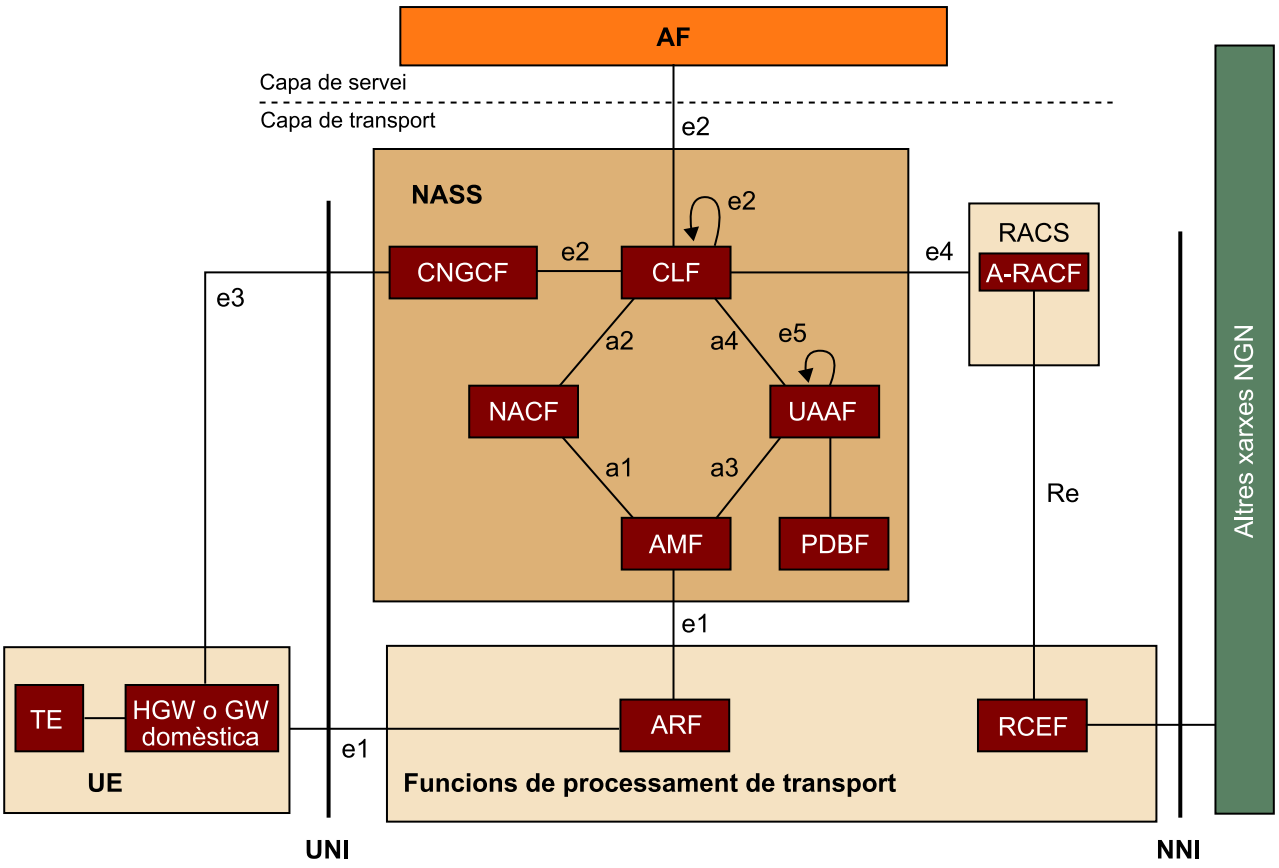
1) Subsistema d'Adhesió a la Xarxa (NASS)

El diagrama següent mostra la composició de l'arquitectura de referència per al NASS segons l'ETSI-TISPAN. Equival íntegrament entitat rere entitat i interfície rere interfície amb el model de la ITU-T, el NACF, amb excepció de l'absència d'interactivitat amb algun bloc que gestioni la mobilitat en la capa de transport.

Vegeu també

En la taula 7 de l'annex es pot veure un resum dels punts de referència del NASS.

Figura 8. Arquitectura de referència del NASS per a l'ETSI-TISPAN



Nota

L'ETSI-TISPAN s'ha especialitzat a integrar les xarxes fixes cablades en l'estàndard de les xarxes NGN i és per això que l'estàndard de l'ETSI per a NGN no preveu interfícies (punts de referència) a cap bloc funcional que gestioni la mobilitat en la capa de transport. Els terminals són fixos i, per tant, no hi ha mobilitat per suportar, almenys tal com l'entenem en les xarxes mòbils de 3GPP.

a) Funcionalitat de Configuració d'Accés a la Xarxa (NACF): la Network Access Configuration Function equival exactament a l'entitat funcional NACFE del model de la ITU-T per al NACF, amb l'única excepció que assigna una IP

i no dues (solament la IP persistent, en no haver-hi mobilitat). De la mateixa manera els punts de referència anomenats *a1* i *a3* corresponen als Nd i Na del model de la ITU-T, respectivament.

b) Funcionalitat d'Autenticació i Autorització de l'Usuari (UAAF): la User Authentication and Authorizaction Function (UAAF) equival exactament a l'entitat funcional TAA-FE del model de la ITU-T per al NACF (inclusivament les seves funcionalitats de servidor intermediari en un escenari d'itinerància). De la mateixa manera que els punts de referència anomenats *a3*, *a4* i *e5* corresponen als *Na*, *Nc* i *Ni* del model de la ITU-T, respectivament.

Nota

I també en el model de la ITU-T es defineix un punt de referència entre la TAA-FE i la TUP-FE, en l'ETSI-TISPAN no n'especifiquen cap (llibertat total d'especificació) entre l'UAAF i el PDBF.

c) Funcionalitat de Base de Dades de Perfils (PDBF): la Profile Data Base Function (PDBF) és, com el seu nom indica, el lloc on s'emmagatzema tota la informació de credencials i perfils de QoS a escala de transport. En definitiva, equival exactament a la TUP-FE de la ITU-T. El format dels perfils d'usuari és equivalent als de la ITU-T.

Lectura complementària

Podeu trobar més informació sobre el format proposat per a aquests perfils en el document ES 282 004.

d) Funcionalitat de Repositori i Localització de Connectivitat de Sessió (CLF): la Connectivity session Location and repository Function equival exactament amb l'entitat funcional TLM-FE del model del model de la ITU-T per al NACF (inclusivament la seva funcionalitat de servidor intermediari en un escenari d'itinerància amb un CLF d'un altre domini). De la mateixa manera que els punts de referència anomenats *a2*, *a4*, *e2* i *e4* corresponen als *Ne*, *Nc* (*S-TC1*, *Ng* i *Nx*) i *Ru* del model de la ITU-T, respectivament.

Veiem que la interconnexió amb la subcapa de Control de Servei (per a l'ETSI es diu Application Function o AF) es fa per mitjà del punt de referència e2, però a diferència de l'ITU-T s'especifica la mateixa interfície per a interconnectar el CLF amb el CNGCF (l'equivalent d'HGWCFE amb la seva interfície Nx) i que el que interconnecta el CLF visitat amb el CLF local (mode itinerància a escala de CLF).

Per a l'ETSI-TISPAN, es defineix l'AF com aquella entitat de la capa 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 RACS via la interfície Gq'. Si el servei està basat en IMS l'AF serà el P-CSCF i si no està basat en IMS serà una entitat equivalent.

e) Funcionalitat de Configuració de la Passarel·la de la Xarxa del Client (CNGCF): la Customer Network Gateway Configuration Function (CNGCF) equival exactament a l'entitat funcional HGWC-FE del model de la ITU-T per al NACF. De la mateixa manera que els punts de referència e2 i e3 corresponen als Nx i TC-Ux del model de la ITU-T, respectivament.

Passarel·la residencial (CNG)

L'ETSI-TISPAN considera, gairebé com l'única opció, que l'equip d'usuari o UE estigui format per una passarel·la residencial (CNG) i darrere tota una xarxa local de client amb dispositius connectats. En aquesta passarel·la CNG, com l'element equivalent de la ITU-T per a passarel·les residencials, es desenvolupen les Funcions d'Usuari, com per exemple:

- aplicació de polítiques de QoS des del RACS,
- interfície per a autenticació dels usuaris a la xarxa local (en suport del NASS),
- traducció de protocols de senyalització a IMS per a suportar terminals d'altres tecnologies en aquesta xarxa local, i
- aplicació de traduccions d'adreces IP o ports (NAT o NAPT).

L'ETSI-TISPAN ha dedicat esforços a la definició concisa de les Funcions d'Usuari atribuïdes a una CNG. Una descripció més detallada (amb blocs funcionals i tots els punts de referència) la podeu trobar en el document TS 185 003.

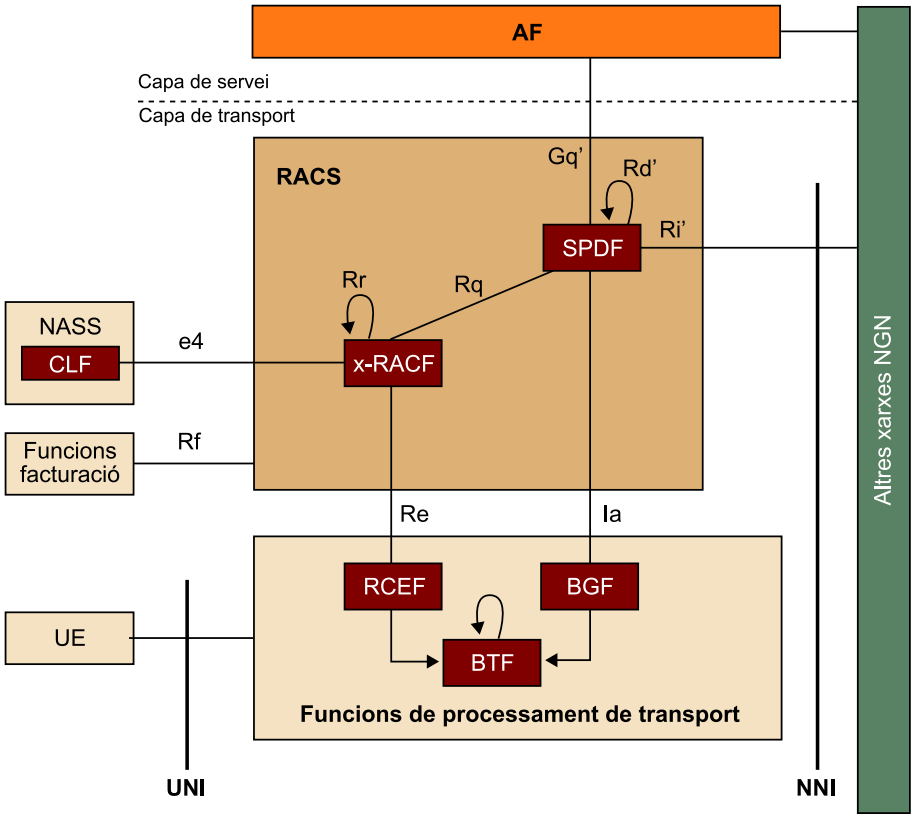
2) Subsistema de Control d'Admissió i Recursos (RACS)

La figura 9 mostra l'arquitectura funcional de referència del RACS. Encara que manté moltes similituds amb l'arquitectura de referència de la ITU-T del RACF, sí que té certes diferències a escala de distribució de funcions de control d'admissió entre els blocs que la formen. El RACS està format per dues entitats funcionals, les quals descriurem a continuació.

Vegeu també

En la taula 8 de l'annex podeu trobar un resum de les interfícies del RACS.

Figura 9. Arquitectura de referència del RACS per a ETSI-TISPAN



a) Funcionalitat de Decisió de Polítiques de Servei (SPDF): la Service Policy Decision Function, com el seu equivalent en el model de la ITU-T (PD-FE), representa per a la subcapa de Control de Servei (AF) un únic punt de contacte amb la capa de transport a l'hora d'autoritzar i aplicar reserves de recursos de transport i QoS.

L'SPDF aplica el que es coneix com a **polítiques basades en serveis** per a prendre la decisió final sobre l'acceptació o no de la sol·licitud de nova sessió de reserva de recursos de QoS i també la modificació d'una sessió ja activa. Aquesta reserva l'ETSI-TISPAN l'anomena *sessió de servei de control de transport*. Aquestes sol·licituds poden ser rebudes des de l'AF (mode *push*) via un punt de referència anomenat *Gq'* o des d'un altre SPDF adjacent via una interfície anomenada *Ri'* (si és d'un altre domini administratiu a manera d'itinerància) o via una interfície anomenada *Rd'* (si són del mateix domini). El resultat d'aquesta decisió, ja sigui positiva o negativa, s'ha de notificar a l'AF o SPDF adjacent via la interfície des d'on s'hagi rebut la petició.

Una **política basada en servei** és aquella política dissenyada per a ser aplicada per l'SPDF. Està formada per una Condició sobre el servei descrit en la petició rebuda i per una Acció per a prendre si la condició es compleix. La Condició està basada en la comparació de paràmetres inclosos en la informació rebuda en la petició amb valors especificats en la política mateixa. Si la comparació compleix la política llavors la sol·licitud és autoritzada i es procedeix a l'Acció, la qual pot implicar interrogar altres elements del RACS o de la subcapa de Processament de Transport sobre els recursos disponibles (l'x-RACF, la BGF, un altre SPDF o qualsevol combinació d'aquests).

L'SPDF ha de suportar la sol·licitud de terminació de la sessió de reserva de recursos. Això desencadena en l'x-RACF l'alliberament de recursos i la desinstal·lació de les polítiques que se'ls apliquin.

Un SPDF es pot comunicar amb més d'un AF i amb altres SPDF adjacents (ja sigui dins del seu domini administratiu o en un de diferent a manera d'itinerància).

Per a l'ETSI-TISPAN quins passos ha de fer l'SPDF per a prendre la decisió final sobre si autoritzar o no una nova (o modificada) sol·licitud de recursos en mode *push* a la xarxa de transport (ja sigui d'accés o troncal)?

Per a l'SPDF prendre aquesta decisió comporta fer una llista de control d'admissions similar a les dutes a terme pel PD-FE de la ITU-T i també esperar la notificació d'altres elements del RACS:

- Ha d'**autoritzar la sol·licitud mateixa de recursos de QoS** aplicant regles de polítiques de xarxa arbitràries a escala de servei i també SLA particulars amb l'operador de l'AF.

- Ha de **sol·licitar la reserva o assignació dels recursos a la xarxa de transport** sempre que la sol·licitud rebuda hagi estat autoritzada. En tal cas, la política de servei mateixa dirà a l'SPDF quins altres elements del RACS

haurà de consultar (a un o més x-RACF per a la reserva de recursos o a un C/I-BGF per a la traducció de ports o habilitació d'accés de tallafoc). La resposta d'aquesta consulta o consultes condicionarà la decisió final per prendre.

L'**SPDF no té coneixement en absolut de la topologia ni de la tecnologia** subjacent de la xarxa d'accés (o troncal, si fos el cas). Tampoc no té accés a informació de perfil de subscripció d'usuari ni de l'estat dels recursos del sistema. Aquest és un dels serveis que sol·licita a l'x-RACF via una interfície anomenada *Rq* (aquesta interfície és intradomini), la resposta de la qual és necessària per a poder prendre la decisió final. En el cas que hi hagi un C/I-BGF en la xarxa de transport l'SPDF sol·licitaria a aquest el servei d'assignació de traducció d'**adreça IP o ports, control de limitació de velocitat**, **habilitació d'accés** (Gate Control) i **marcatge de paquets**. La resposta a aquesta sol·licitud enviada des del C/I-BGF (via la interfície Ia) s'hauria de tenir en compte també abans d'enviar la resposta a l'AF.

Fa alguna cosa més l'SPDF?

Doncs l'SPDF pot notificar a l'AF (via el punt de referència Gq') sobre esdeveniments ocorreguts en la xarxa de transport si així ho ha requerit l'entitat que ha sol·licitat els recursos de QoS. Aquests esdeveniments poden haver estat reportats per entitats a càrrec seu (C/I-BGF via Ia o x-RACF via Rq).

A part de tot això, l'SPDF és capaç de **processar la prioritat de petició de servei**. És a dir, l'AF o SPDF interconnectat pot indicar a l'SPDF en la sol·licitud un nivell de prioritat de servei (servei de control de transport). D'acord amb aquest nivell, l'SPDF pot definir un nivell de prioritat de servei en la seva sol·licitud de reserva de recursos enviada a l'x-RACF.

b) Funcionalitat Genèrica de Control d'Admissió de Recursos (x-RACF): la Resource and Admission Control Function és una entitat funcional que rep sol·licituds de servei de reserva o assignació de recursos des de l'SPDF per mitjà de la interfície Rq (si la reserva és en mode *push*) o des de l'RCEF via la interfície Re (si la reserva és en mode *pull*).

x-RACF i SPDF

L'x-RACF i l'SPDF amb el qual està interconnectat sempre estaran en el mateix domini. No es preveu cap punt de referència d'interconnexió entre dues x-RACF que pertanyin a diferents dominis administratius (la itinerància a escala de sol·licitud de recursos és sempre a escala d'SPDF).

L'x-RACF realment és un punt de decisió més on es fa un nou control d'admissió diferent del que fa l'SPDF (aplicable tant a trànsit unidestinació –*unicast*– com multidestinació –*multicast*–). El resultat d'aquesta decisió s'ha de notificar a l'SPDF després de la recepció de la petició.

No obstant això, els tipus de control que fa depenen del tipus d'x-RACF que s'implementi. L'ETSI-TISPAN en preveu dos tipus:

- **A-RACF (Access)**: es tracta del que està situat en l'àmbit de la xarxa d'accés. Amb això fa doble control d'admissió: primer comprova que la petició de recursos entra **dins del perfil QoS de subscriptor** de l'usuari que els sol·licita i després **comprova que hi ha suficients recursos** a la xarxa d'accés per a reservar o assignar aquests recursos. Per a fer el control de perfil de subscriptor pot accedir a la informació de perfil per mitjà d'una interfície anomenada *e4*, que el connecta amb l'entitat funcional de Repositori i Localització de Connectivitat de Sessió (CLF) dins del bloc de Control d'Adhesió a la Xarxa (NASS).

  Control de subscripció d'usuari

  La funció de control de subscripció d'usuari solament s'aplica a l'A-RACF i ha d'autenticar i autoritzar els recursos que sol·liciten les entitats funcionals (RCEF en mode *pull* i SPDF o un altre RACF en mode *push*) en nom d'un subscriptor. Ha de comprovar que la sol·licitud de recursos estigui dins dels paràmetres esperats segons el perfil del subscriptor, o dit d'una altra manera, que un subscriptor no sol·liciti més recursos dels que ha contractat.

- **C-ARACF (Core)**: en aquest cas es tracta del que està situat en l'àmbit de la xarxa troncal. Amb això solament fa la **comprovació que hi ha suficients recursos**. Aquesta implementació no fa el control d'admissió sobre el perfil QoS del subscriptor (amb la qual cosa no té interfície e4).

En tots dos casos, si al final el control d'admissió ha estat satisfactori i la sol·licitud de recursos rebuda ho especifica així, l'x-RACF assigna els recursos sol·licitats i pot decidir si és necessari instal·lar i aplicar polítiques de QoS sobre les entitats d'aplicació de polítiques de QoS de la subcapa de Processament de Transport (RCEF) via la interfície Re.

Nota

Igual que amb el cas de la TRC-FE de la ITU-T, l'x-RACF i l'SPDF han de suportar la reserva de recursos en dues fases (*Reserve* i *Commit*) o en una sola fase (*Commit*) per al cas de reserva en mode *push*.

L'x-RACF és un element que coneix la topologia de la xarxa d'accés o troncal però les polítiques de QoS que confecciona contenen majoritàriament paràmetres de QoS independents de la tecnologia de la xarxa d'accés. Serà l'RCEF qui, en instal·lar-les, traduirà aquests en uns paràmetres equivalents adaptats a la tecnologia de la xarxa d'accés.

Nota

Cada política de QoS porta associat un nom que la identifica de manera única pel que fa a altres polítiques. I el seu estat d'activació o desactivació en l'RCEF va íntimament lligat a l'estat de la sessió de petició de recursos que les ha creades. Amb això, quan es rebi una sol·licitud de terminació d'aquesta sessió de reserva des de l'SPDF (mode *push*) o RCEF (mode *pull*) les polítiques corresponents han de ser desinstal·lades.

Segons la complexitat de la xarxa de transport (amb diversos segments susceptibles d'una gestió particular d'alguns recursos) l'x-RACF es pot multiplicar en diverses instàncies dins del mateix domini repartides per diverses parts de la xarxa. Així, doncs, un x-RACF pot rebre una sol·licitud de recursos des de l'SPDF i a continuació pot delegar el control de part o tots els recursos en altres instàncies de RACF. L'intercanvi d'informació entre x-RACF es fa via un punt de referència intradomini anomenat *Rr*.

A part de tot això, l'x-RACF és capaç de **processar per separat la prioritat de petició de mitjans d'una banda i de servei per l'altra**. També és capaç de processar esdeveniments rebuts des de l'RCEF sobre la xarxa de transport i reenviar-los a l'SPDF.

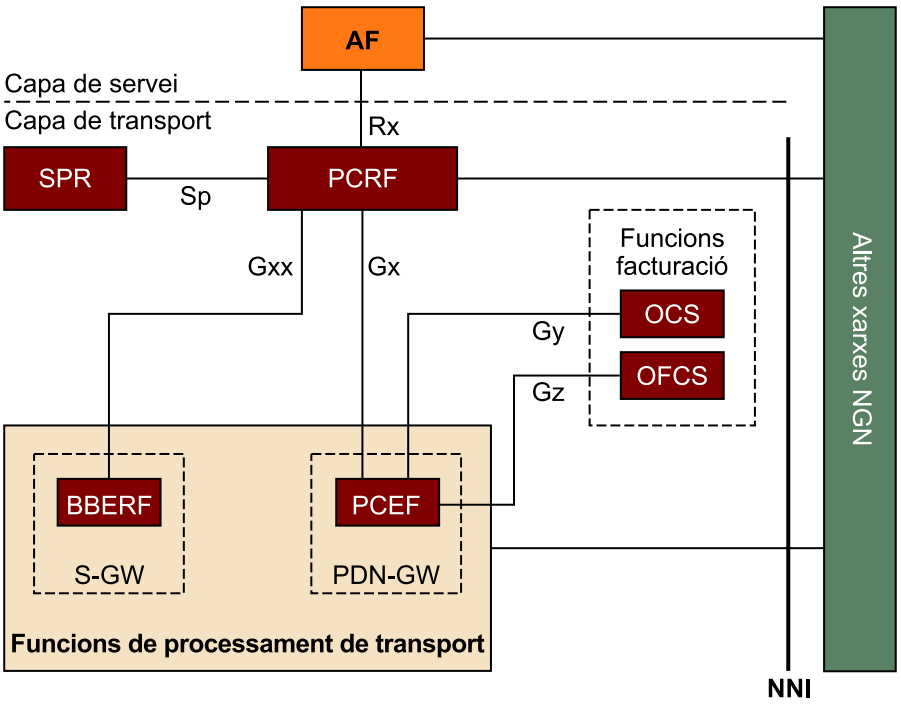
Què significa el nivell de prioritat de mitjans?

L'estàndard defineix que per a la sol·licitud de recursos l'SPDF o x-RACF adjacent ha de desglossar aquesta sol·licitud en components de mitjans (VÍDEO, ÀUDIO, TEXT, etc.) i cadascun podrà tenir un nivell de prioritat més o menys alt pel que fa a altres mitjans dins de la mateixa sol·licitud.

1.2.3. Arquitectura de referència del 3GPP

El 3GPP és l'entitat que ha especificat les tecnologies més importants de telefonia mòbil, des de GPRS passant per UMTS i acabant en LTE. En la figura 10 es pot apreciar l'arquitectura de referència del model de control de polítiques que el 3GPP proposa. Es diu Control de Polítiques i Càrrecs (Policy Control and Charging o PCC) i permet als operadors fer control de polítiques de QoS basades en servei i control de càrrecs basats en fluxos.

Figura 10. Arquitectura de referència del PCC



Veurem primer conceptes clau i també l'arquitectura funcional de la xarxa d'accés i troncal d'LTE (anomenada *Evolved Packet System*) i posteriorment veurem el model de referència PCC amb tots els seus blocs i les seves interfícies.

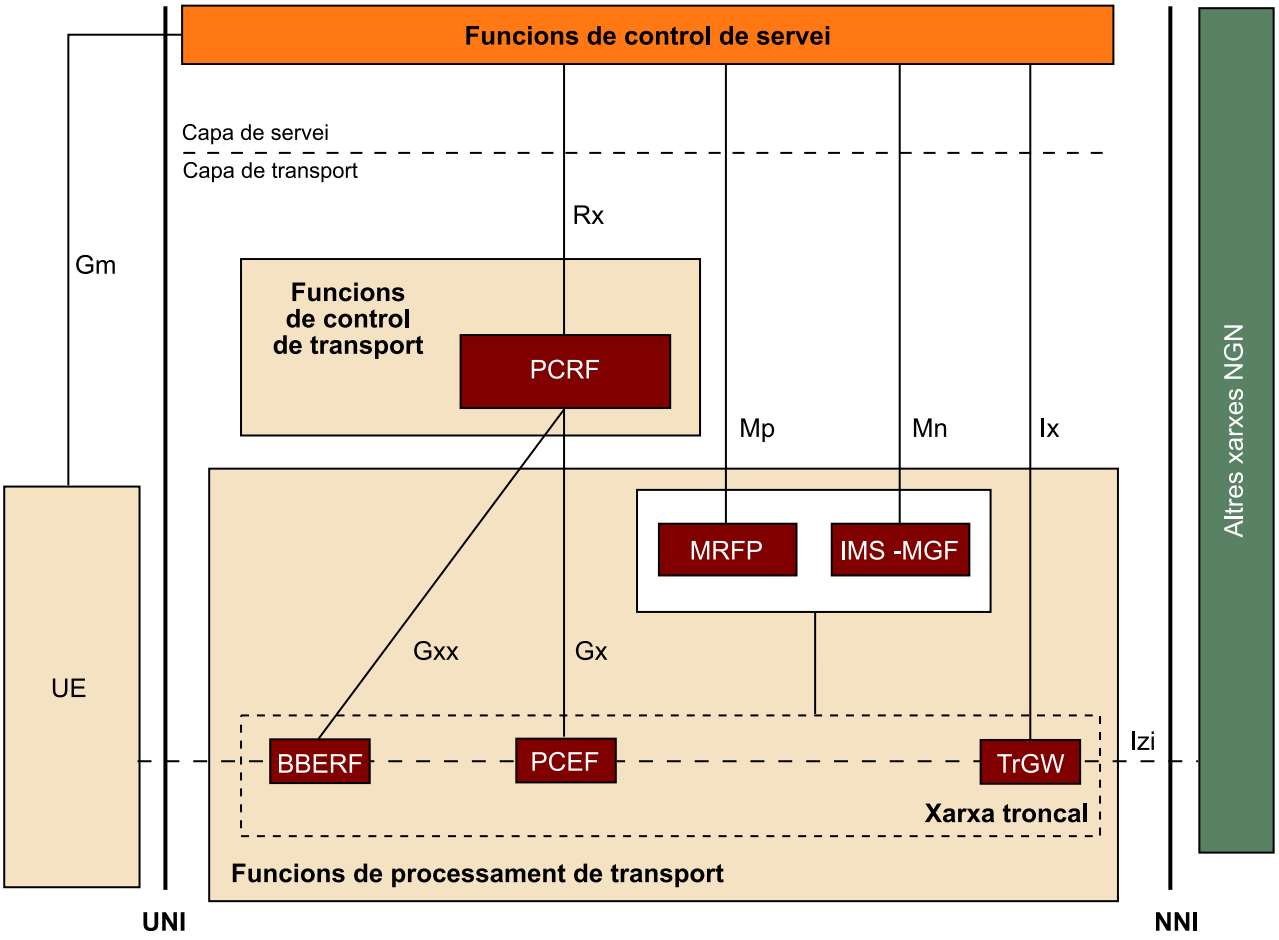
Vegeu també

Sobre els blocs i interfícies del model de referència PCC, en podeu veure un resum explicatiu en la taula 9 de l'annex.

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

En la figura següent podem veure altres funcions de processament de transport a part de les mostrades en la figura que mostra el model PCC.

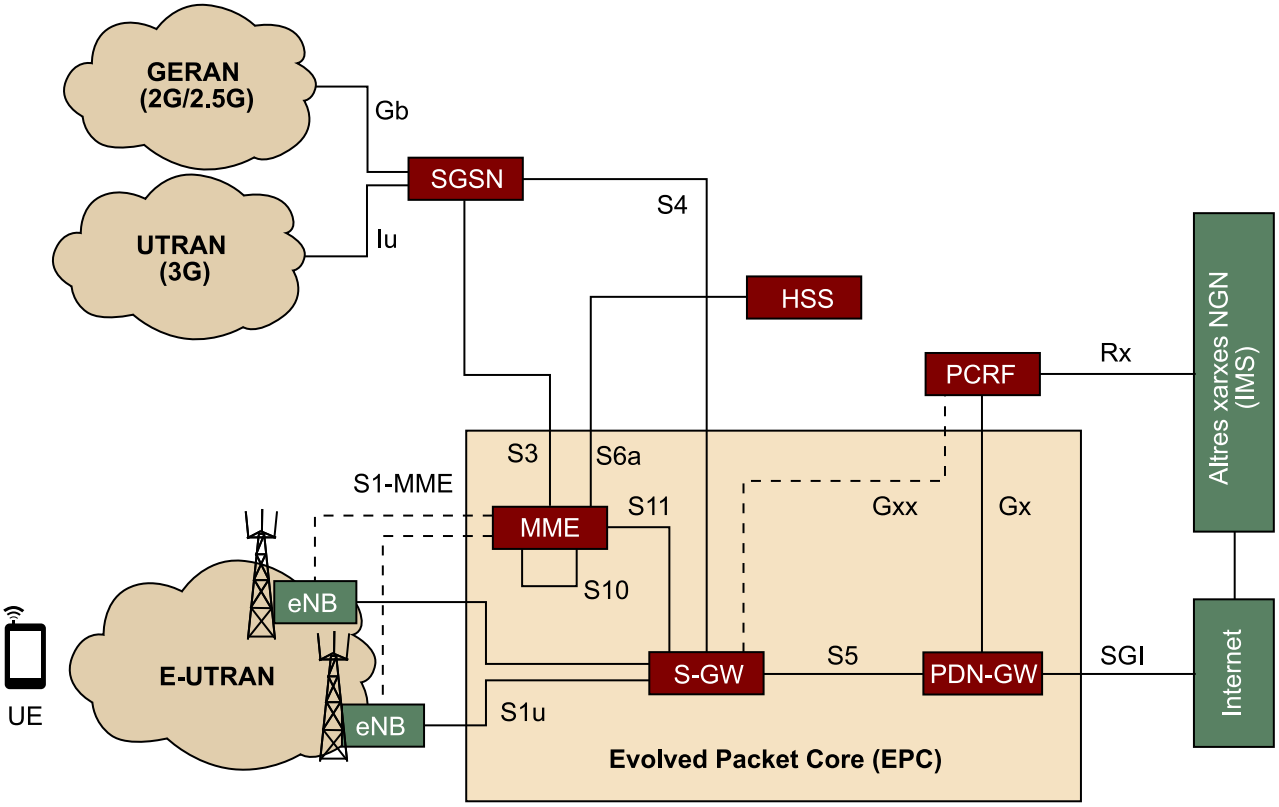
Figura 11. Altres funcions de processament de transport segons 3GPP



Introducció a l'Evolved Packet System

La figura 12 mostra l'arquitectura de l'EPS, també anomenada *SAE* (System Architecture Evolution). A continuació veurem els elements que la componen.

Figura 12. Arquitectura de referència d'EPS



Comencem per la part de l'equip d'usuari (UE). L'equip d'usuari en una xarxa de comunicacions mòbils LTE equival a un terminal únic portàtil (no preveu *a priori* l'existència d'una passarel·la residencial amb equips connectats al darrere). Això té simplificacions importants en l'arquitectura de processament de transport en la part de la xarxa d'accés.

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

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

En aquest servei de mobilitat cal destacar un altre element molt important: l'MME o Mobility Management Entity. Aquest element no processa paquets d'usuari sinó que fa tasques de control de mobilitat dins de les xarxes 3GPP.

Nota

Les xarxes 3GPP es consideren no solament 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 per mitjà de punts de referència dedicats que l'uneixen amb els nodes d'aquestes xarxes d'accés ràdio (GERAN per a GPRS i UTRAN per UMTS).

L'MME fa altres funcions. Per exemple, aglutina informació actualitzada de localització de cada equip d'usuari (a quin eNodeB està associat). Això és important quan es produeix una trucada entrant cap a un usuari (el servei de localització s'anomena *paging*) i cal localitzar-lo. També fa tasques d'autenticació de l'equip d'usuari al moment en què es produeix l'adhesió a la xarxa. És per això que l'MME té un punt de referència dedicat d'interconnexió a l'HSS (Home Subscriber Server), on s'emmagatzema la informació de credencials de l'usuari i perfil de subscripció a escala de transport (i també a escala de Control de Servei). Finalment l'MME també té tasques de gestió de *radio bearers*.

Finalment tenim l'últim element de l'EPC, el PDN GW o Packet Data Network Gateway. És l'element fronterer del sistema EPS amb altres xarxes externes com Internet o IMS. Aquest element té un paper molt important en la garantia de QoS, com veurem més endavant. Aquesta entitat també s'encarrega d'assignar les adreces IP als equips d'usuaris.

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

Per començar definirem el concepte d'***EPS bearer***. L'*EPS bearer* és un canal virtual amb unes característiques de QoS i amplada de banda particulars. És a dir, és una espècie de túnel els extrems del qual van des de l'equip d'usuari mateix fins a la PDN GW i tot paquet IP que entri en aquest túnel gaudirà d'un tractament a escala de garantia de QoS especifiques al llarg de tot l'EPC. A partir d'ara anomenarem l'*EPS bearer* com a túnel EPS.

Nota

El 3GPP ha definit un concepte més abstracte associat al túnel EPS en els documents d'especificació com a *IP-CAN bearer* o IP-Connectivity Access Network *Bearer*. Hi ha dos tipus d'*IP-CAN bearer*: *default bearer* i *dedicated bearer*.

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 del 3GPP prohibeix explícitament que més d'un túnel EPS es pugui mapar a una sola portadora ràdio.

Així, un sol equip d'usuari pot tenir més d'un *IP-CAN bearer* (túnel IP-CAN a partir d'ara) establert amb la PDN GW corresponent i cadascun té les seves característiques pròpies de QoS. Els túnels IP-CAN poden ser unidireccionals o bidireccionals i poden ser establerts, modificats o alliberats per l'equip d'usuari mateix o per la xarxa d'accés.

Quins paràmetres defineix el 3GPP per a caracteritzar a escala de QoS un túnel IP-CAN? El 3GPP ha definit quatre paràmetres:

1) QoS Class Identifier: que defineix el comportament de QoS del trànsit associat a un túnel IP-CAN.

Un QCI, o *QoS Class Identifier*, és un identificador que especifica 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 enter 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 des de l'equip d'usuari fins a la PDN GW) i Taxa de Pèrdua de Paquets (la taxa de pèrdua de paquet màxima desitjada des de l'equip d'usuari fins a la PDN GW). El 3GPP ha estandarditzat 9 QCI, amb valors assignats als respectius paràmetres, per a nou tipus de serveis predefinits.

2) Allocation and Retention Priority: aquest paràmetre indica com d'important (nivell de prioritat) és el túnel IP-CAN pel que fa a altres túnels IP-CAN.

> Posem un 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 IP-CAN no es pot fer perquè no hi ha recursos suficients? Doncs cal desallotjar altres túnels IP-CAN 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: indica la quantitat garantida de bits per segon que es necessiten (capacitat reservada) per a aquest túnel IP-CAN. S'usa solament per a serveis en temps real. El GBR es pot modificar si es requereix una ampliació o disminució del volum de trànsit per garantir.

4) Maximum Bit Rate: indica la quantitat màxima de bits per segon permesa (de pic) per a aquest túnel IP-CAN. S'usa solament per a serveis en temps real.

Així doncs, el mecanisme que l'EPS utilitza per a garantir la QoS està basat en aquests túnels IP-CAN. Un equip d'usuari pot tenir assignats diversos túnels IP-CAN simultanis dedicats amb diferents característiques de QoS.

> Com a curiositat, tan aviat com un terminal mòbil s'encén, el sistema li atorga automàticament una adreça IP i un túnel IP-CAN bidireccional sense cap garantia de QoS ni GBR (però sí amb un MBR fixat segons la subscripció de l'usuari), el qual el manté fins que s'apaga. Aquest túnel IP-CAN és de tipus *default* i és establert per la xarxa d'accés (gestionat per l'MME). A partir d'aquest moment el terminal o la xarxa pot establir túnels IP-CAN addicionals de tipus *dedicated* per a garantir la QoS dels serveis que s'invoquin.

Tant la PDN GW en sentit de baixada o *downlink* com l'equip d'usuari en sentit de pujada o *uplink* mapen els paquets IP entrants a uns filtres de paquets IP anomenats **fluxos de dades de servei** i una vegada identificat a quin flux de servei pertany es mapa al túnel IP-CAN assignat per a garantir la QoS.

Els **fluxos de dades de servei** es defineixen com un agregat de fluxos de paquets, cadascun caracteritzats per tenir idèntiques adreces IP tant d'origen com de destinació, i pels ports usats i el protocol.

El model de referència PCC

El PCC treballa a escala de fluxos de dades de serveis i proporciona funcions per al control de polítiques i de facturació (càrrecs associats) i també informa d'esdeveniments per als fluxos de dades de servei. La funcionalitat del PCC es resumeix en dues funcions principals:

1) Facturació sobre la base de fluxos: s'hi troben el control de càrrecs associats i el control de crèdit en línia.

2) Control de polítiques: s'hi troben control d'accés i control de QoS, entre altres.

Cada flux de dades de servei ha d'estar associat a una regla de PCC i pot estar subjecte a control de polítiques, a control de facturació o a tots dos alhora.

Una **regla PCC** (definida pel PCRF després de prendre la decisió de control d'admissió de la sol·licitud de recursos de servei via la interfície Rx en mode *push* o des de la interfície Gx en mode *pull*) està composta pels paràmetres següents:

- Nom de regla (identificador únic)
- Identificador de servei (valor enter que identifica un servei o component de servei)
- Filtre(s) de fluxos de dades de servei (fixa paràmetres de capçalera del paquet TCP/IP per a mapar el trànsit real en el servei)
- Precedència (ordre d'aplicació dels filtres)
- Estatus d'accés (obert o tancat)
- Paràmetres QoS (conté QCI, ARP i velocitat de bit per a pujada i baixada)
- Clau de facturació (és a dir, *rating group*) i altres paràmetres de facturació (usats per a facturació en línia i fora de línia)
- Clau de monitoratge

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

Una sessió IP-CAN es caracteritza per ser l'associació entre l'equip d'usuari i una xarxa IP. Una sessió IP-CAN pot incorporar una agrupació d'un o més túnels IP-CAN. Una sessió IP-CAN està present sempre que l'adreça IP estigui assignada a l'equip d'usuari i notificada a la xarxa IP.

1) Subcapa de processament de transport

La figura 10 mostra dos elements que conformarien 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. Aquí hem inclòs les dues entitats encarregades del control de càrrecs associats: l'OCS i l'OFCS. Finalment descriurem les tres entitats funcionals de processament de transport restants que apareixen en la figura 11, les quals seran agrupades en la xarxa troncal.

Reflexió

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

a) Funció d'Aplicació de Polítiques i Càrrecs Associats (PCEF): en anglès es tradueix com Policy and Charging Enforcement Function (PCEF) i aquesta entitat funcional s'encarrega d'aplicar les polítiques que defineixen les regles PCC que un o més PCRF li indiquin per mitjà de punt de referència Gx. Això significa que defineix els túnels IP-CAN, limita la velocitat de bit que indica el *bearer* (GBR i MBR) i fa filtratge de paquets (inspecció de paquets IP d'entrada des de les xarxes externes) segons els filtres definits per les regles PCC actives per a mapar el trànsit als IP-CAN *bearers* adequats per a la QoS requerida. A més mapa els IP-CAN *bearers* a paràmetres de QoS concrets de la xarxa troncal o EPC (DiffServ, bàsicament).

La localització del PCEF en l'arquitectura EPS és en el PDN GW. En el cas d'una xarxa GPRS, el PCEF es localitzaria en la GGSN; en el cas d'una xarxa Wi-Fi seria la PDG.

Passarel·les

Totes aquestes passarel·les amb diferents noms guarden una similitud entre si. Són passarel·les frontereres de la xarxa d'accés amb altres xarxes externes basades en paquets i administrades per altres operadors. Són les entitats funcionals encarregades d'interconnectar cadascuna de les xarxes d'accés ràdio amb altres xarxes externes terrestres.

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 túnels IP-CAN, etc.), incloent-hi funcions que afecten l'informe d'esdeveniments cap al PCRF per a notificar la modificació o l'establiment d'un túnel IP-CAN de l'usuari (mode *pull* de sol·licitud de recursos) o també inclouen funcions relacionades directament amb la facturació del servei en ús.

Per exemple, el PCEF s'ha d'assegurar 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 anomenades **regles PCC** són en realitat el resultat de les decisions a escala de sessió que l'entitat funcional PRCF (servidor de polítiques en la subcapa de Control de Transport) pren una vegada ha avaluat informació de disponibilitat de la xarxa i polítiques de l'operador de la xarxa mateixa. És una decisió de control d'admissió a escala de fluxos de dades de servei (la descripció del qual és rebuda des del punt de referència Rx) i les regles PCC són el resultat d'aquesta.

Així doncs, els fluxos de dades de servei (associats a cada regla PCC en forma de filtres) també poden estar subjectes a un control de facturació si el servei al qual va associat així ho requereix. Així doncs, el PCEF ha d'estar al corrent d'aquest control també. De fet, el 3GPP ha definit dues interfícies dedicades amb les entitats funcionals OCS i OFCS amb uns punts de referència anomenats *Gy* i *Gz*, respectivament.

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

Per al cas de tenir un flux de dades de servei que està subjecte a tots dos controls de polítiques de QoS i de facturació, el PCEF solament permet el pas d'aquest flux de dades a través d'ell si i solament si es donen les condicions de control de polítiques i facturació correctes. És a dir, que l'accés corresponent (a escala de tallafoc) hagi estat habilitat i, en el cas de facturació en línia, l'OCS hagi autoritzat el crèdit per al servei associat als fluxos.

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

b) Funció d'Associació de Túnels i Informe d'Esdeveniments (BBERF): en anglès es diu *Bearer Binding and Event Reporting Function* i aquesta entitat funcional està mapada sobre l'SGW en l'arquitectura EPS i està interconnectada amb el PCRF via el punt de referència Gxx.

Tal com les sigles indiquen, aquest element també és capaç de mapar el trànsit als túnels IP-CAN. Us preguntareu per a què el BBREF fa aquesta funció si el PCEF ja ho fa com a extrem de túnel. Resulta que 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 d'informe d'esdeveniments en el PRCF també pot estar associada a aquesta entitat funcional amb les mateixes condicions esmentades pel que fa al PCEF.

Amb això és possible que en una xarxa d'accés mòbil no existeixi el BBERF ni la interfície Gxx.

c) Sistema de Facturació en línia (OCS): l'Online Charging System du a terme la gestió del crèdit per a la facturació de prepagament. Dins d'aquesta entitat funcional hi ha 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 per gastar en un mes. Si se supera tal límit, la velocitat màxima de descàrrega baixa (velocitat del túnel IP-CAN de tipus *default*).

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 a 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 postal o electrònic.

e) Processament de Funcionalitats de Recursos Multimèdia (MRFP): aquesta funcionalitat és equivalent a la descrita en el model de l'ETSI-TISPAN amb el mateix nom. (Vegeu el punt "Entitats funcionals de processament de transport en la xarxa troncal".)

f) Funcionalitat de Passarel·la de Mitjans d'IMS (IMS-MGF): aquesta funcionalitat és equivalent a la descrita en el model de l'ETSI-TISPAN amb el nom T-MGF. (Vegeu el punt "Entitats funcionals de processament de transport en la xarxa troncal".)

g) Passarel·la de Transició (TrGW): la Transition Gateway (TrGW) té funcions molt similars a la funcionalitat de l'I-BGF de l'ETSI-TISPAN (explicada en el punt "Entitats funcionals de processament de transport en la xarxa troncal"). Està interconnectada amb la capa de Control de Servei via una interfície anomenada *Ix*.

2) Subcapa de control de transport

En el model del 3GPP, aquesta subcapa està formada per dos elements: SPR i PCRF.

a) Repositori de Perfils de Subscripció (SPR): aquesta entitat funcional anomenada en anglès *Subscriber Profile Repository* emmagatzema els perfils d'usuari a escala de capa de transport (entre altres paràmetres el GBR i l'MBR associats a aquest usuari i la llista de serveis permesos) i està interconnectat amb el PCRF per mitjà d'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 regles PCC corresponents.

Nota

Fixeu-vos que si ho comparem amb els blocs dedicats a l'adhesió dels terminals a la xarxa d'accés de la ITU-T (anomenat *NACF*) i de l'ETSI-TISPAN (NASS), l'SPR compliria solament la funció d'interconnexió entre la TLM-FE i la PD-FE dins del RACF (via la interfície Ru) o entre el CLF i l'A-RACF dins del RACS (via la interfície e4).

b) Funció de Regles de Polítiques i Facturació (PCRF): en anglès respon a les sigles de Policy and Charging Rules Function i és l'element que pren les decisions quant a control d'admissió sobre les sol·licituds de recursos rebuts des de l'AF (Application Functions) a través del 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 al 3GPP l'AF 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. El 3GPP preveu que si el servei està basat en IMS l'AF és el P-CSCF, i si no està basat en IMS és una entitat equivalent.

Desglossant pas per pas les tasques que fa el PCRF amb una miqueta més de detall, s'obté la llista següent:

- **Autorització de la sol·licitud de recursos de servei mateixa i control d'admissió de subscripció**: en rebre una sol·licitud de recursos de servei via la 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 de l'usuari que ha sol·licitat. En cas que no es compleixi solament una d'aquestes dues comprovacions la sessió es rebutja.

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

- **Informe d'esdeveniments**: el PCRF pot, per exemple, reportar esdeveniments ocorreguts en la capa de Transport (estatus de túnels IP-CAN o sessi-

ons IP-CAN) o esdeveniments de facturació a l'AF si aquest ho ha sol·licitat expressament via la interfície Rx.

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

Reflexió

Després de veure la descripció del PCRF, podem treure la conclusió que en comparar-ho amb els elements de control d'Admissió i Recursos equivalents per a la ITU-T (RACF) i l'ETSI-TISPAN (RACS), tots compleixen en general funcions molt similars i que en l'única cosa que es diferencien és pel desglossament intern en entitats funcionals i com les funcions es reparteixen entre elles.

1.3. Capa de Servei

En la capa de servei no hi ha gaires divergències entre entitats d'estandardització, ja que es tracta d'una capa que no té relació amb cap tecnologia en particular, com sí ocorria en la capa de transport.

No obstant això, cada entitat d'estandardització ofereix el seu punt de vista i la seva perspectiva particular respecte a aquesta capa:

- 3GPP: com a entitat creadora de l'IMS, centra la seva arquitectura de control de servei en aquesta tecnologia.

- ITU-T: en la seva recomanació Functional Requirements and Arquitecture (FRA), especifica un model funcional genèric del pla de serveis que pretén ser independent dels serveis i protocols emprats. D'aquesta manera, aquest model es pot concretar en models més específics, coneguts com a **components de serveis** (dels quals s'extreu el component IMS, el d'emulació XTC/XDSI i el d'IPTV).

- ETSI-TISPAN: presenta un enfocament orientat a **subsistemes**. Cada subsistema té el seu propi model d'arquitectura i s'especifica independentment dels altres subsistemes. D'aquesta manera es poden afegir amb el temps nous subsistemes que cobreixin noves demandes i classes de servei, i permet la importació i adaptació de subsistemes ja definits, com és el cas d'IMS. A part del d'IMS, el model d'ETSI-TISPAN defineix dos subsistemes més: el d'emulació XTC/XDSI i el d'IPTV.

De tots aquests components (ITU-T) i subsistemes (ETSI-TISPAN) n'hi ha un que volem destacar: el component, subsistema o nucli IMS.

El **nucli IMS** aguanta la provisió de qualsevol servei multimèdia existent avui i també els futurs que estan per arribar. IMS pot suportar la provisió de serveis equivalents a les xarxes XTC/XDSI i fins i tot el servei IPTV.

Quan es defineix un servei multimèdia en xarxes NGN se sol distingir entre que estigui basat en IMS (participació de nucli IMS amb senyalització SIP) o que no ho estigui (amb un component o subsistema dedicat, el qual té els seus propis blocs de control de servei i el seu propi protocol de senyalització de servei). Això ocorre ja amb altres components o subsistemes separats que l'especificació de xarxes NGN preveu, com el d'emulació XTC/XDSI i el d'IPTV. Així, les entitats d'estandardització de les xarxes NGN a escala de servei deixen la porta oberta a l'especificació d'aquests serveis sense que hagin d'estar basats en IMS.

Així doncs, ens centrarem exclusivament en el nucli IMS com a plataforma de provisió i habilitació de serveis multimèdia.

Com les especificacions del component o subsistema IMS de la ITU-T i de l'ETSI-TISPAN estan basades en l'estàndard del 3GPP, intentarem donar una descripció més uniforme d'aquest subsistema posant l'accent en les diferències entre especificacions d'una o una altra entitat d'estandardització prenent com a base la del 3GPP.

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:

- Emmagatzemament de perfils d'usuari a escala 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 està associat a un operador, del qual els usuaris són subscriptors d'una llista de serveis, representats pels AS (Application Servers) als quals accedeixen per mitjà del nucli IMS.

Els Servidors d'Aplicacions (*Application Servers*, AS) són l'element central de l'arquitectura de serveis d'NGN/IMS. La seva funció és la d'allotjar i executar els serveis de valor afegit de la plataforma (com són la presència i *push to talk* sobre entorns mòbils), i també 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 a interactuar amb IMS a un nivell superior. No obstant això, hi recau la provisió de la majoria dels serveis que aporten valor a 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.

1.3.1. Components del nucli IMS

Seguint la línia d'apartats anteriors farem un repàs per les tres especificacions que estem analitzant: 3GPP, ETSI-TISPAN i ITU-T. En les figures següents es mostren les tres arquitectures funcionals per a cadascuna d'aquestes. No obstant això, atesa la gran similitud entre elles, donarem una única explicació descriptiva, la del model 3GPP, i esmentarem les diferències que hi pugui haver amb les dues restants: ITU-T i ETSI-TISPAN.

Vegeu també

Un resum conjunt de les interfícies que componen els tres models d'IMS es pot trobar en la taula 10 de l'annex.

Figura 13. Arquitectura de referència del component IMS per a ITU-T

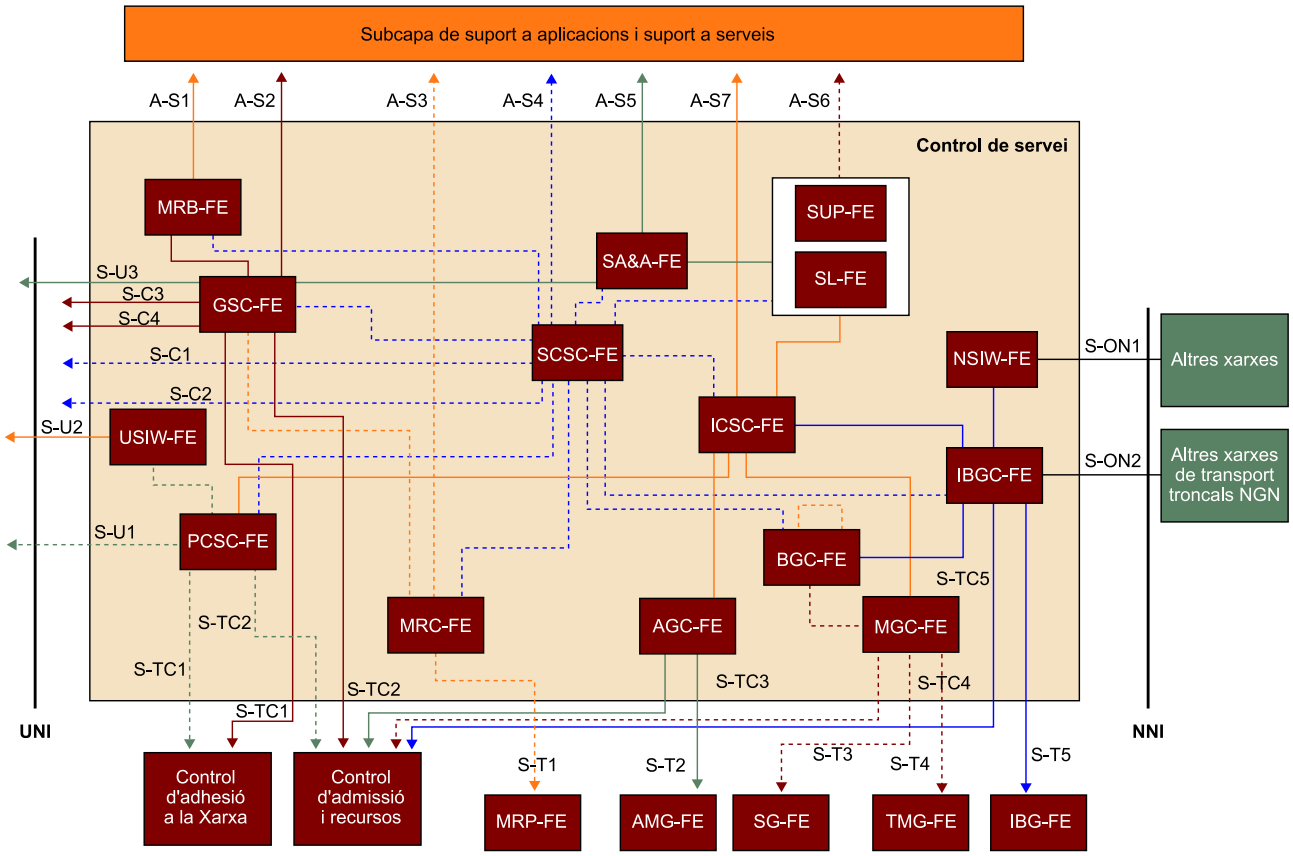


Figura 14. Arquitectura de referència per al subsistema IMS per a l'ETSI-TISPAN

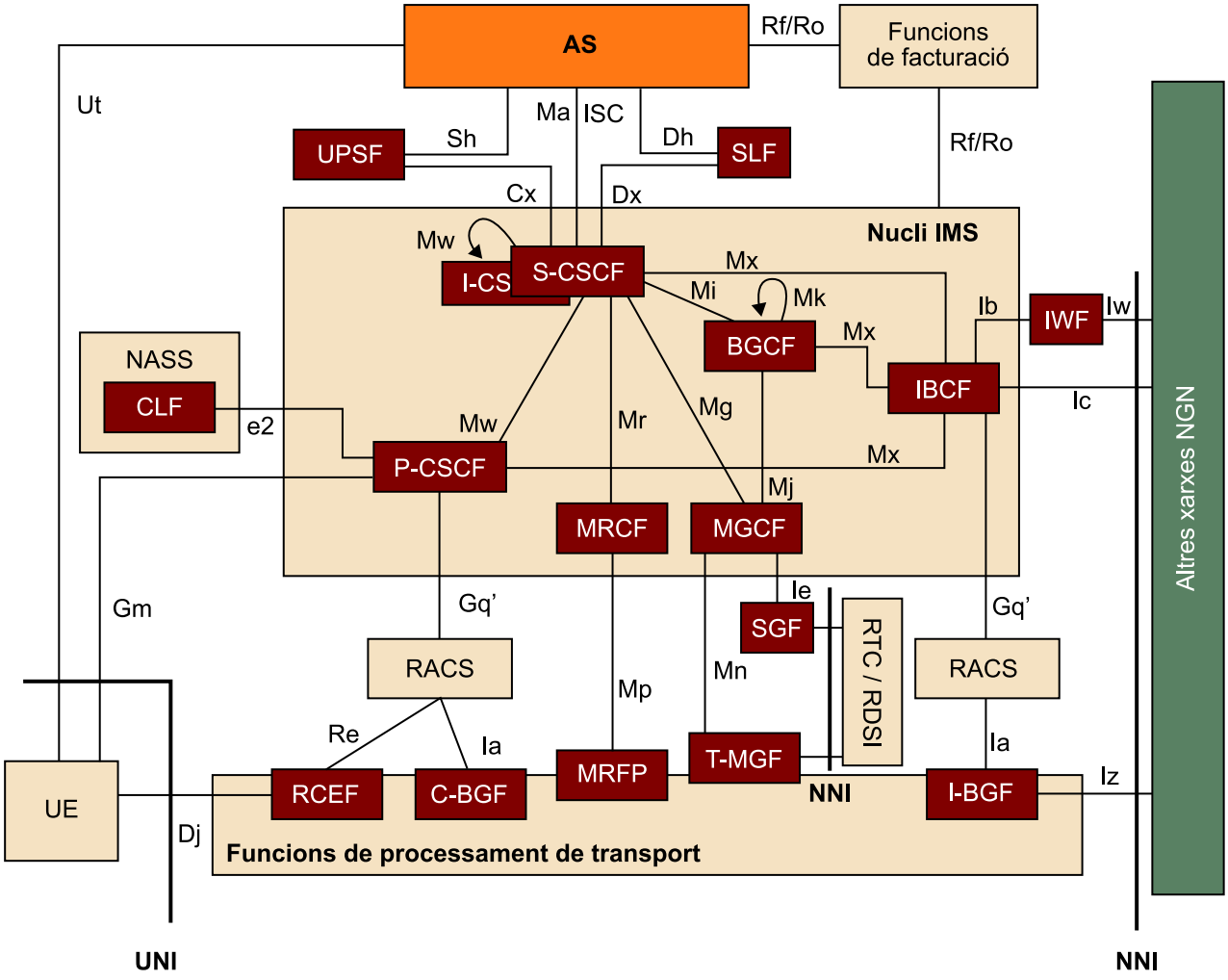
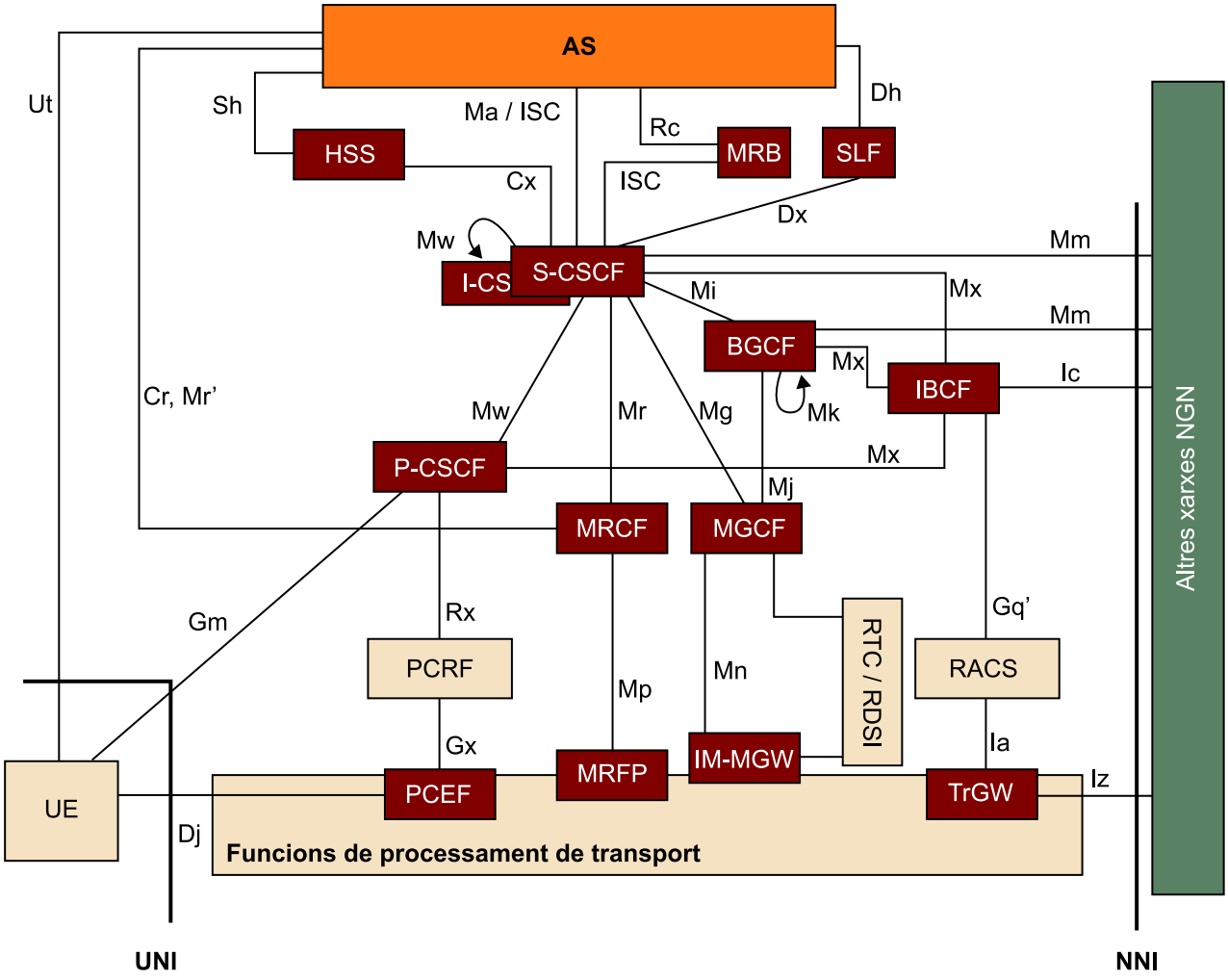


Figura 15. Arquitectura de referència d'IMS per a 3GPP



Tant en la figura 14 com en la figura 15, les entitats S-CSCF i I-CSCF s'han mostrat juntes per simplificar el diagrama, però en realitat són dues entitats completament independents. Totes dues estan interconnectades a través de la interfície Mw. Però a més, cada interfície que surt de l'S-CSCF ha de ser replicada també per l'I-CSCF (exceptuant el Mr i Mi, que solament estan associats a l'S-CSCF). La interfície que connecta l'S-CSCF amb l'AS és l'ICS i la que connecta l'I-CSCF amb l'AS és el Ma.

El protocol utilitzat en l'establiment de sessions de serveis multimèdia basats en IMS és el protocol SIP (Session Initiation Protocol) definit per l'IETF en l'RFC 3261. No obstant això, el protocol SIP requereix certes extensions que van més enllà de l'especificació de l'IETF per a ser usat en un entorn IMS.

Vegeu també

Les extensions del protocol SIP estan descrites en el subapartat "Extensions per a IMS".

Funció de Control de Sessió de Trucada - Proxy (P-CSCF)

El P-CSCF és el primer punt de contacte dins d'IMS per als usuaris adherits a una xarxa d'accés i és per això que 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 en el qual hi hagi una frontera de domini administratiu (és a dir, tant en la interfície UNI, on equip d'usuari i domini IMS s'uneixen, com en la interfície NNI, on dos dominis IMS s'uneixen).

Session Border Controller o SBC

Un Session Border Controller o 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. Aquests problemes són la **seguretat** on es fa

control d'admissió de trucada a les fronteres de la xarxa per a garantir QoS del trànsit que entra i surt, s'evita l'abús en l'ús del servei i es fan tasques de protecció de la privadesa de l'operador i l'usuari. També comprenen funcions per a solucionar els problemes de l'ús de protocols com SIP en presència d'un **tallafoc o NAT** (SIP ALG o Application Level Agreement) o funcions de **monitoratge regulatòries** com la intercepció de trànsit per llei (*lawful interception*), **facturació** i **monitoratge del servei**. Un SBC pot tenir entitats separades per a senyalització i mitjans.

Entre les funcions que ha de fer el P-CSCF hi ha les següents:

a) En el procés de registre de l'usuari, reenviar la petició de SIP REGISTER des de l'UE (rebuda via una interfície anomenada *Gm*) al punt d'entrada del domini local. Mirant la part que descriu el domini en el SIP URI inclòs en la capçalera SIP sap a quin I-CSCF (servidor de control de sessió de trucada de tipus *Interrogating*) ha de reenviar el SIP REGISTER.

Nota

En el 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 via l'element corresponent de control fronterer o SBC de la xarxa visitada, que en aquest cas és l'entitat IBCF (usant una interfície anomenada *Mx*).

b) Emmagatzemar informació del registre, com la informació de contacte de l'UE (IP assignada), l'adreça de l'S-CSCF (servidor de control de sessió de trucada de tipus *Serving*) i les sessions en actiu.

c) Redirigir els missatges SIP des de l'UE a l'S-CSCF via una interfície anomenada *Mw*, i viceversa.

d) Fer la compressió i descompressió dels missatges SIP que provenen de l'UE.

L'UE, en enviar els seus missatges SIP per la interfície de senyalització d'IMS anomenada *Gm*, posarà sempre l'adreça IP del P-CSCF com a destinació, ja que aquest fa de servidor intermediari per a totes les transaccions SIP.

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

Quan el P-CSCF rep un intent de trucada (SIP INVITE) (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 la mateixa llista independentment del país gràcies a acords internacionals, com el número 112).

f) L'associació entre el P-CSC-FE i cada UE és sempre segura (s'usa IPSec). Per tant, el P-CSCF és responsable del manteniment de les Associacions de Seguretat (SA-Security Associations) i l'aplicació de la protecció de confidencialitat i integritat de senyalització SIP.

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 què hi ha dues claus: IK o Integrity Key i CK o Cipher Key, que haurà d'usar el P-CSCF per a negociar associacions de seguretat IPSec. Així pot aplicar protecció de confidencialitat i integritat per a la resta de la senyalització SIP.

g) Participa en l'autorització i la gestió de qualitat de servei dels recursos multimèdia (es comunica amb la subcapa de Control de Transport per a sol·licitar recursos via la interfície Rx). És normal que en ser un SBC hagi de consultar elements de gestió de recursos en la capa de transport.

El P-CSCF rep totes les peticions SIP que fan els UE en el seu domini, independentment de la destinació final d'aquestes, i les reenvia a un I-CSCF o un S-CSCF del seu mateix domini perquè en continuï el processament. Així mateix, rep totes les peticions SIP destinades als UE del seu domini. El P-CSCF ha de mantenir informació de registre i d'estat.

Dins de la xarxa d'un operador hi pot haver diversos P-CSCF de manera concurrent.

Diferències que cal destacar per al model de l'ETSI-TISPAN respecte al 3GPP

- La interfície e2 apareix per a connectar-se amb el NASS.
  El P-CSCF pot obtenir l'adreça de l'element que gestiona els recursos en la capa de transport gràcies a la informació de localització de l'usuari proporcionada via la interfície e2. En el model del 3GPP no s'usa perquè està basat en túnels IP-CAN.

- La interfície Rx es passa a anomenar *Gq'* i es connecta al RACS en comptes del PCRF.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- El nom d'aquesta entitat (P-CSCF) canvia a P-CSC-FE.

- La interfície Gm es passa a anomenar *S-U1* i també està basada en SIP. Cal destacar també que la ITU-T inclou una entitat anomenada User Signalling Interworking Functional Entity (USIW-FE) que implementa una interfície anomenada *S-U2* amb l'equip d'usuari (UE) i una altra interfície amb el P-CSC-FE (podria ser equivalent al Gm o S-U1) i la seva funció és adaptar o traduir la senyalització de tots aquells terminals d'usuari que no suporten el protocol SIP d'IMS.

- La interfície e2 (ETSI-TISPAN) es passa a anomenar *S-TC1* amb la mateixa funció que aquesta.

- La interfície Rx es passa a anomenar *S-TC2* (o *Rs*) i es connecta al bloc de control d'admissió i recursos de la subcapa de Control de Transport (RACF) en comptes del PCRF.

Funció de Control de Sessió de Trucada - Interrogating (I-CSCF)

I-CSCF és el punt de contacte dins de la xarxa de l'operador per a totes les connexions destinades a un subscriptor d'aquest operador de xarxa.

Vegem les quatre funcions assignades a l'I-CSCF:

- Obtenir el nom del salt següent (S-CSCF o AS) des de l'HSS via la interfície Cx.

- Assignar un S-CSCF en funció de les capacitats rebudes des de l'HSS. L'assignació del S-CSCF tindrà lloc quan un usuari es registra a la xarxa. També s'assigna un S-CSCF quan rep una petició SIP mentre no està registrat a la xarxa, però en canvi té serveis relatius a un estat de no registrat (per exemple, missatges de veu).

- Encaminar les peticions SIP d'entrada en relació amb un S-CSCF assignat (via la interfície Mw) o amb un AS (via una interfície anomenada *Ma*).

- Proporcionar funcionalitat THIG (Topology Hiding Inter-network Gateway) de manera opcional. Un altre operador que vulgui enviar senyalització SIP cap al nostre domini 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. L'I-CSCF pot actuar com un element SBC solament a escala de senyalització SIP per a la interfície entre dos dominis o xarxes NGN (NNI). No obstant això, no preveu gestió de recursos amb la capa de transport.

Nota

En el Release actual del 3GPP l'IBCF ha substituït aquesta funcionalitat de THIG a l'I-CSCF. No obstant això, es poden trobar encara nombrosos documents que descriuen fluxos de crides IMS en les quals l'I-CSCF és l'element visible entre diferents dominis IMS.

En el cas de tramitació d'un registre d'usuari, l'I-CSCF contacta amb la base de dades de subscriptors del domini o HSS (via una interfície anomenada *Cx*) per a obtenir l'adreça de l'S-CSCF, i llavors reenvia el missatge SIP a aquest S-CSCF via la interfície dedicada a tal fi, anomenada *Mw*. Aquesta operació es fa de la manera següent: l'I-CSCF contacta amb l'HSS per fer el registre, aquest autoritza aquest registre i, per mitjà de la interfície Cx, basada en el protocol Diameter, l'I-CSCF sol·licita i selecciona en una llista de l'HSS el primer servidor que satisfà les capacitats requerides.

Apareix una interfície anomenada *Mm*, la qual, segons el 3GPP, és una interfície IP entre els CSCF/IBCF i altres xarxes IP, per exemple, per a rebre una petició de sessió des d'un altre servidor SIP o terminal.

Reflexió

L'estàndard del 3GPP no dóna gaire més informació sobre la inclusió d'aquesta interfície Mm. Aquesta interfície està basada en SIP i serveix per a comunicar-se amb altres servidors SIP externs.

Per a la recepció dels missatges destinats a l'I-CSCF s'han d'habilitar ports específics. L'I-CSCF no manté cap tipus d'informació de registre o estat. Hi pot haver múltiples I-CSCF concurrentment en la xarxa d'un operador.

Diferències que cal destacar per al model de l'ETSI-TISPAN respecte al 3GPP

- L'entitat HSS es passa a anomenar User Profile Subscription Function (UPSF).
- La interfície Mm no existeix.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- El nom d'aquesta entitat (I-CSCF) canvia a I-CSC-FE.
- L'entitat HSS es passa a anomenar Service User Profile Functional Entity (SUP-FE).
- La interfície Mm no existeix.

Funció de Control de Sessió de Trucada - Serving (S-CSCF)

L'S-CSCF és el punt central del nucli IMS i el domini corresponent, i és responsable de mantenir el procés de registre, prendre decisions d'encaminament i manteniment de l'estat de sessió SIP, i l'emmagatzemament dels perfils de servei per a usuaris activament registrats.

Quan un usuari envia una petició de registre (SIP REGISTER) aquesta s'envia a l'S-CSCF (des de l'I-CSCF via la interfície Mw), el qual descarrega les dades d'autenticació des de l'HSS (via la interfície Cx). Després d'aquest procediment de registre l'usuari pot iniciar i rebre serveis IMS. Finalment, l'S-CSCF descarrega de l'HSS un perfil de servei de l'usuari com a part del procés de registre.

Aquest perfil inclou les iFC o initial Filter Criteria, les quals s'usen per a decidir quins servidors d'aplicacions (AS) estan habilitats quan un usuari envia una petició SIP. 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).

Per al trànsit SIP entrant en el domini cap a un equip d'usuari (UE), l'S-CSCF encamina les sessions al P-CSCF, l'adreça del qual es va emmagatzemar durant el registre. En el cas del trànsit sortint, l'S-CSCF pregunta al DNS/ENUM per a determinar la ruta de la trucada. És a dir, encamina el missatge cap a l'IBCF (element fronterer entre dominis IMS), que el connecta amb el domini destinació. L'S-CSCF ha de ser capaç d'encaminar basant-se en formats SIP URI o Tel URI. En aquest últim cas, el missatge SIP s'encaminarà cap a una entitat que gestiona aquests tipus d'URI de destinació, la Breakout Gateway Control Function o BGCF. Aquest, en veure que és de tipus Tel URI, el reenviarà a una Media Gateway Control Function o MGCF (passarel·la de control cap a XTC/XDSI) de la seva elecció.

Cal definir ports específics per a la recepció de missatges en l'S-CSCF. L'S-CSCF ha de mantenir tant l'estat del registre com el de la sessió. Hi pot haver múltiples S-CSCF concurrentment en la xarxa d'un operador.

Diferències que cal destacar per al model de l'ETSI-TISPAN respecte al 3GPP

- La interfície Mm desapareix.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- El nom d'aquesta entitat (S-CSCF) canvia a S-CSC-FE.

Funció de Control de Sessió de Trucada - Emergency (E-CSCF) i Funció d'Obtenció de Localització (LRF)

Aquestes entitats no han estat incloses en la figura 15 per a no complicar més l'arquitectura però hem cregut convenient incloure'n la descripció, ja que, d'acord amb la normativa de la majoria dels països, tot operador de telecomunicacions ha de proporcionar comunicacions d'emergència i l'E-CSCF s'ha definit per a tal fi, juntament amb l'LRF, que realitza funcions d'obtenció de localització auxiliar.

L'E-CSCF pot formar part d'un mòdul únic CSCF o funcionar com una aplicació independent. En aquest últim cas, es relaciona només amb el P-CSCF via la interfície Mw basada en senyalització SIP.

El funcionament d'aquesta entitat és el següent:

- Quan el P-CSCF rep un intent de trucada (SIP INVITE) el número de telèfon (Tel URI) es compara amb una llista preconfigurada de telèfons d'emergència.

- Si hi ha una coincidència, la trucada s'encamina amb màxima prioritat (no s'aplica control de càrrecs o facturació) i s'envia a l'E-CSCF perquè la processi.

- L'E-CSCF comprova si hi ha informació de localització (capçalera PANI, P Access Network Info) en el missatge. Si no n'hi ha, la tracta d'obtenir de l'HSS (si escau, amb intervenció del node SLF).

- A continuació, si s'ha configurat un node LRF, obté d'aquest el nombre d'un centre d'emergència (Public Safety Answering Point o PSAP) adequat a la informació de localització proporcionada, i hi redirigeix la trucada (amb la intervenció d'una passarel·la MGC en cas de ser necessari).

Funció de Control de Passarel·la de Sortida (BGCF)

La BGCF (Breakout Gateway Control Function) s'empra per a seleccionar el salt següent (passarel·la capaç d'encaminar) d'una petició SIP (rebuda des d'un I/S-CSCF via una interfície dedicada anomenada *Mi*) quan aquesta està destinada a un àlies que no pot ser traduït com un SIP URI (per exemple, és el cas

d'un Tel URI). La selecció d'aquesta passarel·la es fa sobre la base del número de telèfon de l'usuari a qui s'ha trucat, i si és possible, també del que truca. L'àlies de destinació pot ser especificat per un equip d'usuari (UE) o un servidor d'aplicacions (AS).

En el cas de trucades cap a l'XTC/XDSI (l'àlies de destinació és un Tel URI), la BGCF reenviaria la senyalització de sessió SIP a un Media Gateway Control Function (MGCF) que ell mateix selecciona via una interfície anomenada *Mj* (si està en el mateix domini) o una interfície anomenada *Mk* (si està en un altre domini), mentre que si es tracta de trucades cap a altres dominis IMS, s'enviarien via la interfície anomenada *Mx* a una Interconnection Border Control Function o IBCF.

La BGCF implementa altres capacitats addicionals, com redundància (possibilitat de seleccionar una altra BGCF en cas que aquest fallés) o encaminament basat en minimització de cost (cap a la passarel·la més propera a la xarxa final).

Diferències que cal destacar per al model de l'ETSI-TISPAN respecte al 3GPP

- La interfície Mx s'usa també per a encaminar trucades cap a xarxes H.323 o altres protocols a un IBCF/IWF que la gestionaria.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- El nom d'aquesta entitat (BGCF) canvia a BGC-FE.

- La interfície que comunica la BGC-FE amb IBGC-FE s'usa també per a encaminar trucades cap a xarxes H.323 o altres protocols a un IBC-FE / NSIW-FE (Network Signalling Interworking Functional Entity) que la gestionaria.

Funció de Control d'Interconnexió Fronterera (IBCF)

L'element funcional IBCF (Interconnection Border Control Function) fa la tasca principal d'interconnectar nuclis IMS pertanyents a diferents operadores (és un element de tipus SBC). Aquest bloc fa un traspàs de la senyalització SIP que rep des dels CSCF a través de les interfícies Mx cap a una altra entitat IBCF pertanyent a l'altre domini. Aquesta IBCF estarà connectada amb la IBCF de l'operador remot a través d'una interfície anomenada *Ici*, que està basada en SIP.

Pot fer tasques de THIG o ocultació en les capçaleres SIP d'informació que puguin donar pistes sobre la topologia del nucli IMS (reescriptura del camp *Record Route:* de la capçalera SIP). Per mitjà de la interfície Ici passarà tota la senyalització SIP d'establiment de sessió entre els dos nuclis IMS.

La funcionalitat de la IBCF abasta també el següent:

- Du a terme funcions de control fronterer (SBC) en la capa de transport via la interfície de control Ix amb l'entitat TrGW (Transition Gateway, en la subcapa de processament de transport). Aquesta aplica sobre el trànsit d'usuari les traduccions de NAT, control d'accés o conversions d'IMS ALG (IPv4/IPv6) que li indica per a aquesta interfície. Hi ha una interfície anomenada *Izi* (en la subcapa de processament de transport) que interconnecta dos TrGW de diferent domini per a transferir-se fluxos de mitjans entre ells.

- Fa funcions d'IMS ALG (Application Level Gateway) per a la traducció d'IP (a escala de capçalera SIP com SDP) entre sessions IMS basades en IPv4 a sessions IMS basades en IPv6 i viceversa.

- Explora la informació de senyalització basada en font/destinació, més enllà de la ja feta en cada subsistema.

Diferències que cal destacar per al model de l'ETSI-TISPAN respecte al 3GPP

- La IBCF controla la I-BGF de la subcapa de Processament de Transport via la interfície que el connecta amb la subcapa de Control de Transport representat per un RACS (Gq').

- La IBCF insereix la IWF en la senyalització de la ruta quan hi ha necessitat d'interacció entre perfils SIP diferents o protocols diferents (per exemple, SIP i H.323 o SIP estàndard d'IETF i SIP amb extensions IMS). En aquest cas, l'IWF actua com un punt d'entrada a la xarxa IMS.

- La IBCF es comunica amb una altra IBCF homòloga per mitjà d'una interfície anomenada *Ic* (la Ici, que hem esmentat abans, és una implementació especial de la Ic) per a intercanviar-se senyalització SIP.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- El nom d'aquesta entitat (IBCF) canvia a Interconnection Border GW Control - Functional Entity (IBGC-FE).

- A l'hora de fer la sol·licitud de reserva de recursos, l'IBCF-FE es comunica amb la RACF via la interfície Rs, i aquest al seu torn selecciona i controla la IBG-FE via la interfície Rw.

Gestor de Recursos de Mitjans (MRB)

El Media Resource Broker (MRB) gestiona un grup heterogeni de recursos MRF per compartir entre un grup heterogeni de servidors d'aplicacions (AS). Assigna recursos del servidor de mitjans a les trucades a petició dels AS. Per a això empra mètodes i algorismes que l'ajuden a determinar com cal fer aquesta assignació; i recopila informació sobre l'operativitat o no d'un determinat servidor de mitjans, o el seu nivell de càrrega en cas que estigui operatiu, a fi de seleccionar el més adequat a cada moment. Té una interfície anomenada *Rc* amb l'AS i una interfície anomenada *ISC* (IMS Service Control) amb l'S-CSCF.

Diferències que cal destacar per al model de l'ETSI-TISPAN respecte al 3GPP

- L'entitat equivalent a l'MRB no existeix en aquest model de referència.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- El nom d'aquesta entitat (MRB) canvia a Media Resource Broker Functional Entity (MRB-FE).
- La interfície Rc es passa a anomenar *A-S1*.

Encara que està localitzat en les funcions de control de serveis, l'MRB-FE pot ser vist com a part de les funcions de la subcapa de Suport a Serveis i Suport d'Aplicacions (vegeu la figura 1).

Control de Funcions de Recursos Multimèdia (MRFC)

El Multimedia Resource Function Control (MRFC) és un node de senyalització que actua davant l'S-CSCF com a Agent d'Usuari SIP (terminal SIP), i que controla l'MRFP (Multimedia Resource Function Processor) per mitjà d'una interfície anomenada *Mp*. Interpreta les demandes procedents del servidor d'aplicació (AS) via l'S-CSCF (interfície Mr) i controla l'MRFP consistentment per a oferir els serveis que ofereix aquest: IVR, anuncis, etc.

Té altres interfícies que el connecten directament amb l'AS perquè aquestes accedeixin als recursos multimèdia sense haver de passar a través de l'S-CSCF (via l'MRB). La interfície anomenada *Cr* és utilitzada per l'AS per a controlar els mitjans i l'Mr' (basada en SIP) per a controlar la sessió en l'ús d'aquests recursos.

Diferències que cal destacar per al model de l'ETSI-TISPAN respecte al 3GPP

- Les interfícies Cr i Mr' desapareixen.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- El nom d'aquesta entitat (MRFC) canvia a Multimedia Resource Control Functional Entity (MRC-FE).
- La interfície d'interacció amb l'MRP-FE és l'S-T1.

Funció de Control de Passarel·la de Mitjans (MGCF)

La Media Gateway Control Function (MGCF) permet controlar un IMS-MGF (en la subcapa de processament de transport) per mitjà de la interfície Mn. També està directament connectada a escala de traducció de la missatgeria SIP d'establiment de sessió a senyalització SS7/ISUP amb la xarxa XTC/XDSI i viceversa.

Aquest control inclou l'assignació i alliberament de recursos de la passarel·la de mitjans, i també la modificació de tals recursos. L'MGCF es comunica amb el CSCF via el BGCF (Breakout Gateway Control Function) a través de la interfície Mj d'una banda i les xarxes de commutació de circuits per una altra (a través de les entitats de la subcapa de Processament de Transport).

Per a trucades entrants des de les xarxes de commutació de circuits, l'MGCF reenvia els missatges SIP equivalents a l'S-CSCF via una interfície anomenada *Mg*. Amb això, depenent de l'adreça de la trucada utilitza la interfície Mj (trucada sortint cap a XTC/XDSI) o l'Mg (trucada entrant cap a IMS).

Per al cas del 3GPP, l'MGCF apareix com a element dins de l'arquitectura d'IMS mateixa i interconnecta les xarxes basades en circuits.

Diferències que cal destacar per al model de l'ETSI-TISPAN respecte al 3GPP

- L'MGCF està interconnectat amb la Signalling Gateway Function o SGF (en la subcapa de Processament de Transport) per a permetre la interoperabilitat entre SIP i senyalització SS7 via una interfície anomenada *Ie*.

- El T-MGF és l'equivalent a l'IMS-MGF del 3GPP.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- Aquesta entitat (MGCF) es passa a anomenar Media Gateway Control Functional Entity (MGC-FE).

- La interfície de connexió entre l'MGC-FE i la TMG-FE (equivalent al T-MGF de l'ETSI) és la S-T4 en comptes de l'Mn.

- La interfície de connexió entre l'MGC-FE i l'SG-FE (equivalent a l'SGF de l'ETSI) és l'S-T3 en comptes de l'Ie.

- Les funcions que fa l'MGCF es poden mapar en l'entitat equivalent en el model de la ITU-T: la Network Signalling Interworking Functional Entity (NSIW-FE).

1.3.2. Components de magatzematge d'informació de subscripció

Tot seguit explicarem aquelles entitats especialitzades en l'emmagatzematge de subscripcions d'usuari i que són clau en la provisió de serveis. En total hi ha dues entitats i les interfícies involucrades estan resumides en la taula 11 de l'annex.

Servidor de Perfils Local (HSS)

En IMS, la base de dades HSS (Home Subscriber Server) manté la relació entre les diferents identitats (privada, pública...), emmagatzema els perfils d'usuari i els distribueix a les entitats de xarxa que controlen les sessions d'usuari (CSCF). Així mateix, és capaç de manejar diferents identificadors públics de servei (PSI) d'acord amb les especificacions de 3GPP.

Un **PSI (Public Service Identifier)** identifica tot allò que pugui ser receptor d'un missatge petició SIP i no és un usuari (per al qual s'usaria un IMPU). Llavors un PSI pot identificar qualsevol recurs d'un servei proveït per un servidor d'aplicació (AS), el qual pot ser el servei en si. Com a exemples de recursos, un PSI pot identificar un contingut en concret, una conferència ja predefinida, una habitació de xat, etc. Pot identificar també, per exemple, tot un grup d'usuaris.

El perfil d'usuari ha d'incloure 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 o àudio en una trucada), etc.

L'HSS participa en els procediments de registre, reregistre i desregistre d'usuari, registre implícit i maneig de sessió.

- L'usuari inicia un procés de registre (enviant un missatge SIP REGISTER) per informar la xarxa de la seva localització i capacitat per a participar en una sessió. Durant aquest procés se li assigna un S-CSCF (entitat de control de sessió de tipus *Serving*). 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, en les da-

des de configuració de l'HSS i en la informació d'usuari emmagatzemada. L'HSS permet el procés d'assignació d'S-CSCF i comunica a l'I-CSCF (entitat de control de sessió de tipus *Interrogating*) la identitat de l'S-CSCF en la 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.

- El reregistre és un procés periòdic iniciat per l'equip d'usuari per a recarregar el registre actual, o bé per a canviar l'estat de registre de l'equip d'usuari (UE). El paper de l'HSS en el reregistre és similar al del registre.

- Com a resultat del desregistre l'usuari deixa d'estar disponible amb la identitat pública (IMPU) desregistrada. Aquest pot ser sol·licitat per l'usuari, iniciat per la xarxa mitjançant una ordre en l'HSS o a causa d'un *time-out*.

- El procediment de registre implícit permet a un usuari registrar-se i desregistrar-se amb un conjunt d'identitats públiques (IMPU) identificant-ne només una en la petició de registre. L'usuari és informat de la resta de les seves identitats com a resposta a la petició, de manera que estiguin disponibles més endavant per al maneig de la sessió.

- L'HSS participa així mateix en l'establiment de la sessió quan l'usuari la inicia (enviant missatge SIP INVITE). L'HSS retorna a l'I-CSCF la identitat de l'S-CSCF assignat a un usuari en el cas que la identitat pública involucrada en la sessió hagi estat registrada amb anterioritat. Si no, l'HSS té serveis per a estat no registrat. Si la identitat pública no està registrada, i l'usuari no té serveis per a no registrats, l'HSS indica a l'I-CSCF que l'usuari no és assolible.

Juntament amb altres procediments de xarxa, l'HSS fa l'autenticació de l'usuari. L'HSS ha de suportar diversos models d'autenticació: IMS AKA, IETF HTTP Digest i IMS SSO.

- El procediment de l'IETF HTTP Digest és el següent: l'HSS genera un o més tests d'autenticació relatius al perfil d'usuari, i els inclou en la resposta a l'S-CSCF en el registre. L'S-CSCF envia aquest test a l'usuari. L'aplicació client genera la resposta adequada al missatge (i llavors pot ser necessari que l'usuari introdueixi la seva contrasenya). L'S-CSCF transfereix aquesta informació a l'HSS, que és llavors l'encarregada de verificar la resposta.

- L'autenticació IMS SSO permet que un usuari que ja tingui accés a la xarxa IP per mitjà de la infraestructura del nucli de l'operador no necessiti autenticar-se de nou per a accedir al domini IMS.

- Per la seva banda, IMS AKA permet l'autenticació mútua de l'usuari i la xarxa IMS, i ofereix plena protecció del trànsit de senyalització en tots dos sentits.

L'HSS també ha de suportar la subscripció i notificació de canvis: els servidors d'aplicacions es podran subscriure a notificacions per a l'actualització de dades transparents i no transparents per a un determinat usuari. L'operador podrà configurar una llista de servidors d'aplicacions autoritzats, i també polítiques de privadesa per als usuaris.

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 (PS) i commutació de circuits (CS), l'HSS conté funcionalitats de Home Location Register (HLR) i Authentication Center (AUC), tal com defineix el 3GPP.

El model del 3GPP diferencia entre dos dominis principals: el domini CS (Circuit Switched) són aquelles xarxes basades en commutació de circuits, com ara les xarxes XTC/XDSI o les xarxes de telefonia mòbil 2G. L'altre domini és el PS (Packet Switched), el qual està format pel nucli IMS mateix i l'EPS (Evolved Packet System). Tots dos dominis estan interconnectats per mitjà de passarel·les com la Media Gateway Control Function (MGCF).

Vegeu també

Tant l'Evolved Packet System com la Media Gateway Control Function (MGCF) han estat descrits anteriorment.

La funcionalitat d'HLR es requereix per a donar suport a entitats del domini de PS, com l'SGSN i el GGSN, i permeten que el subscriptor es connecti als serveis de la xarxa de commutació de paquets. De la mateixa manera, l'HLR també possibilita el suport a entitats de commutació de circuits, com els servidors MSC/MSC, que permeten l'accés del subscriptor a serveis del domini CS i la itinerància a xarxes GSM i UMTS.

Per la seva banda, l'AUC emmagatzema una clau secreta per a cada subscriptor mòbil, que s'usa per a generar dades dinàmiques de seguretat. Aquestes dades són utilitzades per a l'autenticació mútua de l'IMSI (International Mobile Subscriber Identity) i la xarxa, i també per a xifrar la comunicació ràdio entre l'UE i la xarxa.

Diferències que cal destacar per a model de l'ETSI-TISPAN respecte al 3GPP

- L'entitat HSS es passa a anomenar User Profile Subscription Function (UPSF).

- La UPSF es pot considerar com un subconjunt de l'HSS que exclou les funcionalitats d'HLR i AUC, i que emmagatzema únicament dades relacionades amb IMS.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- L'entitat Service User Profile Functional Entity (SUP-FE) es correspon amb la part de l'UPSF de TISPAN que gestiona els perfils d'usuari.

- L'entitat Service Autentication & Autorization Functional Entity (SAA-FE) es correspon amb la part de l'UPSF de TISPAN que gestiona l'autorització i l'autenticació.

Funció de Localització de Subscripció (SLF)

Quan hi ha més d'una HSS a la xarxa, cal la implementació d'una entitat SLF i dels seus punts de referència, anomenats *Dx* (connexió amb les entitats de control de sessió de trucada: CSCF) i Dh (connexió amb servidors d'aplicacions: AS).

En una xarxa en la qual s'han desplegat múltiples HSS independents, ni l'I-CSCF ni l'SCSCF coneixen en quina d'aquestes HSS es troba la informació que necessiten consultar. Per tant, han de contactar en primer lloc amb l'SLF.

L'SLF ha de proveir d'una funcionalitat d'encaminament que permeti que altres entitats descobreixin quin node HSS conté la informació de subscripció d'un determinat usuari (identitat pública o MSISDN), i atorgui a l'operador la flexibilitat de distribuir els seus usuaris lliurement entre diverses HSS.

Diferències que cal destacar per al model de l'ETSI-TISPAN respecte al 3GPP

- No hi ha diferències.

Diferències que cal destacar per al model de la ITU-T respecte al 3GPP

- El nom d'aquesta entitat canvia a Subscription Locator Functional Entity (SL-FE).

1.3.3. Altres components del model de l'ETSI-TISPAN de control de Servei

L'ETSI-TISPAN (vegeu la figura 14) incorpora una entitat funcional que no apareix en altres arquitectures de control de servei.

Funció d'Interoperabilitat (IWF): la Interworking Function es considera una entitat externa al nucli IMS en si. Es comunica amb el nucli via una interfície anomenada *Ib* per a garantir la interacció entre protocols emprats en els subsistemes de control de serveis NGN (SIP-IMS) i altres protocols IP. Aquesta

traducció de protocols IP de senyalització es plasma sobre una interfície anomenada *Iw*, que l'interconnecta amb el domini extern que suporta altres protocols.

Per exemple, pot traduir entre els perfils SIP d'IMS i altres perfils SIP, o altres protocols basats en IP com H.323.

Diferències que cal destacar per al model de la ITU-T pel que fa a l'ETSI-TISPAN

- Les funcions que fa l'IWF es poden mapar a l'entitat equivalent en el model de la ITU-T: la Network Signalling Interworking Functional Entity (NSIW-FE). La NSIW-FE també té com a tasca traduir a protocols de senyalització de xarxes de circuits, i en aquest cas es maparia a MGCF.

1.3.4. Altres components del model de la ITU-T de control de Servei

La ITU-T incorpora tres entitats funcionals que no apareixen en altres arquitectures de control de servei.

- **Interacció de Senyalització d'Usuari (USIW-FE)**: la User Signalling Interforking Functional Entity agrupa les funcions d'interoperabilitat de xarxes i monitoratge d'informació per a diferents tipus de senyalització d'aplicacions (diferents de SIP d'IMS), en el costat del subscriptor. Pot estar situat a la vora de la xarxa d'accés o del nucli de xarxa per a gestionar la senyalització en el costat del subscriptor.

- **Control de Passarel·la d'Accés (AGC-FE)**: l'Access Gateway Control Functional Entity controla un o més AMG-FE via la interfície S-T2 per a accedir als usuaris de xarxes bàsiques XTC/XDSI, i en gestiona el registre, l'autenticació i la seguretat. Pot iniciar i acabar senyalització de control de sessions, fluxos de control de sessió de passarel·les (*gateways*) per a controlar els AMG-FE, o fluxos de control UNI per a proporcionar serveis complementaris d'XDSI. D'altra banda, també pot reenviar fluxos de control a l'S-CSC-FE, i processar i reenviar peticions de l'AMG-FE a l'S-CSC-FE, o a l'AS-FE passant a través de l'S-CSC-FE.

- **Control de Serveis Generals (GSC-FE)**: la General Services Control Functional Entity pretén proporcionar una plataforma que doni suport als futurs serveis que es plantegin sobre xarxes de paquets. La GSC-FE ha d'actuar com un punt de contacte per a les entitats funcionals de suport de servei i aplicacions, i també per als terminals d'usuari. Haurà d'autenticar les comunicacions que es donin entre ells, i proporcionar informació sobre els fluxos de sessió i els seus requisits de QoS a la PD-FE o a l'IBC-FE.

General Service Control-FE

La GSC-FE o General Service Control-FE és una entitat funcional creada per l'ITU-T per a copar amb aquells serveis la invocació dels quals no porti associada un establiment de sessió prèvia, com sí que ho fa IMS. És un esforç que fa la ITU-T per tal d'incloure qualsevol altre mecanisme d'invocació de servei futur.

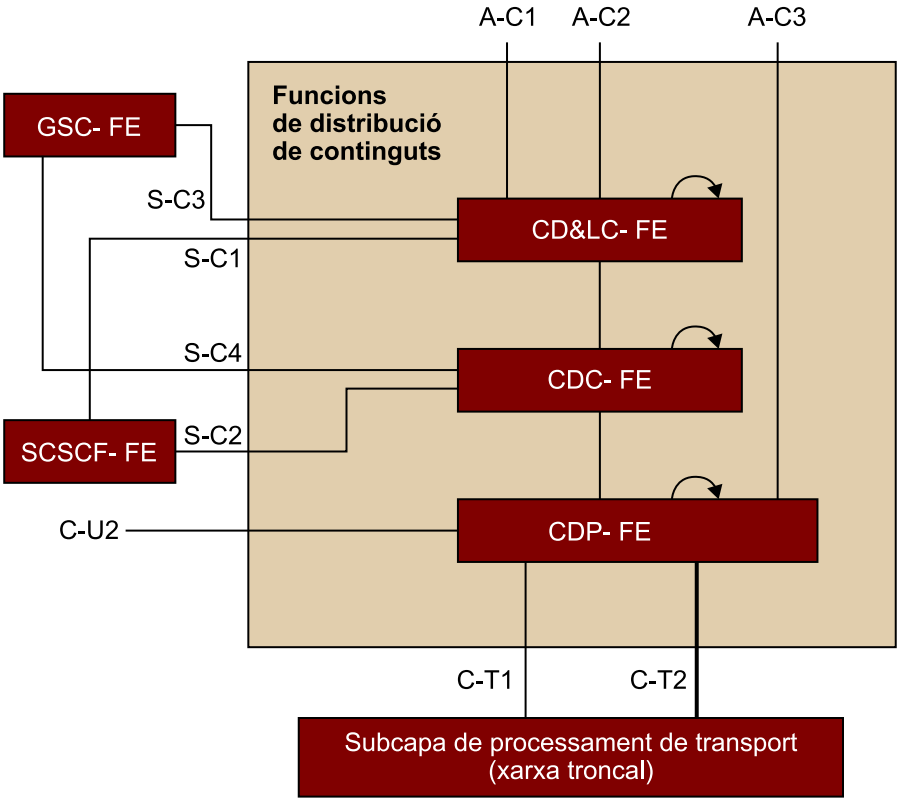
1.3.5. Components de la subcapa de Distribució de Contingut

Els components de les Content Delivery Functions (CDF) reben continguts des de la subcapa de les funcions de Suport a Aplicacions i Suport a Serveis (ASF&SSF), els emmagatzema, els processa i els lliura a les funcions d'usuari utilitzant les capacitats de les funcions de transport sota control de la subcapa de control de servei.

Aquests components els ha definit la ITU-T per a permetre als serveis d'IPTV, entre altres, distribuir els seus continguts entre els usuaris tant si són unidestinació (*unicast*) com si són multidestinació (*multicast*).

No obstant això, la ITU-T no tanca la porta al fet que opcionalment aquests serveis de distribució siguin duts a terme fora de l'àmbit de les xarxes NGN.

Figura 16. Arquitectura de les funcions de distribució de continguts



Si donem un cop d'ull a la figura 16, veiem les entitats funcionals i les interfícies que les interconnecten. Els punts de referència S-C1 i S-C2 corresponen al servei d'IPTV basat en IMS, mentre que els punts de referència S-C3 i S-C4 són per al servei d'IPTV no basat en IMS.

Control de Lliurament i Control de Localització (CD&LC-FE)

La Delivery Control and Location Control Functional Entity (CD&LC-FE) du a terme les funcions següents:

- Interacció amb les entitats funcionals de control de servei.

- Control de la distribució del contingut des de la CPR-FE (Preparació de Contingut) en la subcapa de suport a serveis i aplicacions cap a la CDP-FE.

- Aglutinament de la informació sobre les CDP-FE (ús de recursos, si està o no en servei o estat de càrrega).

- Selecció de les CDP-FE per a servir les funcions d'usuari en funció de la informació aglutinada i les capacitats del terminal d'usuari.

Control de Distribució de Continguts (CDC-FE)

La Content Delivery Control Functional Entity (CDC-FE) gestiona les funcions de control relacionades amb la CDP-FE. Part de les funcions que fa la CDC-FE són:

- Control del lliurament de recursos de mitjans.

- Gestió de les ordres de recodificació com per exemple per a VCR (Video Cassette Recorder).

- Informe d'estat (nivell de càrrega i disponibilitat) al CD&LC-FE.

- Generació d'informació per a facturació.

Processament de Distribució de Continguts (CDP-FE)

La Content Delivery Processing Functional Entity (CDP-FE) emmagatzema i desa el contingut, el processa sota control de la CPR-FE (en la subcapa de suport a serveis i aplicacions) i la CDC-FE. La CDP-FE distribueix el contingut entre instàncies de CDP-FE basades en la política del CD&LC-FE.

La CDP-FE és responsable de lliurar el contingut a les funcions d'usuari usant les funcions de transport (incloent-hi mecanisme d'unidestinació i multidestinació).

Altres funcions de la CDP-FE:

- Interacció amb les entitats funcionals de control de servei.

- Gestió del lliurament de continguts a l'usuari final.

- Emmagatzematge del contingut i la informació associada.

- Inserció, transcodificació i xifratge del contingut.

- Distribució de continguts entre CDP-FE.

- Gestió de la interacció amb l'usuari final: funcions de control de visualització del contingut (en el cas de vídeo) com per exemple rebobinar, anar cap endavant, pausa, etc.

1.3.6. Subcapa de Suport a Serveis i Suport a Aplicacions

La ITU-T concentra les funcions relacionades estrictament amb la provisió de serveis en una subcapa dins de la capa de servei (vegeu la figura 1) anomenada **subcapa de Suport a Aplicacions i Suport a Serveis** (ASF&SSF), que complementen els blocs de la subcapa de control de servei, on se situaria el nucli IMS (vegeu la figura 13).

El mòdul d'ASF&SSF controla els serveis oferts mitjançant la interacció amb l'S-CSC-FE (funció equivalent a l'S-CSCF del 3GPP) via una interfície anomenada *A-S4* (equivalent a l'ISC del 3GPP), l'GSC-FE via una interfície anomenada *A-S2* o l'usuari final via una interfície anomenada *A-U1*. Pot estar situat tant en la xarxa local d'usuari com en una tercera xarxa, i comprèn les entitats funcionals següents: Servidor d'Aplicacions (Application Server FE), Passarel·la d'Aplicacions (Application GW FE), Gestió de Coordinació entre Serveis d'Aplicacions (Application Service Coordination Manager FE) i Entitat Funcional de Commutació de Serveis (Service Switching FE).

Aquest mòdul genera les peticions de control de sessió i els diàlegs en representació de l'usuari. Així mateix, executa la lògica de servei basada en els perfils d'usuari i de terminal (capacitats del dispositiu).

El mòdul ASF&SSF pot actuar d'acord amb quatre models d'interacció de sessió en relació amb l'S-CSC-FE: agent d'usuari de terminació, agent d'usuari d'origen, servidor intermediari SIP o controlador de trucada *third-party*.

Pel que fa a la seva interacció amb les entitats del pla de control de servei, l'ASF&SSF pot interactuar amb l'AGC-FE (Access Gateway Control Functional Entity) per mitjà de l'S-CSC-FE per a permetre l'accés a les aplicacions a aquells usuaris que empren terminals tradicionals XTC o XDSI. Pot també controlar recursos multimèdia (tons, missatges àudio d'espera, etc.) amb l'MRP-FE (Media Resource Processing Functional Entity) per mitjà de l'MRC-FE (Media Resource Control Functional Entity) via la interfície A-S3 o l'S-CSC-FE via la interfície A-S4. Pot finalment accedir a l'MRB-FE (Media Resource Broker Functional Entity) via la interfície A-S1 per a assignar recursos multimèdia a les trucades o relacionar-se amb les funcions d'usuaris finals per a permetre que aquests gestionin i configurin les seves dades per als serveis d'aplicacions.

2. 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 la xarxa troncal de transport: mode *push* o mode *pull*.

Aquests dos mecanismes s'intenten adaptar a qualsevol xarxa d'accés que hi pugui haver en termes de reserva de recursos i negociació de QoS en la capa de transport. És a dir, hi haurà xarxes d'accés que posseeixin aquests mecanismes en capa 2 ja definits i hi haurà xarxes que no els posseeixin. En aquest sentit, es poden classificar els equips d'usuari en tres tipus. Aquesta classificació ens servirà per a saber quin tipus de mecanisme (*push* o *pull*) es pot relacionar a cada tipus de terminal:

- **Tipus 1**. Equip d'usuari sense capacitat de negociació de QoS ni en la capa de servei ni en la de transport. Es pot comunicar amb el nucli IMS (o entitat equivalent de la capa de servei) per a iniciar i negociar el servei però no pot sol·licitar recursos directament.

  Un exemple del tipus 1 seria una consola de jocs.

- **Tipus 2**. Equip d'usuari amb capacitat de negociació de QoS a escala de capa de servei. Usant la senyalització IMS negocia la QoS, com l'amplada de banda requerida, però desconeix totalment els paràmetres de QoS equivalents aplicables a la xarxa de transport.

  IMS negocia la QoS usant SDP (Session Description Protocol, RFC 4566) integrat dins dels missatges SIP.

- **Tipus 3**. Equip d'usuari amb capacitat de negociació de QoS a escala de capa de transport (tipus protocol RSVP o un altre protocol de transport). És capaç de fer directament negociació de QoS de transport al llarg de tota la infraestructura de transport (per exemple, DSLAM per a ADSL, CMTS per a cable, SGSN/GGSN per a telefonia mòbil).

  Un exemple del tipus 3 seria un terminal LTE.

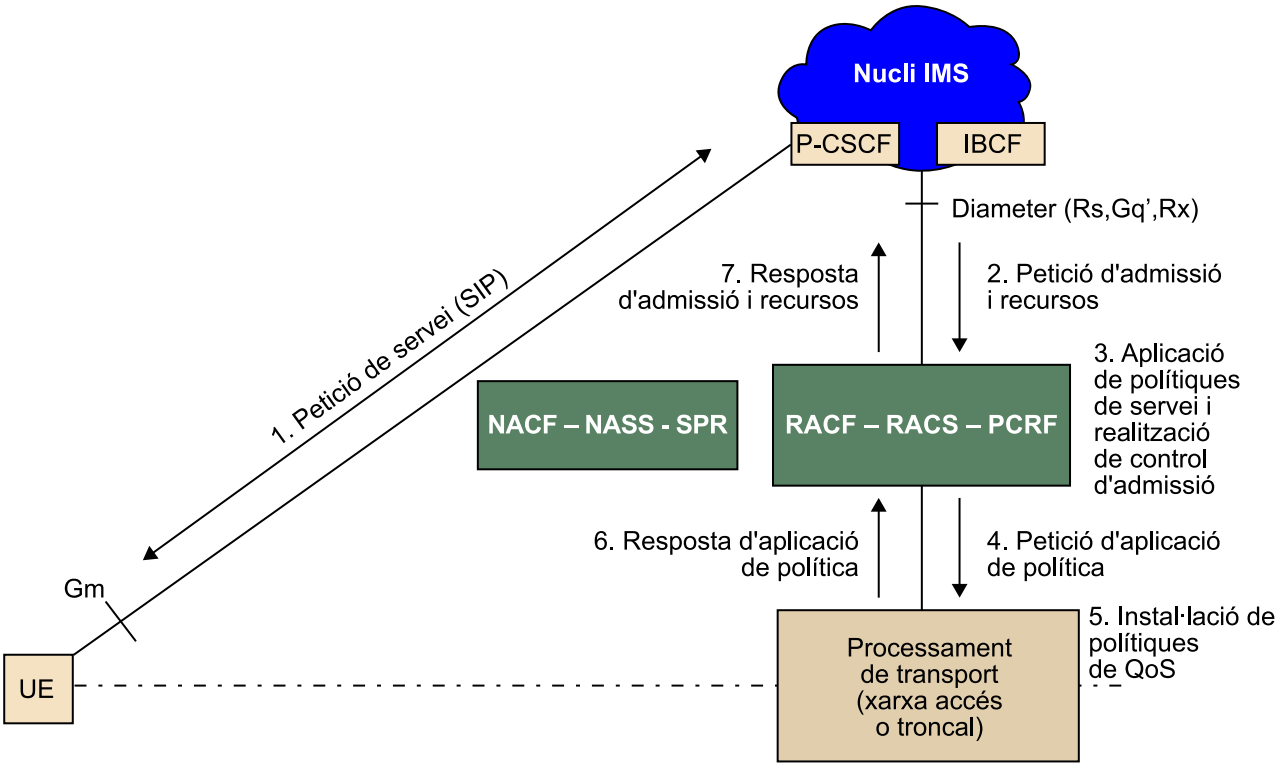
2.1. Mode *push*

La figura 17 ens mostra pas per pas el procés de reserva de recursos i garantia de QoS corresponent al mode *push*. Fixeu-vos que, seguint l'ordre dels passos, la reserva es dispara des de la capa de control de servei (en aquest cas el nu-

cli IMS, amb el P-CSCF si és la xarxa d'accés i l'IBCF si és la xarxa troncal) i posteriorment es tradueix en la instal·lació de polítiques de QoS sobre la capa de processament de transport.

En aquest cas, els tipus de terminals que s'adapten a aquest mecanisme en mode *push* són aquells que no tenen capacitat de negociar la QoS directament en la capa de transport: tipus 1 i tipus 2.

Figura 17. Mecanisme de reserva de recursos en mode *push*



Vegem amb una mica més de detall què succeeix en cada pas:

1) L'equip d'usuari (UE) inicia la petició de servei enviant un SIP INVITE. Si l'UE és de tipus 1 envia el missatge SIP amb les seves capçaleres pertinents, però si és de tipus 2 inclou una capçalera extra d'SDP amb l'especificació de QoS a escala d'aplicació o servei que sol·licita, en el qual inclou la sol·licitud de recursos. El P-CSCF reenvia aquest missatge a l'S-CSCF i espera un missatge de resposta que contingui la rèplica a l'INVITE amb la proposta final de QoS negociada en la capçalera SDP. D'aquí el P-CSCF extreu els paràmetres de QoS que necessita per a fer la sol·licitud de reserva de recursos a l'entitat per a fer el control d'admissió de recursos en la xarxa d'accés. Si el terminal és de tipus 1, no hi haurà SDP, però igualment el P-CSCF ha d'extreure paràmetres de QoS basant-se en polítiques pròpies prefixades.

2) El P-CSCF, via la interfície Diameter corresponent, sol·licita l'autorització QoS i la reserva de recursos amb els paràmetres QoS explícits cap a l'entitat que controla els recursos a la xarxa d'accés (subcapa de control de transport). Aquesta sol·licitud es du a terme amb un missatge AAR (AA-Request) el qual inclou una descripció detallada dels components multimèdia de la sol·licitud (informació d'amplada de banda, tipus de dades i altres paràmetres de QoS per a cada flux IP que els componen).

Lectura complementària

Per a conèixer els paràmetres dels missatges Diameter de la interfície Rx, llegiu el document 3GPP TS 29.214. Per al cas de la interfície Gq' recorreu a l'ETSI TS 183 017.

3) L'entitat de control de transport rep la petició i aplica les polítiques de xarxa a aquesta sol·licitud (regles arbitràries d'operador) per a poder autoritzar-la. Després aplica el control d'admissió consultant primer el perfil d'usuari i després la disponibilitat dels recursos sol·licitats en el sistema. Si tots els controls són superats i aquesta entitat decideix que és necessari instal·lar les polítiques de QoS pertinents (també cal tenir en compte si des del P-CSCF s'ha sol·licitat en una sola fase l'assignació final de recursos o *Commit*), es generen aquestes polítiques de QoS a partir de la sol·licitud rebuda des del P-CSCF per a ser instal·lades en les entitats de processament de transport pertinents.

4) Les entitats reben les polítiques de QoS per instal·lar, l'especificació de les quals pot ser tan simple com el nom d'una política ja predefinida o també una descripció detallada d'aquesta política (ja sigui amb paràmetres de QoS dependents de la tecnologia o no). En Diameter, per a instal·lar aquestes polítiques de QoS, s'utilitzen missatges com PIR (Policy Installation Request) en el cas de la interfície Re de l'ETSI-TISPAN o RAR (Re-Auth Request) en el cas de la interfície Gx del 3GPP.

5) Les polítiques s'instal·len i es converteixen aquells paràmetres de QoS que siguin independents de la tecnologia en paràmetres instal·lables i adaptats a paràmetres de la tecnologia pròpia. Aquí es du a terme també l'assignació de recursos a l'UE d'acord amb la definició de tals polítiques de QoS.

6) L'entitat que s'encarrega de l'aplicació de les polítiques de QoS notifica al gestor de recursos de la xarxa d'accés l'èxit d'aquesta instal·lació. Per a això, en Diameter s'usen els missatges respectius de respostes PIA (Policy Installation Answer) o RAA (Re-Auth Answer) segons sigui ETSI-TISPAN o 3GPP, respectivament.

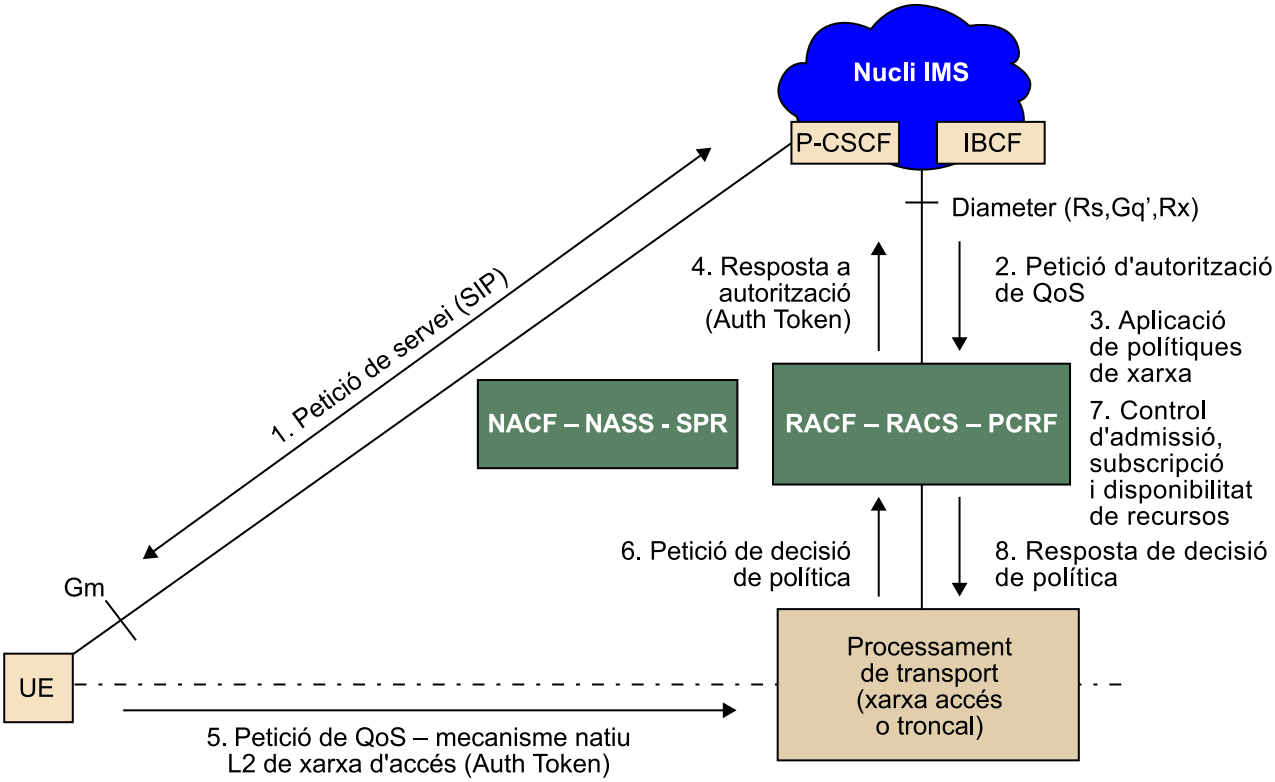
7) L'entitat de control de transport espera les respostes de totes les entitats a les quals ha sol·licitat la instal·lació de polítiques abans d'enviar una resposta amb la decisió final sobre la sol·licitud de recursos al P-CSCF. En Diameter, s'utilitza el missatge AAA (AA Answer).

2.2. Mode *pull*

La figura 18 ens mostra pas per pas el procés de reserva de recursos i garantia de QoS corresponent al mode *pull*. La reserva es divideix en dues parts, una feta des del nucli IMS per a autoritzar els recursos, i una altra per a assignar els recursos utilitzant el mecanisme natiu de la xarxa d'accés.

En aquest cas l'únic tipus de terminal que s'adapta a aquest mecanisme en mode *pull* és el de tipus 3.

Figura 18. Mecanisme de reserva de recursos en mode *pull*



Vegem amb una mica més de detall què succeeix en cada pas:

1) L'equip d'usuari (UE) inicia la petició de servei enviant un SIP INVITE. L'UE inclou una capçalera extra d'SDP amb l'especificació de QoS a escala d'aplicació o servei que sol·licita, en el qual inclou la sol·licitud de recursos. El P-CSCF reenvia aquest missatge a l'S-CSCF i espera un missatge de resposta que contingui la rèplica a l'INVITE amb la proposta final de QoS negociada en la capçalera SDP. D'aquí el P-CSCF extreu els paràmetres de QoS que necessita per a fer la sol·licitud de reserva de recursos a l'entitat per a fer el control d'admissió de recursos a la xarxa d'accés.

2) El P-CSCF, via la interfície Diameter corresponent, sol·licita el control d'admissió i la reserva recursos amb els paràmetres QoS extrets a l'entitat que controla els recursos en la xarxa d'accés (subcapa de control de transport). Per a aquests s'usa el missatge AAR ja esmentat.

3) L'entitat de control de transport rep la petició d'autorització de QoS i aplica les polítiques de xarxa a aquesta sol·licitud (regles arbitràries d'operador). Si la petició és autoritzada pot crear opcionalment un testimoni (*token*) d'autorització amb un únic identificador que representa la petició de QoS.

4) El bloc de control de recursos respon a la petició (missatge Diameter AAA) i si ha estat satisfactòria pot incloure el testimoni creat perquè el P-CSCF l'inclogui en el missatge SIP de retorn a l'UE.

5) L'UE sol·licita directament a les entitats de transport els recursos per a allotjar el trànsit del servei sol·licitat. Pot opcionalment incloure informació de QoS i també el testimoni d'autorització per a ajudar l'entitat de control de transport a associar la sol·licitud de recursos amb la sol·licitud autoritzada en els passos previs. L'associació es pot fer amb altres mètodes.

6) Les entitats de processament de transport detecten la petició de recursos remesa per l'UE i transfereixen aquesta petició en forma de petició de decisió de política a l'entitat de control de transport. Si el testimoni ha estat inclòs en la sol·licitud de recursos, aquest pot ser traspassat també. En aquest cas, tant per al cas de la interfície Re de l'ETSI TISPAN i com de la interfície Gx del 3GPP s'utilitza el missatge CCR (Credit Control Request) però el format intern pot variar lleugerament en funció de l'especificació.

Lectura complementària

Per a conèixer els paràmetres dels missatges Diameter de la interfície Gx, recorreu al document 3GPP TS 29.212. Per al cas de la interfície Re recorreu a l'ETSI TS 183 060.

7) L'entitat de control de transport aplica llavors el control d'admissió per als recursos sol·licitats consultant primer el perfil d'usuari i després la disponibilitat dels recursos sol·licitats en el sistema. Si la sol·licitud de recursos implica fer reserva i assignació en una sola fase, elabora les polítiques de QoS que cal instal·lar en les entitats de processament de transport que consideri oportunes (incloent-hi l'assignació dels recursos).

8) Les entitats de processament de transport reben la resposta del control d'admissió (missatge CCA) i apliquen les polítiques de QoS derivades de tal decisió per a assignar els recursos sol·licitats per l'UE.

Els passos de l'1 al 4, en els quals es fa una autorització mitjançant el testimoni, són opcionals, ja que l'associació entre la sol·licitud autoritzada i la petició de recursos des de la subcapa de processament de transport es pot fer d'altres maneres.

3. Protocols bàsics emprats en les xarxes NGN i IMS

Com hem vist en les descripcions dels punts de referència en apartats anteriors, els protocols que dominen la capa de servei són SIP, Diameter i H.248. En aquest apartat veurem les característiques principals de cadascun però focalitzant-nos més en els dos primers, ja que tenen molta més presència i complexitat.

3.1. Protocol SIP

Session Initiation Protocol o SIP (Protocol d'Iniciació de Sessió) és un protocol de senyalització definit per l'IETF (Internet Engineering Task Force) que permet l'establiment, l'alliberament i la modificació de sessions multimèdia (RFC 3261). Aquest protocol hereta certes funcionalitats dels protocols HTTP, utilitzats per a navegar sobre el Web, i SMTP, utilitzat per a transmetre correus electrònics. SIP es recolza sobre un model transaccional client/servidor, com HTTP. Com en SMTP, el format d'un missatge SIP està basat en capçaleres o *headers*, les quals estan expressades en text.

Per a temes d'adreçament SIP utilitza el concepte Uniform Resource Identifier o SIP URI, el qual és semblant a una adreça electrònica (usuari@domini.com). Cada participant en una xarxa SIP és llavors assolible via una adreça, per mitjà d'una SIP URI.

És important destacar que SIP és un protocol de senyalització per a iniciar, modificar i alliberar sessions multimèdia. D'altra banda, SIP no és un protocol de reserva de recursos i, en conseqüència, no pot assegurar la qualitat de servei. Es tracta d'un protocol de control de trucada i no de control del medi. 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 es recolzen en el protocol RTP/RTCP (Real Time Protocol / Real Time Control Protocol). El protocol SIP es pot usar sota TCP, UDP o SCTP.

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 el protocol especifica. Finalment, veurem les extensions a l'especificació SIP de l'IETF que IMS ha introduït.

3.1.1. 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.

- **Servidor de Readreçament** (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 Proxy Server, el Redirect Server no encamina les sol·licituds SIP. En el cas de la devolució d'una trucada, el Proxy Server té la capacitat de traduir el nombre del destinatari en el missatge SIP rebut, en un número de reenviament de trucada i encamina la trucada a aquesta nova destinació, i això de manera transparent per al client d'origen; per al mateix servei, el Redirect Server retorna el nou número (número de reenviament) al client d'origen, que s'encarrega d'establir una trucada cap a aquesta nova destinació.

- **Agent Usuari** (User Agent) o UA: es tracta d'una aplicació sobre un equip d'usuari que emet i rep sol·licituds SIP. Es materialitza per un programari instal·lat sobre un UE.

- **El Registrador** (Registrar): 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 en Registrar l'adreça on és localitzable (adreça IP). El Registrar actualitza llavors una base de dades de localització. El registrador és una funció associada a un Proxy Server o a un Redirect Server. Un mateix usuari es pot registrar sobre diferents UA SIP; en aquest cas, la trucada li serà lliurada sobre el conjunt d'aquestes UA.

3.1.2. 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 quins tipus de peticions i resposta preveu l'especificació.

Capçalera SIP

Un missatge SIP està 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 amb 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 capçaleres 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-
d56e91fe104f
To: Bob <sip:bob@iptel.org>
Call-ID: d10815e0-bf17-4afa-8412-d9130a793d96@213.20.128.35
CSeq: 2 INVITE
Contact: <sip:213.20.128.35:9315>
User-Agent: Windows RTC/1.0
Proxy-Authorisation: Digest username="jiri",
realm="iptel.org",algorithm="MD5", uri="sip:jiri@bat.iptel.org",
nonce="3cef753900000001771328f5ae1b8b7f0d742da1feb5753c",
response="53fe98db10e1074
b03b3e06438bda70f"
Content-Type: application/sdp
Content-Length: 451

v=0
o=jku2 0 0 IN IP4 213.20.128.35
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 de tipus petició (Request) per a l'inici de sessió. En el subapartat següent podeu veure la resta de mètodes SIP que hi ha. En comptes del mètode també 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 que representa el destinatari d'aquest missatge (anomenat 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 seva 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:* i ens diu que el client SIP (o també anomenat *User Agent*) s'executa en un PC amb IP 176.54.75.23 i usa el port 5040.

Els camps *From:* i *To:*, igual que en SMTP, contenen identificadors de l'originador de la petició (usuari que truca) i el destinatari (usuari a qui s'ha 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 identificar a quina petició fa referència.

La capçalera *Contact:* conté l'adreça IP i el port sobre el qual el sol·licitador està esperant peticions posteriors enviades per l'usuari a qui s'ha 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:* està delimitada del 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 es poden dividir en dos tipus: peticions i respostes. A continuació es mostra una llista de les peticions:

Taula 1. Mètodes SIP

Mètode	Descripció
INVITE	Enviat des del terminal UA que truca a l'UA a qui es truca. Indica que un client està essent 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	Enviat per qui truca a qui es truca per a acabar una sessió.
CANCEL	Cancel·lar qualsevol petició pendent de resposta o qualsevol transacció.
OPTIONS	Sol·licita a un altre UA o a un servidor intermediari quines capacitats tenen (mètodes suportats, els tipus de continguts, les extensions, els codificadors, etc. sense haver de provocar el "ringing" de l'altra part).
REGISTER	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'haurien d'encaminar les peticions.
PRACK	ACK Provisional. És com un ACK per a respostes provisionals amb codi 1xx (RFC 3262).
SUBSCRIBE	Subscripció a un esdeveniment de notificació enviat des d'un notificador (RFC 3265).
NOTIFY	Usat per a notificar a les entitats subscriptores sobre un esdeveniment d'actualització de registre (RFC 3265).
PUBLISH	Enviat per un client per a publicar un esdeveniment en 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 es troben els dígits DTMF, les informacions relatives a la taxació d'una trucada, etc.
REFER	Un UA el pot usar per a instar un altre UA perquè iniciï una petició SIP cap a un tercer UA. Permet emular diferents serveis o aplicacions, incloent-hi la transferència de trucada (RFC 3515).
MESSAGE	Transporta missatges instantanis de text usant SIP. El requisit 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 terminal SIP actualitzar els paràmetres d'una sessió multimèdia (flux de mitjans i els seus codificadors). El mètode UPDATE pot ser enviat abans que la sessió sigui establerta (RFC 3311).

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 formada per tres dígits seguits per una descripció textual del codi.

L'STATUS CODE està dividida en sis famílies diferents en què el primer dígit indica la classe del codi, com es mostra en la taula següent.

Taula 2. Codis de respostes SIP

Codi	Descripció	Exemple
1xx	Respostes provisionals / informacionals	100 Trying, 180 Ringing
2xx	Respostes reeixides	200 OK
3xx	Respostes de readreçament	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

3.1.3. Extensions per a IMS

El protocol SIP va ser triat pel 3GPP com a base per a la senyalització d'IMS. No obstant això, hi havia molts buits entre el protocol SIP de base definit per l'IETF i les característiques requerides per a suportar les prestacions d'IMS al complet. Per a resoldre aquest problema el 3GPP va definir dotzenes d'extensions SIP específiques per a xarxes IMS. Col·lectivament aquestes extensions comprenen el protocol SIP IMS i defineixen un perfil propi de SIP. El protocol SIP IMS està 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 il·lustrar la inherent complexitat del SIP IMS i totes les seves extensions, veurem per damunt les extensions més importants:

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

2) Capçaleres privades o *P-headers*: a més de les capçaleres estàndard, el 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 a escala de seguretat o *Security Agreement*: especifica com es poden negociar les capacitats de seguretat per a múltiples 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 també intercanvi de claus específiques. Es pot trobar més informació sobre AKA-MD5 en l'RFC 3310.

5) IPSec[9]: 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.

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

6) Autorització de mitjans o *Media Authorization*: s'assegura que solament els recursos de mitjans autoritzats són utilitzats. Se'n pot trobar informació més detallada en l'RFC 3313.

7) Registre en mobilitat o *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 de les entitats SIP de les capçaleres Service-route i Path.

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

9) Precondicions o *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 es fa reserva de recursos per a trucades de telèfon o sessions. Més informació en l'RFC 3312.

11) SDP o *Session Description Protocol*: l'SDP defineix el procés de negociació bàsica per als fluxos de mitjans i inclou el codificador i l'amplada de banda que cal usar i també altres atributs. IMS estén l'SDP fins i tot amb més extensions com ara l'agrupació de fluxos, QoS i atributs de precondicions, suport de codificadors 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 amb atributs (a=) la descripció d'un component multimèdia:

```
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-hi 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 de l'IETF que defineix els requisits 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 suficientment eficients per a usar-se en un enllaç sense fil. SIP IMS van estendre aquest estàndard amb el següent: Publicacions i notificacions parcials; Filtratge de Notificacions, i Llista de recursos.

3.2. Protocol DIAMETER

El protocol Diameter deriva del protocol RADIUS amb moltes millores en diferents aspectes com ara la gestió d'errors i fiabilitat de lliurament de missatges. Utilitza l'essència del protocol AAA de RADIUS i defineix una sèrie de missatges bàsics definits en la recomanació Diameter Base Protocol (RFC 3588). Diameter és usat en IMS per a intercanvi d'informació relacionada amb tasques d'AAA (Authentication, Authorization i 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 la Cx, que inclourà els seus missatges propis de petició-resposta i els paràmetres (anomenats Attribute-Value Pair o AVP) que els componen. I així es dóna amb totes les interfícies basades en Diameter que hem anat esmentant en aquest document.

Per exemple, la interfície Rx, com a aplicació que és, té associat un identificador (Application ID) que és únic i té uns missatges (o també anomenats *ordres*) ben definits per a escometre la seva funció. Cada missatge conté una llista d'AVP que defineixen el seu 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.

3.2.1. Nodes i agents Diameter

El protocol Diameter està dissenyat per a arquitectures d'igual a igual. Cada *host* 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 tant a un client com a un servidor i a un agent de Diameter.

En un entorn en què 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 posseeix el NAS aglutina la informació de credencials de l'usuari i l'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 (ja sigui satisfactòria o no) al client.

En les transaccions amb missatges Diameter hi ha, com en SIP, el concepte de domini, el qual està sempre especificat en tots els missatges Diameter. Aquesta informació de domini ajuda els nodes a processar-los d'una manera o una 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 a 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, en comprova la taula de rutes i retorna un missatge de resposta juntament amb informació de readreçament al node que ha enviat la petició. Això seria 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).

3.2.2. Missatges Diameter

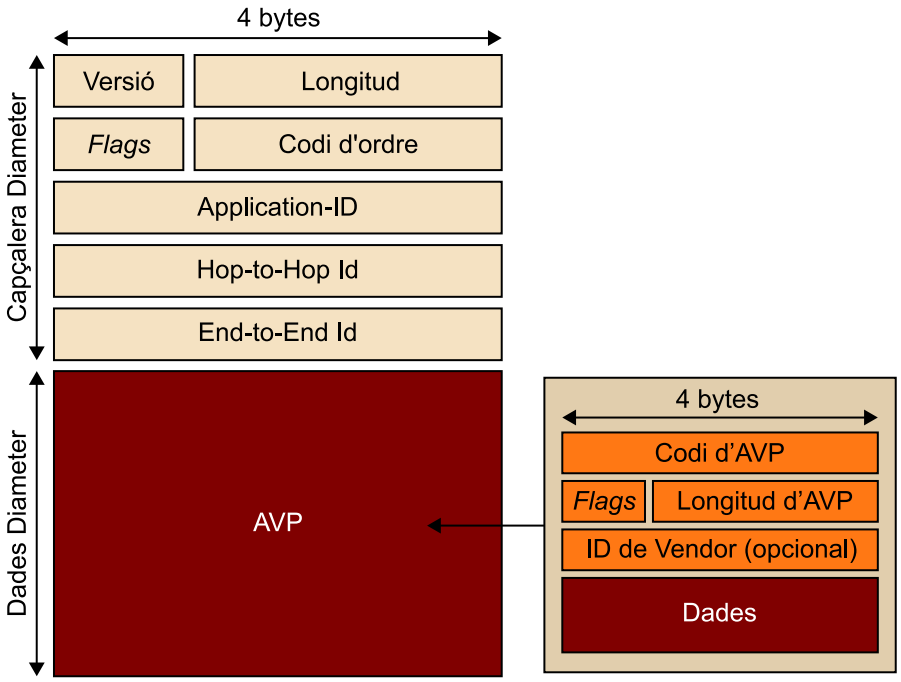
Un missatge Diameter és la unitat base per a enviar una ordre o lliurar una notificació a altres nodes Diameter. Depenent de l'aplicació per implementar, el protocol Diameter ha definit diversos tipus de missatges, que són identificats pel seu codi d'ordre.

Com l'intercanvi de missatges en Diameter és síncron, 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 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 primer de tot 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 en el seu interior estan contingudes 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 a 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 la qual cosa cada AVP ha de seguir el format de dades concret. La figura 19 mostra els camps que componen un missatge de Diameter.

Figura 19. 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[10]).

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

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

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).

Segons l'especificació de l'aplicació de Diameter per implementar, es posarà un valor en el camp d'Application-ID[11] o un altre (assignat també per la IANA).

(11)Per a la interfície Rx l'Application-ID és 16777236.

Entitats d'estandardització com 3GPP i ETSI-TISPAN

Les entitats d'estandardització com el 3GPP i l'ETSI-TISPAN han publicat documentació en la qual descriuen totes les interfícies basades en Diameter que apareixen en les seves especificacions, en què els assignen un Application-ID. En aquests documents es proposen totes les ordres que formen la interfície, i per a cada ordre, depenent de si és *request* o *answer*, es defineixen tots els AVP. Tingueu en compte que hi ha definicions d'AVP que es comparteixen entre especificacions entre dues interfícies perquè fan la mateixa funció o fins i tot es comparteixen entre especificacions de diferents entitats d'estandardització. Pot ser que hi hagi AVP amb Vendor ID 3GPP usats en especificacions de l'ETSI-TISPAN i viceversa. Això és resultat d'uniformitzar les diferents implementacions.

3.3. Protocol H.248 / MEGACO

L'H.248 és un protocol definit per la ITU-T, encara que hi ha una implementació equivalent de l'IETF anomenada MEGACO (RFC 3525). És un protocol per a controlar els elements d'una passarel·la multimèdia físicament separada, que habilita la separació del control de trucada de la conversió de mitjans.

És un protocol basat en una arquitectura mestre/esclau usat per a separar la lògica del control de trucada del processament dels mitjans.

En IMS s'utilitza per a controlar passarel·les localitzades en la subcapa de processament de transport per a instal·lar configuracions d'obertura de control d'accés a manera de tallafoc i fixar traduccions.

4. Exemples de fluxos de trucades en NGN IMS

Amb tal d'afermar els conceptes explicats fins ara donarem 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 els recursos de la subcapa de Control de Transport en la garantia de QoS d'extrem a extrem.

Els dos exemples que veurem són el procés de registre en IMS, en el qual es mostren les dues fases:

1) Adhesió a la xarxa segons el model de l'ETSI-TISPAN i després el registre en el nucli IMS.

2) L'establiment d'una trucada de veu per mitjà de dos nuclis IMS per a veure la interacció entre dos dominis.

També s'inclou al final un exemple del servei de presència en IMS, com a mostra de la interacció amb un servidor d'aplicacions (AS).

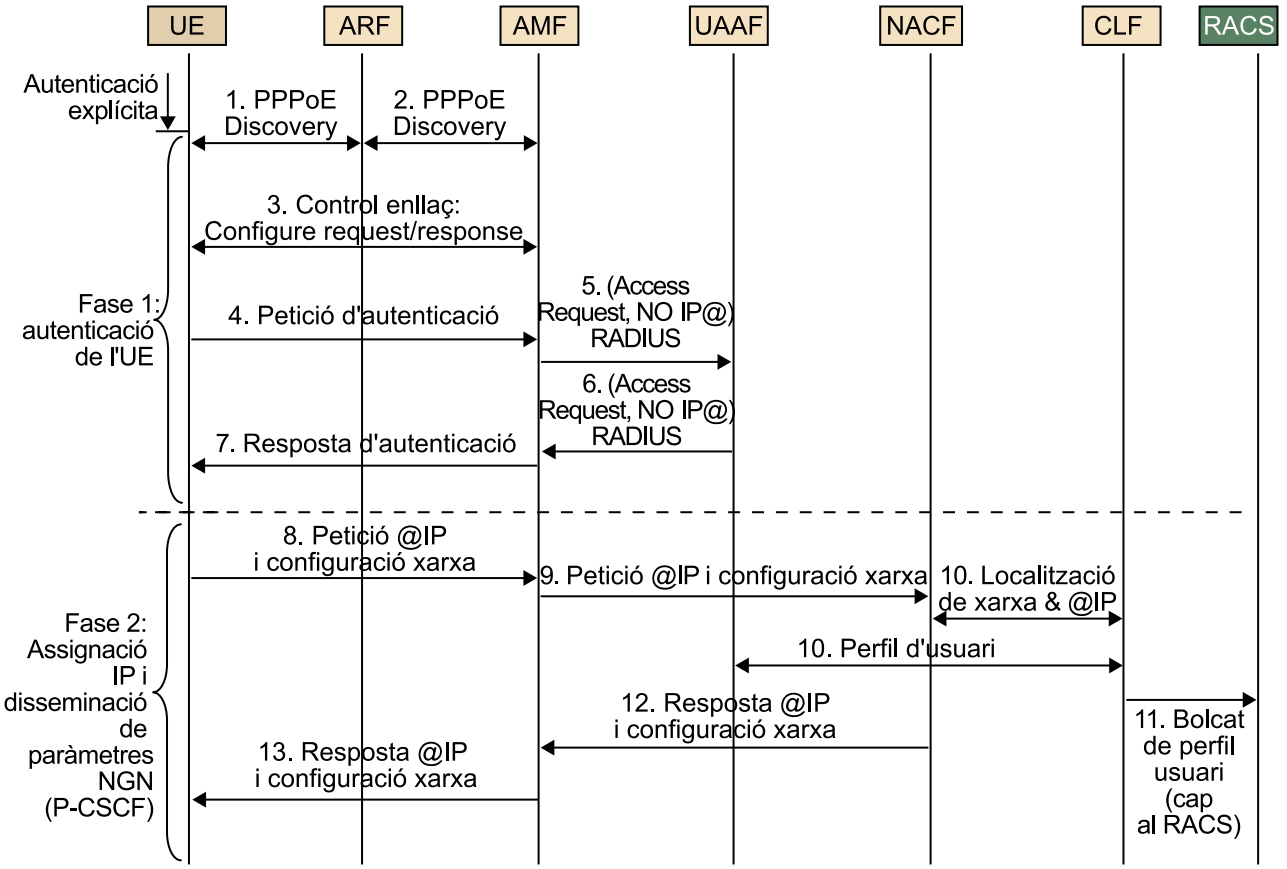
4.1. Adhesió a la xarxa

Seguidament veurem missatge per missatge el procés d'adhesió d'un UE a la xarxa d'accés i com posteriorment es registra en el nucli IMS.

4.1.1. Fase d'autenticació de l'equip d'usuari i assignació d'IP

La figura següent mostra pas per pas un exemple d'adhesió a la xarxa amb autenticació explícita d'un encaminador ADSL (UE) en registrar-se a la xarxa d'accés usant PPPoE com a protocol d'establiment de connexió en capa 2.

Figura 20. Pas per pas d'adhesió d'un UE a la xarxa d'accés (exemple basat en especificació d'ETSI-TISPAN)



Procés d'autenticació, assignació i configuració

a) Passos 1 i 2: l'UE fa els procediments de PPPoE discovery per a identificar l'AMF apropiat i estableix una relació d'igual a igual amb l'AMF, tal com es requereix en PPP. L'ARF implementa un agent intermedi de PPPoE i insereix la identificació de línia d'accés en els missatges de PPPoE.

b) Pas 3: Inicia la fase LCP (Link Control Protocol) del PPP. Negociació de paràmetres d'enllaç de dades entre l'UE i l'AMF incloent-hi la negociació del procediment d'autenticació que s'usarà.

c) Pas 4: l'UE inicia l'autenticació i envia la informació corresponent (identitat de l'usuari i informació sobre la contrasenya) a l'AMF.

d) Pas 5: l'AMF tradueix la petició PPP al missatge equivalent de RADIUS (AMF fa de client) per a sol·licitar accés a l'UAAF, que autentica la identitat de l'usuari associat a l'UE.

e) Pas 6: l'UAAF contesta a l'AMF reportant autenticació reeixida.

Nota

En el cas hipotètic d'un escenari d'itinerància, l'UAAF de la xarxa visitada actuaria com a UAAF proxy (proxy RADIUS en aquest exemple) i reenviaria la petició d'autenticació per la interfície e5 a l'UAAF correcte.

f) Pas 7: l'AMF envia el missatge PPP corresponent per reportar aquesta autenticació reeixida. Finalitza la fase LCP del PPP. L'usuari ha estat autenticat a la xarxa d'accés amb èxit.

g) Pas 8: inicia la fase de NCP (Network Configuration Protocol) del PPP. Sol·licita a l'AMF l'assignació d'una adreça IP.

h) Pas 9: l'AMF tradueix aquesta sol·licitud d'adreça IP a RADIUS i l'envia al NACF.

i) Pas 10: el NACF selecciona una IP del seu repositori i bolca aquesta informació al CLF. De la mateixa manera, l'UAAF bolca al CLF el perfil d'usuari una vegada ja està autenticat.

Nota

L'UAAF pot bolcar la informació de perfil d'usuari tan aviat com l'UE s'autentica amb èxit. No cal que esperi al NACF perquè li assigni l'adreça IP. El CLF és capaç de rebre totes dues informacions i associar-les *a posteriori*.

j) Pas 11: tan aviat com el CLF rep la informació del NACF i de l'UAAF, bolca la informació integrada al RACS (via la interfície e4 basada en Diameter) perquè ho tingui present si aquest UE sol·licita en un futur un servei amb requisits de QoS.

k) Pas 12 i 13: el NACF li proporciona (via l'AMF traduint-ho a PPP) l'adreça IP assignada i informació sobre el P-CSCF (*hostname*) al qual s'ha de dirigir.

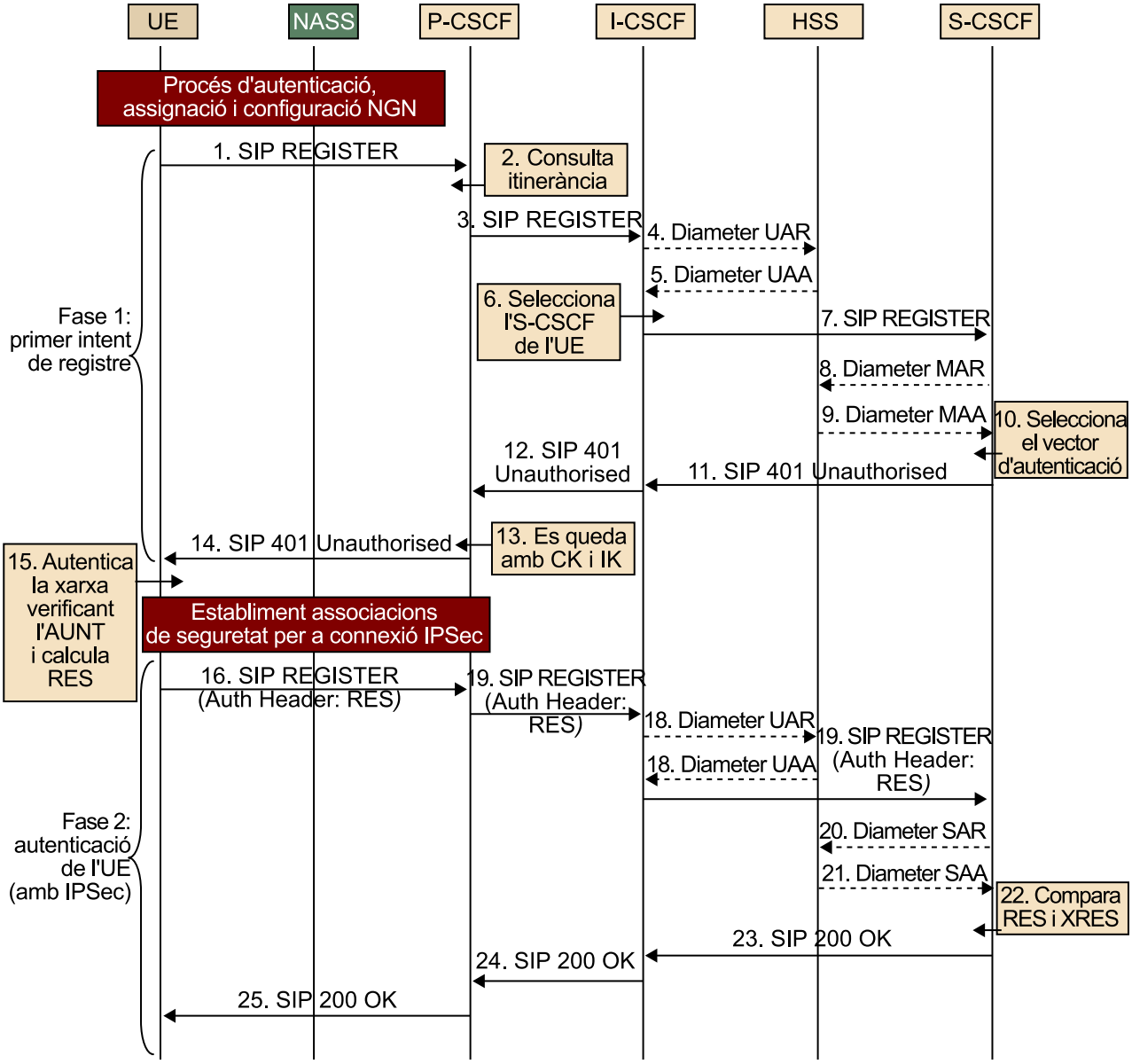
A partir d'aquest instant l'UE ja disposa d'una adreça IP, que és única en l'àmbit de la xarxa d'accés (ja sigui pública o privada). Conseqüentment, l'UE pot sol·licitar serveis IMS per mitjà de la interfície Gm una vegada estigui registrat en el nucli IMS.

Cal esmentar que els protocols d'autenticació i assignació d'IP poden variar. En comptes de PPP es pot usar 802.1x i DHCP per a la sol·licitud d'IP i dissemінació de configuració de nucli IMS.

4.1.2. Fase de registre en el nucli IMS

La figura següent mostra els passos que fa un UE per a registrar-se en el nucli IMS. En aquest cas, no importa quina implementació s'usi per a la xarxa d'accés, ja que IMS és independent d'aquesta.

Figura 21. Pas per pas de registre en nucli IMS



a) Pas 1: l'UE (client IMS) envia un missatge SIP REGISTER cap a la IP del P-CSCF que el seu *hostname* ha rebut des del NASS. La IP la descobreix via consulta de DNS. Afegeix una capçalera *Via:* amb el seu *hostname* per a notificar que el missatge ha passat per ell.

b) 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 seu 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 de 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) i descobreix la seva adreça IP via DNS.

c) 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).

d) Pas 4: l'I-CSCF rep el SIP REGISTER i la seva funció és saber a quina S-CSCF del seu domini l'ha de reenviar. Per saber-ho envia una petició Diameter amb l'ordre User Authorization Request a l'HSS (via la interfície Cx), en què li sol·licita la llista d'S-CSCF.

e) Pas 5: l'HSS contesta amb un User Authorization Answer incloent la llista d'S-CSCF candidats i les seves capacitats.

f) 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 capçalera *Via:* més amb el seu *hostname*.

g) Pas 7: l'I-CSCF reenvia a l'S-CSCF seleccionat el SIP REGISTER.

h) 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.

i) Pas 9: l'HSS respon amb un Multimedia Authentication Answer incloent el Random number (RAND), Authentication token (AUT), signed result (XRES), Cipher key (CK) i Integrity Key (IK).

j) Pas 10: l'S-CSCF selecciona l'Authentication vector (format pels cinc paràmetres anteriors) per usar per a autenticar l'UE.

k) 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. Llavors el missatge es reenvia a l'I-CSCF.

l) Pas 12: el missatge de resposta 401 passa al P-CSCF.

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

n) Pas 14: envia el missatge 401 Unauthorized a l'UE per reptar-lo en l'autenticació.

o) Pas 15: l'UE, usant l'Authentication Token (AUT), s'autentica en 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).

p) 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*.

q) Pas 17: El P-CSCF reenvia de nou el missatge a l'I-CSCF.

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

s) Pas 19: l'I-CSCF reenvia a l'S-CSCF seleccionat el SIP REGISTER.

t) Pas 20: sol·licita a l'HSS amb una ordre Server Assignment Request informació de subscripció de l'usuari que es vol autenticar.

u) Pas 21: l'HSS respon amb un Server Assignment Answer.

v) Pas 22: compara el valor RES rebut des de l'usuari amb el valor XRES. Si coincideixen l'autenticació de l'usuari és correcta.

w) Pas 23 a 25: s'envia un missatge de resposta d'èxit (200 OK) que indica 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 com a registrat (i també la seva adreça IP i identitats públiques registrades).

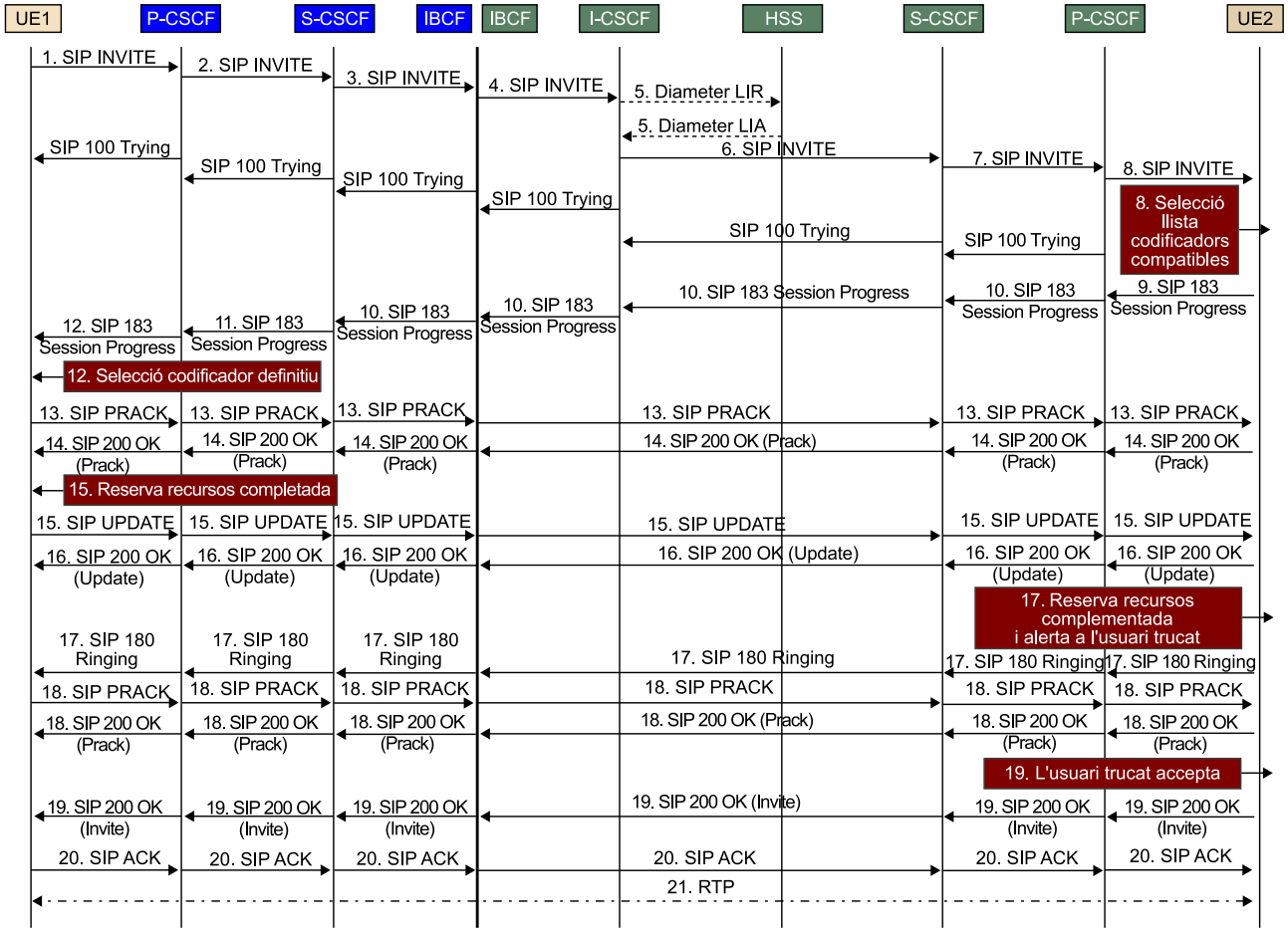
4.2. Establiment de sessions de serveis

Seguidament veurem primer l'exemple de l'establiment d'una trucada de veu amb garantia de QoS d'extrem a extrem en el qual tots dos interlocutors es troben en diferents dominis IMS. Després veurem com funciona el servei de presència en IMS.

4.2.1. Sessió IMS de servei de veu

La figura següent 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 22. Flux de trucada de veu en IMS



1) 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 la del P-CSCF) posant 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 a posar el *hostname* del P-CSCF (es 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, on l'UE1 proposa uns paràmetres de QoS inicials (*Preconditions*) segons els codificadors que suporta per a veu. Recordem també que aquest missatge s'envia per mitjà de la connexió IPSec entre l'UE 1 i el P-CSCF, establerta en la fase de registre.

2) 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 mira la capçalera *Route:* i extreu el *hostname* de l'S-CSCF especificat. Ho resol via DNS i reenvia el SIP INVITE a aquest S-CSCF. Abans d'enviar el missatge, el P-CSCF elimina la capçalera *Route:* que portava el seu propi *hostname*, la capçalera *P-Preferred-Identity:*, i afegeix una capçalera *Via:* amb el seu *hostname* per deixar mostra del camí recorregut fins ara pel missatge SIP. També afegeix una capçalera *Record Route:* per obligar que, si hi ha un missatge de tornada, aquest passi pel P-CSCF.

Nota

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 Triying. Això es repeteix per a tots els altres elements que processen la petició SIP INVITE en el camí.

c) Pas 3: el S-CSCF rep el missatge i procedeix a encaminar el missatge SIP cap al domini detinació. 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 propi *hostname*.

Nota

Un domini IMS no ha de tenir necessàriament un IBCF connectat amb tots els dominis existents del món. En el seu lloc, pot tenir un IBCF cap a un domini IMS "en trànsit" al domini destinació. És com una espècie de ruta per defecte però a escala de dominis IMS destinació.

d) 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 un altre domini sobre la topologia del nucli IMS origen (capçaleres *Via:* sobretot). El SIP INVITE travessa la frontera entre dominis (possiblement per mitjà d'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. Llavors el reenvia a l'I-CSCF que tingui configurat perquè aquest se n'encarregui. Afegeix un *Record Route:* amb el seu *hostname* i també el corresponent *Via:*.

Nota

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

e) Pas 5: l'I-CSCF del domini verd consulta a l'HSS via la interfície Cx (Diameter; intercanvi d'ordres de tipus Location Information o LIR / LIA) a quina S-CSCF (*hostname*) cal enviar el SIP INVITE. És per això que 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 poder reenviar el missatge a la seva destinació.

f) 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 es troba registrat. Si ho està, mapa aquesta identitat amb l'adreça IP i el port amb el qual l'UE 2 està 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 propi *hostname*.

g) Pas 7: el P-CSCF del domini verd rep el missatge i poden succeir dues coses depenent dels mecanismes de reserva de recursos de la xarxa on UE 2 està connectat:

- Mode *pull*: el P-CSCF sol·licitaria al PCRF/RACS/RACF un *Authorization token* per incloure'l en el missatge per enviar a l'UE 2.

- Mode *push*: el P-CSCF no sol·licita res al PCRF/RACS/RACF perquè solament té la informació de QoS de l'UE. Reenvia el missatge a l'UE 2.

En tots dos casos, abans d'enviar el missatge (per mitjà de la connexió IPSec corresponent) el P-CSCF inclou en la capçalera *Via:* el seu *hostname*.

Nota

Per al cas concret del mode *push*, hi ha la possibilitat que el P-CSCF estigui configurat perquè faci una reserva de recursos a la xarxa d'accés però incloent-hi informació de QoS proposada solament per l'UE 1, i esperar que en intercanvis successius de missatges SIP s'actualitzi la informació de QoS definitiva i, per tant, actualitzi els recursos reservats a la xarxa d'accés.

h) Pas 8: l'UE 2 rep el SIP INVITE amb la proposta de codificador de l'UE 1. Llavors selecciona d'aquesta llista aquells codificadors compatibles amb els suportats per ell i 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 UE 2 s'inclouen en un missatge de resposta provisional de tipus 183 Session Progress. Les capçaleres *Via:* i el *Record Route:* són copiades del missatge SIP INVITE rebut. La capçalera *Contact:* es canvia amb la IP i port usats per l'UE 2. S'indica també en el missatge SIP la capçalera *Require: 100rel*, amb la qual 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.

i) 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 reenviar el missatge de resposta (fins que no rep la resposta des del PCRF/RACS/RACF no reenvia el missatge SIP).

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

Nota

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.

k) Pas 11: la resposta 183 Session Progress, amb una capçalera SDP amb una llista de paràmetres de QoS prenegociats, entra en UE 1 i UE 2, i arriba al P-CSCF del domini blau, el qual pot actuar de dues maneres, depenent del model de reserva de recursos de la xarxa d'accés:

- Mode *pull*: en el cas que l'UE 1 estigui en una xarxa d'accés amb mecanismes de reserva de recursos en capa 2, el P-CSCF sol·licitaria al PCRF/RACS/RACF un *Authorization token* per incloure'l en la resposta que ha d'enviar a l'UE 1.
- Mode *push*: el P-CSCF sol·licitaria al PCRF/RACS/RACF l'autorització de QoS i reserva de recursos utilitzant la primera selecció de codificadors proposada en l'SDP (normalment, si hi ha més d'una opció de codificadors la primera especificada en la llista és la preferida per tots dos UE). La xarxa d'accés inicia aquesta reserva de recursos per 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 feta.

l) Pas 12: l'UE 1 selecciona els codificadors definitius de la llista rebuda en l'SDP per usar en la conversa de veu. Com a més veu en el missatge de resposta que hi ha la capçalera *Require:100rel*, prepara un missatge PRACK per a l'UE 2. Seguidament, i ara que ja té el codificadors definitiu, depenent del model de reserva de recursos de la xarxa d'accés de l'UE 1, aquest actuarà d'una manera o una altra:

- Mode *pull*: inicia els mecanismes propis que tingui la xarxa d'accés per a garantir la QoS negociada (amplada de banda en tots dos sentits, entre altres paràmetres de QoS). En aquesta petició de recursos ha d'incloure l'*Authorization Token*, si n'hi ha. En el missatge PRACK per enviar amb els codificadors definitius es notifica a l'UE 2 l'estat de la reserva de recursos amb l'atribut *a=curr: qos local none*. Amb això li indica que els recursos en la xarxa local de l'UE 1 encara no estan disponibles (encara que realment la seva reserva ja ha estat iniciada).

- Mode *push*: l'UE 1 no ha de fer res, ja que tan aviat com ha rebut el 183 Session Progress pot assumir que hi ha una reserva de recursos feta (depenent de la tecnologia de la xarxa d'accés l'UE 1 seria informat sobre els recursos assignats). En el missatge PRACK per enviar amb els codificadors definitius, l'UE 1 ja estaria en posició de notificar a l'UE 2 amb l'atribut *a=curr: qos local sendrecv* que una reserva de recursos ja ha estat feta a la seva xarxa d'accés.

Sobre el mode *push*

Pel que fa al mode *push*, es poden trobar alguns programaris de clients IMS que s'executen en PC connectats a una LAN i, per tant, no reben cap notificació sobre la reserva de recursos. Però no assumeixen cap reserva pel fet de rebre el 183 Session Progress i no notificarien a l'UE 2 que hi ha una reserva de recursos en la seva xarxa d'accés (inclouen l'atribut atribut *a=curr: qos local none*), assumint que posteriorment hi haurà un intercanvi de missatges UPDATE /200 OK, en què sí que es notificarà sobre aquesta reserva definitiva de recursos.

m) Pas 13: el PRACK recorre tot el camí fins a l'UE 2 del domini verd, el qual fa les accions següents depenent del model de reserva de recursos:

- Mode *pull*: inicia la reserva de recursos tenint en compte el codificador definitiu seleccionat. Contesta amb un 200 OK (i el mateix contingut en la capçalera SDP) al PRACK i notifica a l'UE 1 que la reserva de recursos encara no està disponible (*a=curr: qos local none*).

- Mode *push*: simplement contesta amb 200 OK i notifica a l'UE 1 (amb el mateix contingut en la capçalera SDP). L'UE 2 pot assumir que en rebre el PRACK ja s'ha fet una primera reserva de recursos en la seva xarxa d'accés (i estaria en posició de notificar a l'UE 2 amb l'atribut *a=curr: qos local sendrecv)*. Però de la mateixa manera que en el pas 12 en mode *push*, l'UE 2 podria esperar a rebre el missatge UPDATE per a notificar sobre l'estat de la seva reserva de recursos.

n) 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 actualitzacions de la reserva de recursos amb la informació SDP del missatge de resposta (això solament es dóna si tots dos estan en mode *push*).

o) 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 sobre l'estat definitiu de la reserva de recursos en la seva xarxa d'accés. Això es fa enviant dins del missatge UPDATE la capçalera SDP amb el mateix format que el PRACK però incloent-hi l'atribut *a=curr: qos local sendrecv*. No obstant això, depenent del model de reserva de recursos de la xarxa d'accés el missatge UPDATE s'enviarà en un moment o un altre:

- Mode *pull*: l'UE 1 esperarà la reserva de recursos iniciada anteriorment (en rebre el PRACK i seleccionar el codificador definitiu) per a enviar l'UPDATE amb l'actualització de l'estat de reserva en la capçalera SDP.
- Mode *push*: l'UE 1 pot enviar el missatge UPDATE directament sense esperar assumint que si ha arribat a aquest punt tot ha anat bé en la reserva de recursos en la seva xarxa d'accés.

p) 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. No obstant això, aquest missatge de resposta portarà amb si la capçalera SDP amb les condicions negociades de QoS:

- Mode *pull*: si el procés de reserva de recursos iniciats en rebre el PRACK encara no ha finalitzat inclourà en la capçalera SDP l'atribut *a=curr: qos local none*. Amb això dóna a entendre a l'UE 1 que tan aviat com aquests recursos ja estiguin reservats en la seva xarxa d'accés enviarà una resposta 180 Ringing, per notificar que el telèfon de l'UE 2 està sonant (i per tant, tots els recursos ja estan reservats al llarg de tot el camí).
- Mode *push*: l'UE 2 pot assumir que, arribat a aquest punt, el procés de reserva de recursos ja ha estat completat, i per tant envia el 200 OK i seguidament el 180 Ringing.

El 200 OK en resposta a l'UPDATE viatja fins a l'UE 1 per notificar-li la recepció d'aquest.

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

r) 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 truca estarà a l'espera que l'usuari destinació decideixi acceptar o rebutjar la trucada.

s) Pas 19: l'usuari a qui s'ha 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.

t) Pas 20: l'UE 1 contesta amb un SIP ACK final i confirma la recepció del 200 OK.

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

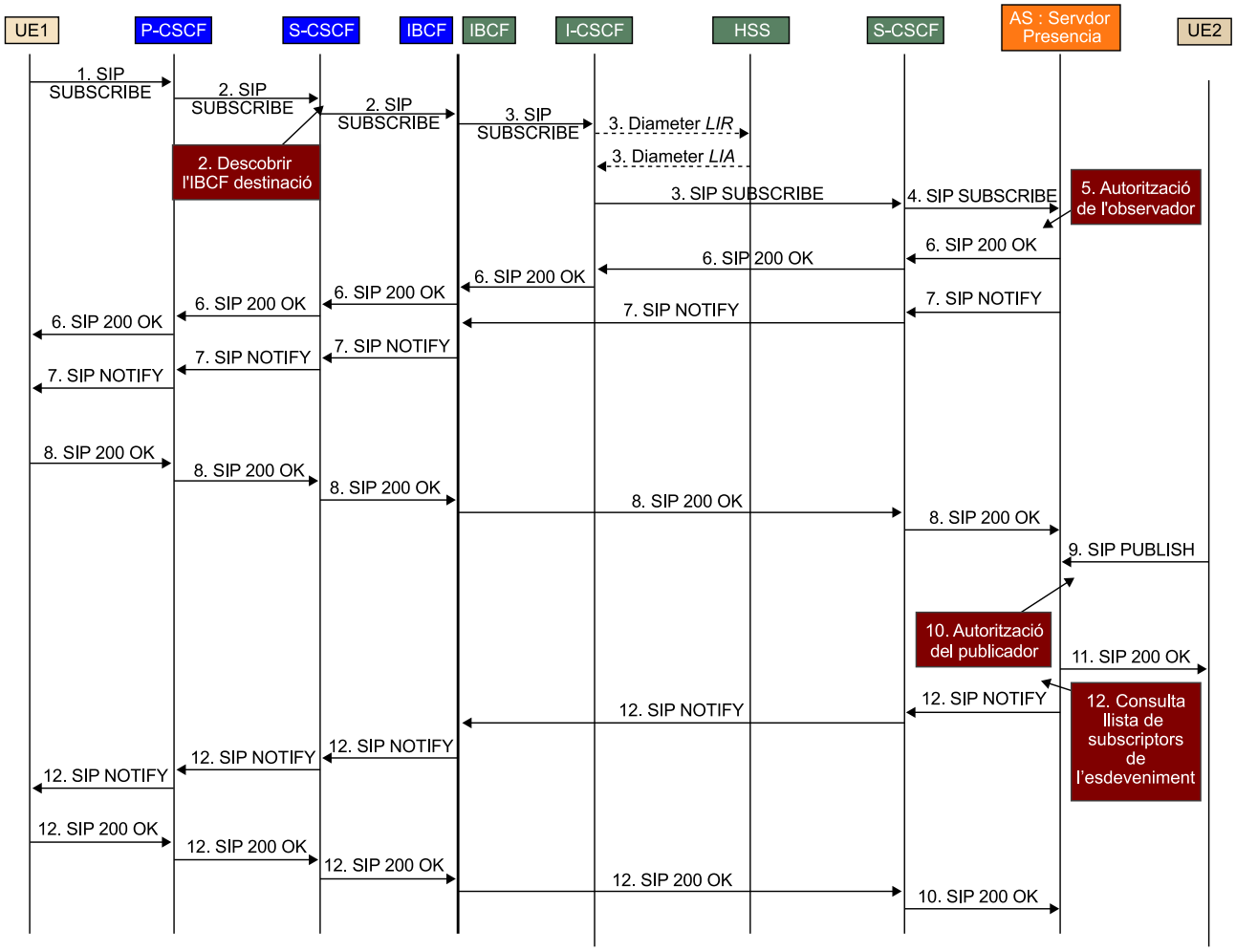
Nota

Fixeu-vos que si l'usuari a qui s'ha trucat accepta el que truca els recursos ja estarien assignats i es podria procedir a l'enviament de fluxos de veu RTP sense dilació. Si el rebutja, provocaria l'enviament d'una resposta SIP 603 Decline cap a l'UE 1, que provocaria l'alliberament immediat de tots els recursos reservats en totes dues xarxes d'accés.

4.2.2. 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, a partir de la figura 23, pas per pas els missatges involucrats en aquest servei.

Figura 23. Flux de missatges SIP en servei de presència



a) Pas 1: l'UE envia un missatge SIP SUBSCRIBE en el qual inclou en la capçalera SIP el camp *Event:*, en què indica 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 per seguir (*Route:*) per al missatge SIP i indica el P-CSCF i S-CSCF assignats.

b) 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. Aquest 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 reenviar el SIP SUBSCRIBE.

c) Pas 3: el missatge arriba finalment a l'I-CSCF del domini que allotja l'AS i aquest sol·licita a l'HSS (intercanvi de missatges Diameter LIR/LIA) el *hostname* de l'S-CSCF assignat a tal AS.

d) Pas 4: l'S-CSCF reenvia el missatge SUBSCRIBE a l'AS corresponent.

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

f) Pas 6: el 200 OK arriba a l'UE seguint el mateix camí de retorn que el SUBSCRIBE.

g) Pas 7: al moment en què es dóna 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 exceptuant l'I-CSCF.

h) Pas 8: l'UE respon amb un 200 OK a aquest NOTIFY.

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

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

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

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

l) Pas 12: llavors 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).

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 nou marc en el qual els proveïdors de servei 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 i ofereixen interoperabilitat amb xarxes i serveis existents avui dia (XTC/XDSI o telefonia mòbil).

En el segment de les xarxes de transport d'accés com LTE, Wi-Fi, WiMAX o ADSL és on es produeixen casos de contesa entre els equips d'usuari en l'accés a serveis contractats amb capacitat garantida. És per això que en aquestes xarxes es requereix més control dels recursos.

A pesar que la tecnologia relacionada amb cada xarxa d'accés (sense fil i cablada) és molt particular (tant en mecanismes d'adhesió a la xarxa i assignació d'adreça IP, com de sol·licitud de recursos) les diferents entitats d'estandardització governamentals han volgut oferir un model de referència avançat en la gestió de recursos que desvinculi en tant que sigui possible aquests dos aspectes:

- Els paràmetres de QoS i SLA (acords contractuals a escala d'aplicació) dels serveis.

- Aspectes concrets de la tecnologia en capa 2 de la xarxa de transport (accés i troncal).

En **la capa de transport**, independentment del model de referència, sempre s'identifica una **subcapa de processament de transport** en la qual s'implementen els mecanismes de garantia de QoS (aplicació de polítiques de QoS particulars a cada usuari) i els d'assignació de recursos (tant en termes de capacitat en bits per segon com en ús d'adreçament IP públic en NAT o NAPT). Posteriorment s'identifica una **subcapa de control de transport** en la qual es troba la intel·ligència en el control d'accés a la xarxa de transport i els seus recursos. En aquesta subcapa es distingeixen dos grans grups de funcions: les que gestionen l'adhesió a la xarxa d'accés de l'UE i les que gestionen les sol·licituds de recursos de QoS de l'UE o de la capa de servei mateixa.

En aquests models de referència es descriuen blocs o entitats funcionals i punts de referència o interfícies que els interconnecten. Les entitats funcionals es descriuen amb unes funcions concretes segons el model de referència. Els punts de referència es descriuen per la informació o paràmetres que

intercanvia cada entitat funcional amb la seva entitat adjacent. Els punts de referència poden ser implementats amb protocols concrets. Les entitats d'estandardització recomanen una llista de protocols per a facilitar la implementació dels punts de referència.

Dins de la tasca d'especificació, entitats com el 3GPP, ETSI-TISPAN i la ITU-T han contribuït molt activament a proporcionar models de referència per a les diferents subcapes. En la taula següent es resumeix la nomenclatura de les entitats funcionals més importants d'aquests models per a les xarxes de transport.

Taula 3. Taula resum d'entitats funcionals de models de referència NGN per a capa de transport

		ITU-T	ETSI-TISPAN	3GPP
Subcapa de processament de transport	Control d'accés, traducció d'adreçament i ports	PE-FE	BGF	PCEF
	Aplicació de polítiques d'assignació de recursos.	TRE-FE	RCEF	
Subcapa de control de Transport	Adhesió a la xarxa d'accés	NACF	NASS	(LTE) MME/SPR
	Control d'Admissió i Recursos	RACF	RACS	PCRF
	Punt de Decisió Final	PD-FE	SPDF	
	Control d'Admissió de Perfil d'Usuari i Recursos	PD-FE / TRC-FE	A-RACF	
Punts de Referència (Interfícies)	Funció d'Aplicació (AF) ←→ Control d'Admissió i Recursos.	Rs (Diameter)	Gq' (Diameter)	Rx (Diameter)
	Punt decisió final ←→ Control Admissió de Perfil i Recursos	Rt (Diameter)	Rq (Diameter)	
	Control d'Admissió de Perfil d'Usuari i Recursos ←→ subcapa de Processament de Transport (Aplicació de polítiques d'assignació de recursos)	Rn (sense especificar), Rc (SNMP o COPS)	Re (Diameter)	Gx (Diameter)
	Punt decisió final ←→ subcapa de Processament de Transport (Control d'accés, traducció d'adreçament i ports)	Rw (Diameter o H.248)	Ia (H.248)	
	Adhesió a la xarxa d'accés ←→ Control d'Admissió i recursos	Ru (Diameter)	e4 (Diameter)	Sp (Diameter)

Per a implementar els interfícies que es defineixen en la taula anterior, les diferents entitats d'estandardització proposen una sèrie de protocols, incloent-hi els missatges que s'han d'utilitzar i els seus paràmetres respectius. Veiem que el protocol predominant és el Diameter, compost per una sèrie de missatges (o també anomenats *ordres*), els quals estan formats per parells d'atributs-valors (o AVP), que contenen informació variada que afecten la descripció de sol·licitud de QoS.

Respecte a la **capa de servei**, les diferents entitats d'estandardització defineixen els seus propis subsistemes o components per a definir els serveis multimèdia que requereixen garantia de QoS d'extrem a extrem. No obstant això, hi ha un subsistema comú en totes les entitats, el que defineix el nucli IMS, el qual va ser definit pel 3GPP i adoptat com a part dels models de referència de la capa de servei per la resta d'entitats d'estandardització.

El **nucli IMS** 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 en una segona part d'elements d'emmagatzematge d'informació de subscripció d'usuari a escala 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, videoconferència o IPTV) i servir-se d'altres protocols encapsulats en la senyalització SIP mateixa, com per exemple SDP, que s'usa per a negociar paràmetres de QoS d'extrem a extrem amb l'altre usuari (veu o videoconferència) o servidor d'aplicació o AS (IPTV).

A part de serveis multimèdia, IMS permet altres serveis sense components de trànsit multimèdia però igualment importants, com missatgeria instantània o presència.

Els elements que componen les funcions d'usuari, la capa de servei i la capa de transport col·laboren i intercanvien informació per a establir sessions de serveis i garantir els recursos necessaris. En aquesta col·laboració, es defineixen dos tipus de mecanismes segons qui dispari la reserva de recursos en la capa de transport. En el mode *push*, l'AF (en aquest cas el nucli IMS) inicia la reserva per mitjà d'un únic punt de contacte amb la capa de transport (usant interfícies Rs, Rx o Gq') i el mode *pull*, en què és la xarxa d'accés mateixa la que sol·licita aquests recursos a la subcapa de processament de transport.

Les xarxes NGN plantegen un nou marc en el qual no solament s'ofereixen els serveis presents actualment (veu, TV, missatgeria, etc.), sinó que deixen el terreny preparat per a la inclusió de nous serveis futurs sense necessitat de fer un canvi arquitectural i tecnològic en les xarxes de transport (amb els costos que això comportaria).

Exercicis d'autoavaluació

1. Un subscriptor A disposa al seu domicili d'un PC amb programari multimèdia (client IMS) i també una TV amb capacitat d'IPTV (client IMS amb connectivitat LAN). A més disposa d'un fax que funciona amb línia telefònica tradicional. Aquest subscriptor ha decidit acceptar l'oferta d'un operador amb infraestructura IMS. Implica la instal·lació d'una passarel·la residencial a través de la seva connexió ADSL existent. Responeu les preguntes següents:

a) Des del punt de vista de la xarxa d'accés, què representa l'equip d'usuari o UE?

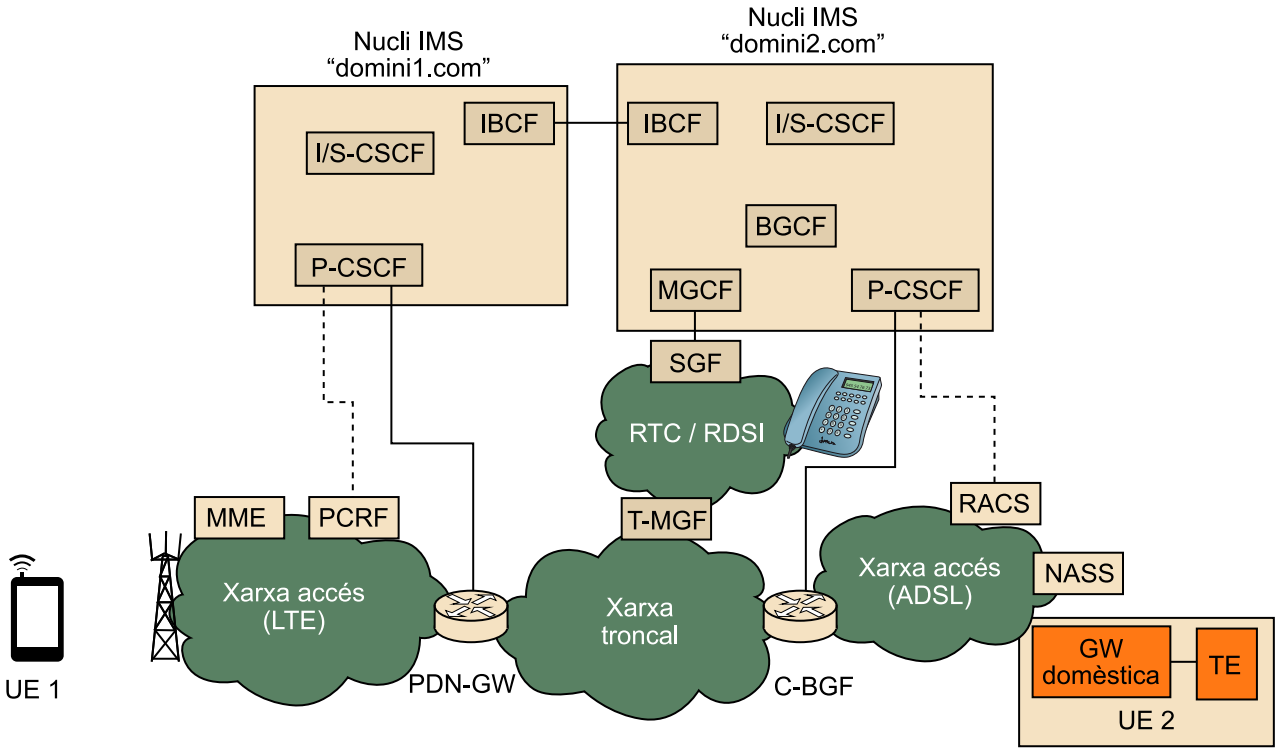
b) A escala d'assignació d'adhesió a la xarxa, quin paper creieu que pot tenir la passarel·la residencial?

c) Com s'integra el fax en aquest entorn i quin impacte tindria en l'estructura funcional de la passarel·la residencial?

d) Quines alternatives ofereix IMS a l'ús d'un fax analògic?

2. Donat el diagrama següent:

Figura 24. Diagrama de l'exercici 2



Tenim un UE 1 registrat en el nucli IMS del domini1.com (amb dos IMPU: usuari1@domini1.com i 674876321@domini1.com) i un UE 2 registrat en el nucli IMS del domini2.com (amb un IMPU: usuari2@domini2.com). En aquest últim cas, la seva adreça IP és privada (l'assignada a la passarel·la residencial). Contesteu les preguntes següents:

a) L'UE 1 fa una trucada de veu a l'UE 2. Identifiqueu i mostreu el recorregut que fan la senyalització SIP IMS i els fluxos RTP en aquesta trucada.

b) Identifiqueu els punts crítics en què cal aplicar polítiques de QoS per a garantir la qualitat de servei de la trucada anterior.

c) L'UE 1 fa una segona trucada cap a un terminal d'XDSI amb número de destinació 934112233. Identifiqueu i mostreu el recorregut de la senyalització i els fluxos RTP. Quin número de telèfon veurà l'usuari que rep la trucada?

d) Per a les dues xarxes d'accés que apareixen en el diagrama, quin model de reserva de recursos creieu que pot tenir cadascun: *push* o *pull*?

3. Vegem el cas de la itinerància centrant-nos en el model de referència de la ITU-T. Responeu les preguntes següents:

a) Un usuari arriba amb un terminal sense fil a un tercer país. Imaginem que l'operador d'aquesta xarxa té un acord d'itinerància amb l'operador original. En engegar-lo, la xarxa d'accés (de tecnologia compatible amb el terminal) li sol·licita autenticació explícita per mitjà dels mecanismes propis de la xarxa d'accés mateixa en capa 2. Descriviu les interaccions entre l'UE i els diferents blocs que componen el NACF visitat i el local per a aconseguir que aquest UE s'autentiqui i aconsegueixi l'adreçament IP, sense oblidar la interacció amb el RACF.

b) Una vegada l'UE ha obtingut l'adreçament IP, inicia la invocació dels serveis IMS per mitjà del seu client. L'operador de la xarxa visitada no disposa d'interconnexió en el seu propi nucli IMS. Especifiqueu almenys un escenari d'itinerància en el qual intervingui algun mecanisme de reserva de recursos en la xarxa visitada.

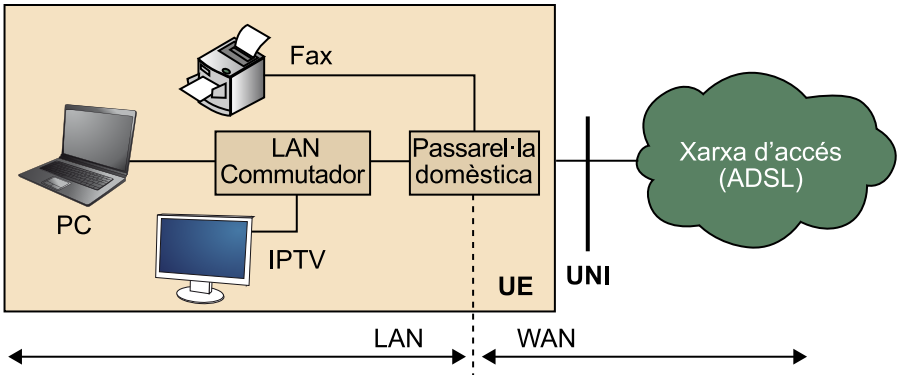
c) Imaginem aquesta vegada que l'UE està en una xarxa visitada operada per un operador i que posseeix interconnexió amb un nucli IMS de domini "visiteddomain.com". L'UE vol accedir a un servei IMS d'IPTV (Application Function) que solament és proporcionat via el nucli IMS de "homedomain.com". Com es fa la interconnexió entre les xarxes de tots dos operadors (visiteddomain.com i homedomain.com)?

Solucionari

Exercicis d'autoavaluació

1. a) L'UE estaria format per la passarel·la residencial mateixa juntament amb tots els equips connectats després d'aquesta (PC, IPTV i fax).

Figura 25. Solucionari de l'exercici 1a



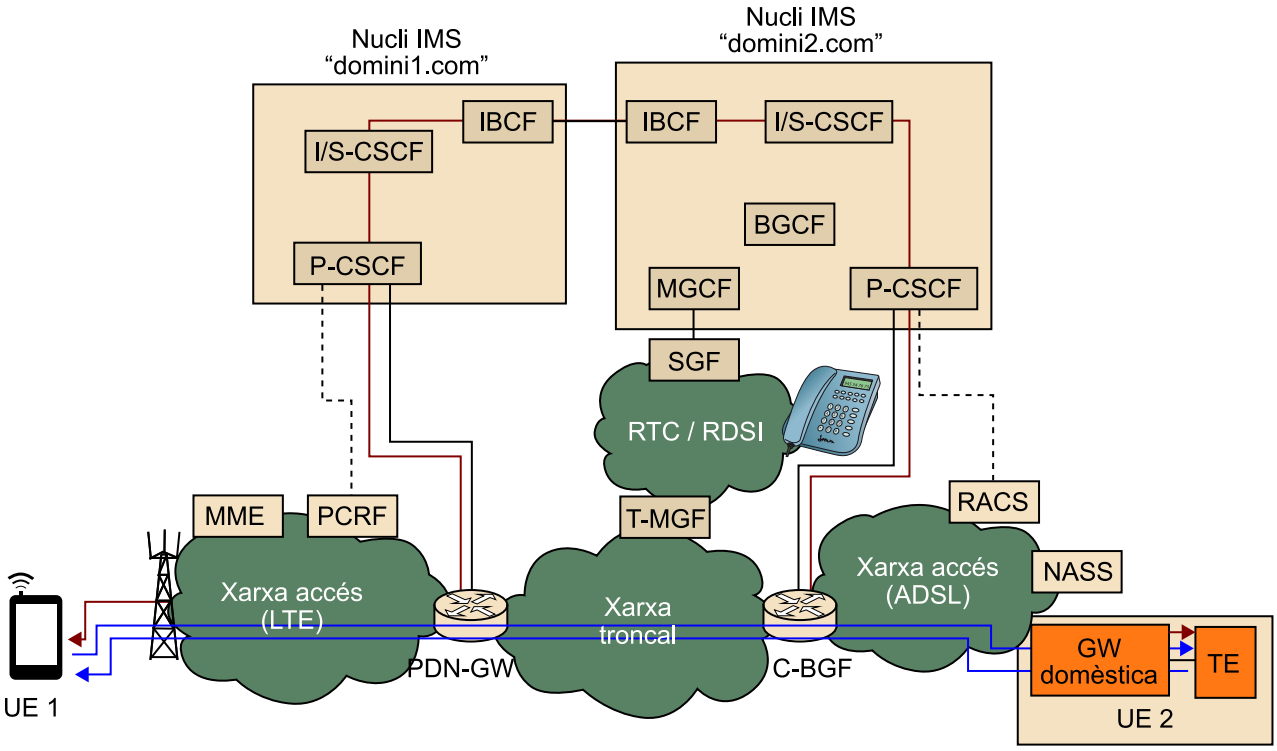
b) En el procés d'adhesió a la xarxa, s'observen dues zones separades per la passarel·la residencial: la zona LAN, on estan connectats tots els dispositius, i la zona WAN, que interconnecta la passarel·la amb la xarxa d'accés. A escala d'autenticació, la passarel·la pot fer pel costat WAN la seva pròpia autenticació contra la xarxa d'accés usant el seu ISIM amb informació d'autenticació del subscriptor. Pel costat LAN pot participar en l'autenticació dels dispositius connectats a ella, ja sigui autenticant localment els dispositius o, en el cas que un dispositiu disposi de la seva pròpia ISIM, exercint el reenviament dels missatges al NACF o NASS. A escala d'assignació d'adreça IP la passarel·la exerciria de servidor DHCP assignant un rang d'IP privades en el costat LAN. Pel costat WAN, la passarel·la rebria una adreça IP pública assignada pels blocs funcionals corresponents del NASS/NACF. Aquesta IP pública la pot utilitzar per a funcions de NATP.

c) El fax és un dispositiu que no ha de disposar necessàriament de connectivitat LAN. La seva interfície és la mateixa que la d'un telèfon analògic. Llavors, ja tenim un primer impacte en la passarel·la, que ha de disposar de ports FXS perquè es pugui interconnectar aquest fax. A més, la passarel·la ha d'exercir d'intermediari entre aquest dispositiu i la xarxa NGN generant la senyalització SIP (IMS) degudament sincronitzada amb la despenjada del fax per a l'establiment de la trucada amb la xarxa XTC/XDSI passant pels elements del nucli IMS. Es pot dir que compleix part de les funcions que s'assignen a l'AMG-FE de la ITU-T (sense comptar la interconnexió amb AGC-FE) i compleix exactament la funcionalitat de l'R-MGF de l'ETSI-TISPAN. Així doncs, la passarel·la exerceix d'intermediari utilitzant la identitat IMS (un IMPU dedicat per al fax) emmagatzemada en el seu ISIM.

d) IMS ofereix un servei d'interconnexió amb les xarxes XTC/XDSI. L'operador d'aquest és subscriptor, i ha de proporcionar aquesta interconnexió (via el bloc MGCF per a senyalització en l'establiment de trucada i T-MGF/TMG-FE/IMS-MGW per al trànsit útil). Però per a poder invocar aquest servei de fax, el PC hauria de tenir el client de fax degudament integrat amb el client IMS perquè per mitjà de la interfície Gm enviï la senyalització SIP/SDP al nucli IMS.

2. a) El diagrama següent mostra per on va la senyalització IMS (en vermell) i els fluxos RTP (en verd) amb la veu. Es pot apreciar la independència de l'arquitectura per a senyalització SIP i RTP.

Figura 26. Solucionari de l'exercici 2a

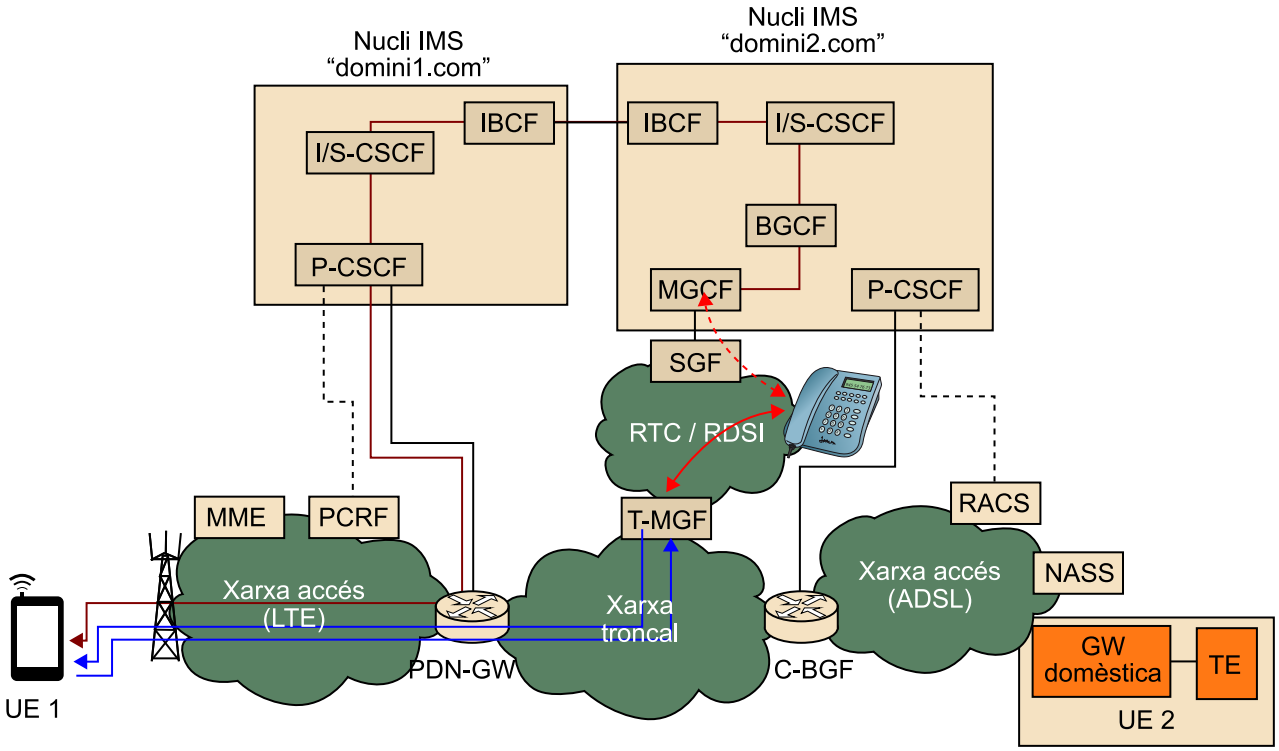


b) En el costat de l'UE 1, el PCRF aplica les regles PCC sobre la PDN-GW, la qual estableix els IP-CAN *bearers* entre l'UE 1 i la PDN-GW. Llavors hi ha un punt per al trànsit en sentit UE 1 → UE 2, on s'han de mapar els fluxos de dades de serveis. Aquest és crític per a introduir els paquets per l'IP-CAN correcte: l'UE 1. La senyalització SIP l'ha de introduir per l'IP-CAN preestablert i dedicat amb QCI explícit per a senyalització IMS i el flux RTP s'ha d'introduir per l'IP-CAN establert dinàmicament per a tal servei. L'altre punt crític en el costat de l'UE 1 és la PDN-GW, en què la senyalització IMS i el flux RTP en sentit UE 2 a UE 1 es mapa als IP-CAN *bearer* correctes (segons el seu QCI).

En el costat de l'UE 2, el RACS aplica les polítiques de servei sobre la xarxa ADSL per garantir la QoS. El RACS configura el C-BGF per possibilitar la traducció NATP per als fluxos RTP entrants i sortints. La passarel·la residencial mateixa també té un paper important en la garantia de QoS en sentit UE 2 → UE 1, ja que es produeix un coll d'ampolla en la seva interfície WAN. És necessari destacar la importància de prioritzar la senyalització IMS per sobre de qualsevol altre trànsit per a evitar retards en l'establiment de la trucada.

c) El diagrama següent mostra per on va la senyalització IMS (en vermell) i els fluxos RTP (en verd) amb la veu. Es pot veure com el nucli IMS del domini1.com no encamina la trucada cap a la seva MGCF sinó que l'encamina al domini2.com perquè aquest la tregui pel seu MGCF. La raó per la qual això és així és arbitrària (polítiques d'encaminament de trucada en el domini1.com).

Figura 27. Solucionari de l'exercici 2c



El número de telèfon que veurà l'usuari en l'XDSI serà el de l'IMPU de l'UE 1: 674876321, ja que és de tipus Tel URI i l'únic compatible amb XDSI.

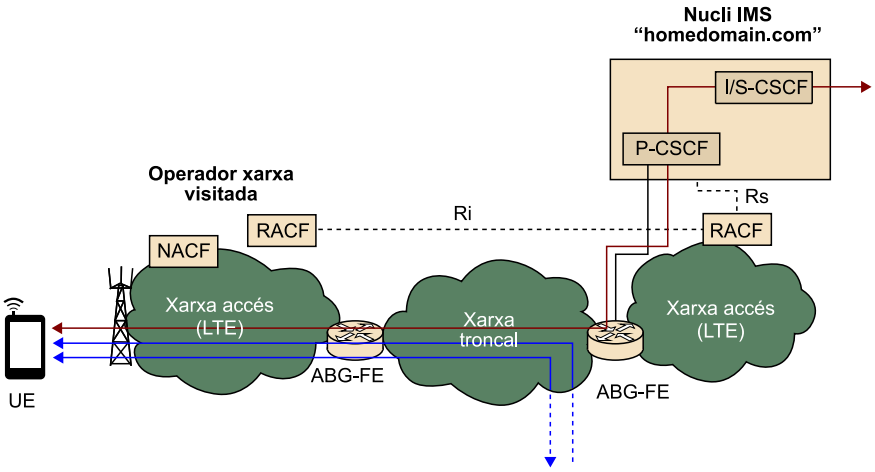
d) La xarxa LTE pot tenir tant *pull* com *push*, depenent de qui inicií l'establiment de l'IP-CAN *bearer*. En canvi, per al cas de l'ADSL veiem més probable que sigui en mode *push*.

3. a) L'UE sol·licita l'establiment d'una connexió en capa 2, que és rebuda per l'AR-FE, el qual reenvia aquesta sol·licitud a l'AM-FE. L'AM-FE detecta aquest intent d'establiment de connexió, de la qual obté els identificadors de canal lògic de capa 2 que l'UE està usant. A més reenvia la petició a la TAA-FE perquè aquest inicií el repte d'autenticació de l'UE. L'UE rep aquest repte i presenta les credencials (IMPI) en la resposta. la TAA-FE de la xarxa visitada detecta (a partir de l'IMPI) que el domini indicat no és el seu. Per tant, la TAA-FE de la xarxa visitada localitza la TAA-FE de la xarxa local (via DNS amb el domini indicat en l'IMPI) i actua com a servidor intermediari per a reenviar el missatge a la TAA-FE local. Per a això utilitza la interfície Ni, que està definida per a tal propòsit. A partir de llavors, el procés d'autenticació es fa entre l'UE i la TAA-FE local passant per la TAA-FE visitada a manera de servidor intermediari. Quan l'usuari ha estat autenticat, la TAA-FE visitada envia la informació de perfil de QoS rebuda de la TAA-FE local a la TLM-FE.

L'UE sol·licita adreçament IP a la NAC-FE visitada, la qual l'hi assigna, i transfereix aquesta informació a la TLM-FE perquè l'associï amb la informació de perfil. Una vegada la TLM-FE té tota aquesta informació, ho bolca al RACF via la interfície Ru.

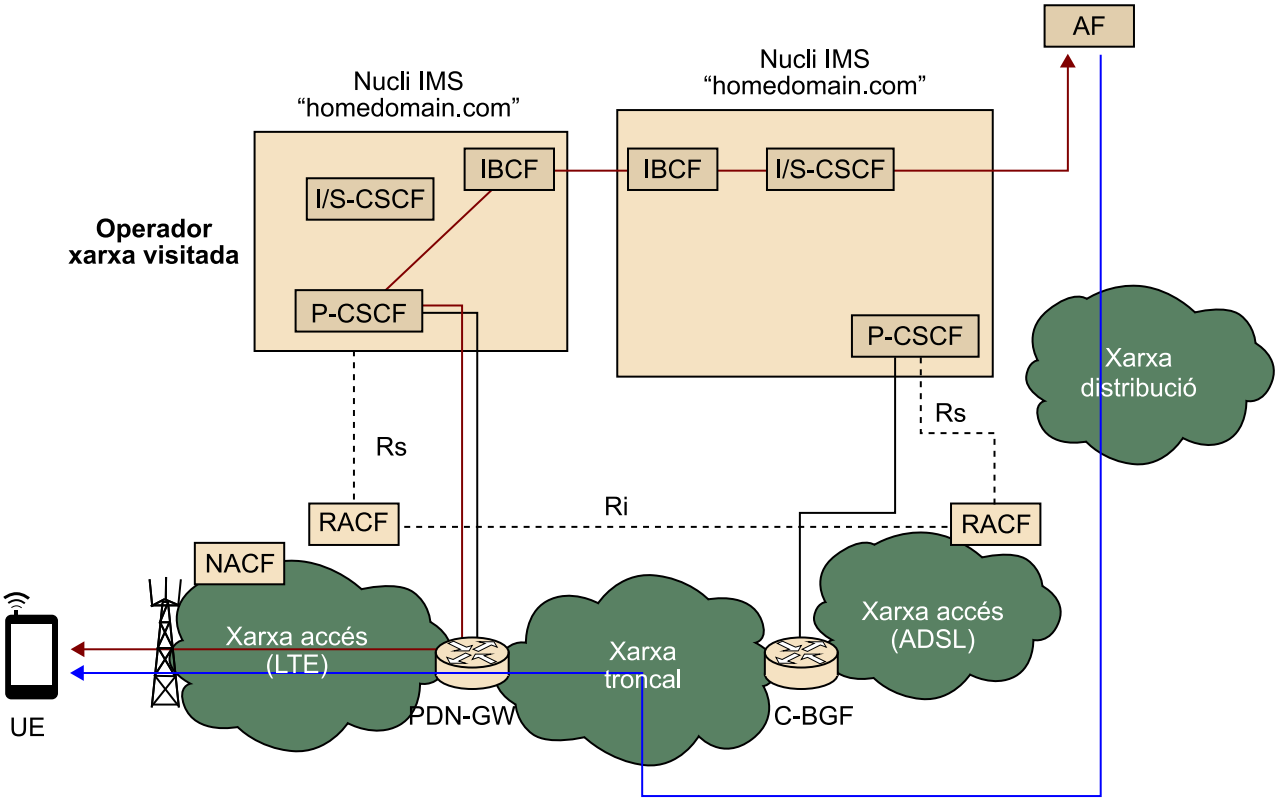
b) La figura següent mostra la interconnexió de tots dos operadors. Cal destacar la interfície Ri, que s'utilitza per a comunicar dues RACF (en realitat, dues PD-FE) entre si de diferents dominis, com és aquest cas. Els missatges SIP arribarien fins al nucli IMS "homedomain.com" per mitjà de la xarxa d'accés LTE de l'operador visitat passant per la xarxa troncal d'interconnexió. Qualsevol petició d'autorització de recursos des del P-CSCF via la interfície Rs seria reenviada des del RACF local fins al visitat per la interfície Ri.

Figura 28. Solucionari de l'exercici 3b



c) En aquest cas, la interconnexió entre totes dues xarxes es podria fer per mitjà dels nuclis IMS mateixos. La senyalització IMS de l'UE viatjaria per la xarxa d'accés visitada fins al nucli IMS visitat (visiteddomain.com) passant pel P-CSCF i l'IBCF directament (sense passar per l'S-CSCF del domini visitat). La interconnexió directa entre P-CSCF i l'IBCF és la interfície Mx. D'aquesta manera la senyalització IMS arriba fins al "homedomain.com", on arriba fins al corresponent S-CSCF (via l'I-CSCF) i d'aquest l'AF. Aquest lliura el contingut (canal de TV) per mitjà d'una xarxa de distribució dedicada a tal fi (línia verda). Ni la xarxa d'accés local ni el RACF local no tenen cap paper. La reserva de recursos a la xarxa visitada es pot fer via el RACF corresponent. El diagrama següent mostra aquesta interconnexió.

Figura 29. Solucionari de l'exercici 3c



Cal esmentar que els IBCF, tant de "visiteddomain.com" com "homedomain.com", poden controlar passarel·les entre xarxes troncals (IBG-FE), on es poden configurar traduccions NAT si fos necessari.

Glossari

3GPP Third Generation Partnership Project. Entitat estandarditzadora de tecnologia mòbil. Entre altres, UMTS i LTE i també IMS.

AAA Authentication, Authorization and Accounting. Protocol de seguretat en xarxes IP.

ABG-FE Access Border Gateway Functional Entity. Funció de passarel·la fronterera amb xarxa d'accés, dins del model de referència de la ITU-T en la subcapa de processament de transport (xarxa troncal).

ADSL Asymmetric Digital Subscriber Line. Tecnologia de la família xDSL en la qual la capacitat de l'enllaç ascendent és inferior que la capacitat de l'enllaç descendent.

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. Element definit per l'ETSI-TISPAN.

AGC-FE Access Gateway Control Functional Entity. Control de passarel·la d'accés en el model de referència de la ITU-T per a la capa de control de servei. Controla una o diverses AMG-FE.

ALG Application Level Gateway. En col·laboració amb un NAT/NATP, és un element que s'encarrega de traduir les adreces IP que es troben en protocols per sobre de la capa 3. Cada protocol necessita el seu ALG (per exemple, FTP ALG o SIP ALG).

AMF Access Management Function. Funció de gestió d'accés en el model de referència del NASS de l'ETSI-TISPAN.

AM-FE Access Management Functional Entity. Funció de gestió d'accés en el model de referència del NACF de la ITU-T.

A-MGF Access Media Gateway Function. Funcionalitat de passarel·la de mitjans amb dispositius d'usuari de telefonia tradicional en el model de referència de l'ETSI-TISPAN per a la subcapa de processament de transport.

AMG-FE Access Media Gateway Functional Entity. Funció de passarel·la de mitjans de xarxa accés dins del model de referència de la ITU-T en la subcapa de processament de transport.

AN-FE Access Node Functional Entity. Funció node d'accés dins del model de referència de la ITU-T en la subcapa de processament de transport.

ARF Access Relay Function. Funció de retransmissió de xarxa d'accés que interactua amb el NASS del model de referència de l'ETSI-TISPAN.

AR-FE Access Relay Functional Entity. Funció retransmissió de xarxa d'accés que interactua amb el NACF del model de referència de la ITU-T.

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

AS Application Server. Element que proveeix un servei en les xarxes NGN.

ATM Asynchronous Transfer Mode. Xarxa de transferència asíncrona.

AUC Authentication Center. En el món de la telefonia mòbil és una base de dades per a controlar els mòbils que es troben en la seva àrea d'influència.

AVP Attribute Value Pair. En el protocol DIAMETER i en un context de xarxes NGN, representen paràmetres que contenen informació sobre una sessió de reserva de recursos.

BBERF *Bearer* Binding and Event Reporting Function. Funció d'associació de *bearers* i informe d'esdeveniments en el model de referència PCC del 3GPP.

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

BGF Border Gateway Function. Funció de passarel·la fronterera, utilitzada en la subcapa de processament de transport en el model de referència de l'ETSI-TISPAN.

BTF Basic Transport Function. Funció bàsica de transport, utilitzada en la subcapa de processament de transport en el model de referència de l'ETSI-TISPAN.

C-BGF Core Border Gateway Function. Funció de passarel·la fronterera entre la xarxa d'accés i la xarxa troncal, utilitzada en la subcapa de processament de transport en el model de referència de l'ETSI-TISPAN.

CD&LC-FE Delivery Control and Location Control Functional Entity. Component de la subcapa de distribució de continguts de la ITU-T que fa la funció de control de lliurament d'informació i de la localització de la distribució del contingut.

CDC-FE Content Delivery Control Functional Entity. Component de la subcapa de distribució de continguts de la ITU-T que fa la funció de control de distribució de continguts.

CDP-FE Content Delivery Processing Functional Entity. Component de la subcapa de distribució de continguts de la ITU-T que fa la funció d'emmagatzematge del contingut, processament d'aquest sota control de la CPR-FE i distribució del contingut a altres instàncies de la CDP-FE sota control del CD&LC-FE.

CGPD-FE Customer Gateway Policy Decision Functional Entity. Element localitzat en la passarel·la residencial per a prendre decisions sobre l'aplicació de polítiques de QoS en col·laboració amb el RACF. Aquesta entitat pertany al model de referència de la ITU-T.

CGPE-FE Customer Gateway Policy Enforcement Functional Entity. Element localitzat en la passarel·la residencial per a instal·lar polítiques de QoS des del RACF. Aquesta entitat pertany al model de referència de la ITU-T.

CLF Connectivity Session Location and Repository Function. Funció de gestió de localització en transport (xarxa d'accés) en el model de referència del NASS de l'ETSI-TISPAN.

CNGCF Customer Network Gateway Configuration Function. Funció de configuració remota de la passarel·la residencial dins del model de referència del NASS de l'ETSI-TISPAN.

COPS Common Open Policy Service. Especifica un model simple client/servidor definit per l'IETF per a suportar el control de polítiques sobre els protocols de senyalització de QoS.

CPE Customer Premises Equipment. Equip dispositiu de client.

DHCP Dynamic Host Configuration Protocol. Protocol de control de *host* dinàmic.

DIAMETER Evolució del protocol RADIUS per al desenvolupament d'aplicacions d'AAA.

DiffServ Serveis Diferenciats. Arquitectura de QoS en IP basada a donar un tracte diferenciat als paquets segons unes classes de servei prèviament fixades.

DNS Domain Name Server. Servidor de resolució de noms de *host* a adreça IP.

ECF Elementary Control Function. Funció de control elemental dins del model de referència de l'ETSI-TISPAN en la subcapa de control de transport.

EC-FE Elementary Control Functional Entity. Funció de control elemental dins del model de referència de la ITU-T en la subcapa de control de transport.

E-CSCF Emergency Call Session Control Function. Component del nucli IMS que exerceix d'element que processa una trucada IMS d'emergència. És un element definit pel 3GPP.

EFF Elementary Forwarding Functionl. Funció de transferència elemental dins del model de referència de l'ETSI-TISPAN en la subcapa de processament de transport.

EF-FE Elementary Forwarding Functional Entity. Funció de transferència elemental dins del model de referència de la ITU-T en la subcapa de processament de transport.

ENUM E.164 Numbering Mapping. Mapatge d'un número de telèfon amb identificadors equivalents de telefonia a Internet.

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

EPS Evolved Packet System. Model de referència del 3GPP per a la capa de transport tant en la part de xarxa troncal (EPC) com de xarxa 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 del 3GPP).

ET Terminal Equipment. Terminal d'usuari.

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. http://www.etsi.org

E-UTRAN Evolved UMTS Terrestrial Radio Access. Definició de la xarxa de ràdio d'LTE segons el 3GPP.

FP Flow Point. Punt de flux d'entrada i sortida de paquets.

GBR Guaranteed Bit Rate. Taxa garantida de bit (usat com a paràmetre de caracterització dels IP-CAN *bearer*).

GERAN GSM Edge Radio Access. Definició de la xarxa ràdio de GPRS segons el 3GPP.

GPRS General Packet Radio Service. És una extensió del GSM per a la transmissió per paquets que permet velocitats de transferència de 56 a 144 kb/s.

GSC-FE General Services Control Functional Entity. En el model de referència de la ITU-T per a la subcapa de control de serveis aquest element proporciona una plataforma que dóna suport als futurs serveis que es plantegin sobre xarxes de paquets.

GSM Global System for Mobile Communications. Estàndard de telefonia mòbil de segona generació.

GTP GPRS Tunneling Protocol. Protocol de tunelització IP usat en GPRS per al transport de paquets IP.

HDC-FE Handover Decision Control Functional Entity. Funció de control de decisió de traspàs de xarxa dins del model de referència de l'MMCF de la ITU-T en la subcapa de control de transport.

HGWC-FE Home Gateway Configuration Functional Entity. Funció de configuració remota de la passarel·la residencial dins del model de referència del NACF de la ITU-T.

HLR Home Location Register. En món de la telefonia mòbil és una 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 a escala de servei (model de referència del 3GPP).

HTTP Digest Mecanisme d'autenticació que utilitza MD5 com a *hash* i que és usat en autenticació en serveis web.

IBCF Interconnection Border Control Function. Funció de control de passarel·la fronterera amb una altra xarxa de troncal, dins del model de referència del 3GPP i de l'ETSI-TISPAN en el nucli IMS.

IBGC-FE Interconnection Border Gateway Control Functional Entity. Funció de control de passarel·la fronterera amb una altra xarxa de troncal, dins del model de referència de la ITU-T en la subcapa de control de servei (xarxa troncal).

I-BGF Interconnection Border Gateway Function. Funció de de passarel·la fronterera entre dues xarxes troncals, utilitzada en la subcapa de processament de transport en el model de referència de l'ETSI-TISPAN.

IBG-FE Interconnection Border Gateway Functional Entity. Funció de passarel·la fronterera amb una altra xarxa de troncal, dins del model de referència de la ITU-T en la subcapa de processament de transport (xarxa troncal).

I-CSCF Interrogating Call Session Control Function. Component del nucli IMS que exerceix d'element d'encaminador de la senyalització SIP cap a l'S-CSCF correcte dins del seu mateix domini. És un element definit pel 3GPP.

I-CSC-FE Interrogating Call Session Control Functional Entity. Component equivalent a l'I-CSCF del 3GPP però en el model equivalent de la ITU-T.

IETF Internet Engineering Task Force. Entitat d'estandardització oberta responsable de la millora dels protocols i els estàndards que defineixen la tecnologia d'Internet.
http://www.ietf.org

IMPI IP Multimedia Private Identity. Representa la identitat privada d'un usuari.

IMPU IP Multimedia Public Identity. Representa la identitat pública d'un usuari.

IMS IP Multimedia Subsystem. Estàndard definit pel 3GPP per a la provisió de serveis multimèdia en telefonia mòbil basat en els protocols definits per l'IETF, com SIP, RTP o DIAMETER.

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

IMS SSO IMS Single Sign-On. És un procediment d'autenticació que habilita l'usuari per a accedir a diversos sistemes amb una sola instància d'identificació.

IMS-MGF IMS Media Gateway Function. Funcionalitat de passarel·la de mitjans amb enllaços de xarxa troncal de telefonia tradicional en el model de referència del 3GPP per a la subcapa de processament de transport.

IntServ Serveis Integrats. Arquitectura de QoS en IP basada en la reserva de recursos individualitzada per a cada servei.

IP Internet Protocol.

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

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

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 *smart card* amb informació sobre la identitat d'un usuari IMS.

ISUP Protocol de circuits commutats, usat per a configurar, manejar i gestionar trucades de veu i dades sobre XTC i XDSI.

ITU-T International Telecommunications Union-Telecommunication. Sector de normalització de les telecomunicacions de la 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.

IWF Interworking Function. Element del model de referència de l'ETSI-TISPAN en la capa de control de servei la funció del qual és adaptar o traduir la senyalització de peticions SIP cap a altres que no suporten el protocol SIP d'IMS.

L2HCF Layer 2 Handover Control Function Entity. Funció de control de la mobilitat en capa 2 dins de l'MMFC en el model de referència de la ITU-T.

L2HE-FE Layer 2 Handover Execution Function Entity. Funció d'execució de la mobilitat en capa 2 en el model de referència de la ITU-T per al processament de transport.

L3HCF Layer 3 Handover Control Function Entity. Funció de control de la mobilitat en capa 3 dins de l'MMFC en el model de referència de la ITU-T.

L3HEF Layer 3 Handover Execution Function. Funció d'execució de la mobilitat en capa 3 en el model de referència de la ITU-T per al processament de transport.

LTE Long Term Evolution. Definida pel 3GPP, es considera la telefonia de 4G.

MAC Medium Access Control. Control d'Accés al Medi (capa 2).

MBR Maximum Bit Rate. Taxa de bit màxima (usat com a paràmetre de caracterització dels IP-CAN *bearer*).

MGCF Media Gateway Control Function. Funció de control de passarel·la de mitjans en el model de referència del 3GPP i l'ETSI-TISPAN en el nucli IMS.

MGC-FE Media Gateway Control Functional Entity. Funció de control de passarel·la de mitjans en el model de referència de la ITU-T en el control de transport.

MGF Media Gateway Function. Funcionalitat de passarel·la de mitjans amb xarxes de circuits tradicionals en el model de referència de l'ETSI-TISPAN per a la subcapa de processament de transport.

MLM-FE Mobile Location Management Functional Entity. Funció de gestió de localització mòbil dins de l'MMFC del model de referència de la ITU-T en la subcapa de control de transport.

MMCF Mobility Management Control Function. Funció de control de la gestió de la mobilitat en el model de referència de la ITU-T.

MME Mobility Management Entity. Entitat que gestiona la mobilitat dels terminals d'usuari en la xarxa ràdio del model EPS (model de referència del 3GPP).

MPLS Multi-Protocol Label Switching. Tecnologia que combina els avantatges de l'encaminament de nivell 3 amb la ràpida commutació de nivell 2, utilitzant la commutació de paquets per a una etiqueta de longitud fixa.

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

MRB-FE Multimedia Resource Broker Functional Entity. Funció de gestió de recursos de mitjans en el model de la ITU-T en la subcapa de suport a serveis i a aplicacions.

MRC-FE Media Resource Control Functional Entity. Funció de control de recursos de mitjans en el model de referència de la ITU-T en el control de transport.

MRFC Media Resource Function Control. Funció de control de recursos de mitjans en el model de referència del 3GPP i ETSI-TIPAN en el nucli IMS.

MRFP Media Resource Function Processor. Funció de processament de recursos de mitjans en el model de referència de l'ETSI-TISPAN i del 3GPP en el processament de transport.

MRP-FE Media Resource Processing Functional Entity. Funció de processament de recursos de mitjans en el model de referència de la ITU-T en el processament de transport.

MSC Mobile Switching Center. Central de commutació mòbil. Element de telefonia mòbil GSM.

NACF (ETSI) Network Access Configuration Function. Funció d'assignació d'adreçament IP a la xarxa d'accés en el model de referència del NASS de l'ETSI-TISPAN.

NACF (ITU-T) Network Attachment Control Function. Conjunt de funcions que defineixen l'adhesió a la xarxa d'accés en el model de referència de la ITU-T.

NAC-FE Network Access Configuration Functional Entity. Funció d'assignació d'adreçament IP a la xarxa d'accés en el model de referència del NACF de la ITU-T.

NAPT Network Address and Port Translation. Traducció de ports i adreçament IP.

NASS Network Attachment Subsystem. Conjunt de funcions que defineixen l'adhesió a la xarxa d'accés en el model de referència de l'ETSI-TISPAN.

NAT Network Address Translation. Traducció d'adreçament IP entre un adreçament privat i un altre de públic.

NGN Next Generation Networks. Xarxes de propera generació.

NID-FE Network Information Distribution Functional Entity. Funció de distribució d'informació de xarxa dins de l'MMFC en el model de referència de la ITU-T.

NIR-FE Network Information Repository Functional Entity. Funció d'emmagatzematge d'informació de xarxa dins de l'MMFC en el model de referència de la ITU-T.

NNI Network-Network Interface. Defineix la frontera entre dues xarxes diferents (dues xarxes troncals o una xarxa troncal i una xarxa d'accés).

NSIW-FE Network Signalling Interworking Funcional Entity. Element del model de referència de la ITU-T en la capa de control de servei la funció del qual és adaptar o traduir la senyalització de peticions SIP cap a altres que no suporten el protocol SIP d'IMS.

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

OFCS Off-line Charging System. Sistema de control de facturació diferit, per a la generació posterior de les factures d'ús d'un servei. Element dins del model de referència PCC del 3GPP.

OFDMA Orthogonal Frequency-Division Multiple Access. Versió multiusuari de la Multiplexació per Divisió de Freqüències Ortogonals o OFDM.

OSPF Open Shortest Path First. Protocol d'encaminament IP dinàmic basat en vector de cost.

PCC Policy Control and Charging. Control de les polítiques de QoS i de facturació, definides en el model de referència del 3GPP per al control de la xarxa de transport.

PCEF Policy and Charging Enforcement Function. Funció d'aplicació de polítiques i facturació en el model de referència PCC del 3GPP.

PCRF Policy Charging and Rules Function. Grups de funcions que conformen el control d'admissió i recursos del model de referència PCC del 3GPP.

P-CSCF Proxy Call Session Control Function. Component del nucli IMS que exerceix d'element fronterer amb l'equip d'usuari a escala de senyalització SIP (IMS). És un element definit pel 3GPP.

P-CSC-FE Proxy Call Session Control Functional Entity. Component equivalent al P-CSCF del 3GPP però en el model equivalent de la ITU-T.

PDBF Profile Data Base Function. Entitat que emmagatzema els perfils d'usuari en el nivell de xarxa de transport en el model de referència del NASS de l'ETSI-TISPAN.

PD-FE Policy Decision Functional Entity. Funció de decisió de polítiques dins del model de referència de la ITU-T en la subcapa de control de transport.

PDN GW Packet Data Network Gateway. Element de l'EPC frontera que interconnecta amb la xarxa troncal d'un altre operador.

PE-FE Policy Enforcement Functional Entity. Funció d'aplicació de polítiques dins del model de referència de la ITU-T en la subcapa de processament de transport.

PPP Point to Point Protocol. Protocol de capa 2 de punt a punt.

PPPoE PPP over Ethernet. Protocol PPP sobre Ethernet.

PSI Public Service Identifier. És un identificador de servei públic que identifica qualsevol element de destinació d'una trucada SIP i que no és un usuari.

QCI QoS Class Identifier. Paràmetre que defineix el comportament de QoS del trànsit associat a un *bearer* d'EPS.

QoS Terme que qualifica la qualitat de servei o Quality of Service.

RACF (ITU-T) Resource and Admision Control Function. Grups de funcions que conformen el control d'admissió i recursos del model de referència de la ITU-T.

RACS Resource and Admision Control Subsystem. Grups de funcions que conformen el control d'admissió i recursos del model de referència de l'ETSI-TISPAN.

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

RCEF Resource Control Enforcement Function. Funció d'aplicació de control de recursos i aplicació de polítiques de QoS des del RACS. És un element pertanyent al model de referència de l'ETSI-TISPAN.

RFC Respon a les sigles de Request For Comment i és on es plasmen per escrit els estàndards que defineix l'IETF.

RIP Routing Information Protocol. Protocol d'encaminament IP dinàmic basat en vector distància.

RSVP Resource Reservation Protocol. Protocol de la capa de transport dissenyat per a reservar recursos d'una xarxa sota l'arquitectura de serveis integrats (IntServ).

RTP Real Time Protocol. Protocol basat en UDP per a la transmissió de fluxos multimèdia (àudio, vídeo) en temps real.

SAE System Architecture Evolution. Manera equivalent d'anomenar l'EPS.

SBC Session Border Controller. Element col·locat a les fronteres administratives d'una xarxa gestionada o domini (exemples d'SBC: P-CSCF o IBCF).

SCF Service Control Functions. És la manera com el model de referència de la ITU-T anomena el conglomerat d'entitats funcionals que conformen la capa de control de servei (per exemple, el nucli IMS).

S-CSCF Serving Call Session Control Function. Component del nucli IMS que exerceix de registrador de l'usuari en el nivell 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 de diferent. És un element definit pel 3GPP.

S-CSC-FE Serving Call Session Control Functional Entity. Component equivalent a l'S-CSCF del 3GPP però en el model equivalent de la ITU-T.

SDP Session Description Protocol. Protocol adherit a la senyalització SIP per a negociar paràmetres multimèdia d'establiment de sessió (codificadors o ports UDP on s'envien els fluxos RTP).

SGF Signalling Gateway Function. Funció de passarel·la de senyalització a xarxes de circuits en el model de referència de l'ETSI-TISPAN en el processament de transport.

SG-FE Signalling Gateway Functional Entity. Funció de passarel·la de senyalització a xarxes de circuits en el model de referència de la ITU-T en el processament de transport.

SGSN/GGSN Serving GPRS Support Node/Gateway GPRS Support Node. En una xarxa troncal GPRS l'SGSN s'encarrega de la part de mobilitat del cel·lular a més de donar accés a aquests a la xarxa de dades mòbils, d'autenticar i assignar la qualitat del servei que utilitza cada terminal. El GGSN és la porta d'enllaç o punt central de connexió cap a l'exterior o la PDN (Packet Data Network) d'una xarxa cel·lular (xarxa mòbil), aquestes xarxes externes poden ser Internet o una xarxa corporativa.

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

SIP Session Initiation Protocol. Protocol definit per l'IETF per a l'establiment i negociació de sessions de serveis multimèdia.

SLA Service Level Agreement. Defineix les característiques del servei per a un usuari que és subscriptor.

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

SNMP Simple Network Management Protocol. Protocol per al monitoratge i control remots d'elements de xarxa definit per l'IETF. Està basat en la consulta de bases de dades localitzades en cada dispositiu de xarxa anomenades MIB o Management Information Base.

SPDF Service Policy Decision Function. Funció de decisió de la política de servei dins del RACS en el model de referència de l'ETSI-TISPAN.

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

SS7 Signalling System number 7. Sistema de senyalització núm. 7 usat en els enllaços troncals de telefonia.

SUP-FE Service User Profile Functional Entity. Base de dades que emmagatzema la informació de subscripció d'un usuari juntament amb informació d'autenticació i autorització a escala de servei (model de referència de la ITU-T).

TAA-FE Transport Authentication and Authorization Functional Entity. Funció d'autenticació i autorització en la xarxa de transport (xarxa d'accés) en el model de referència del NACF de la ITU-T.

Taula MAC En un commutador, és la taula en la qual es relaciona el port físic i l'adreça de maquinari (també anomenada *adreça MAC*).

TCP Transport Control Protocol.

TDM Time Division Multiplex.

TDMA Time Division Multiple Access. Repartició de recursos de transmissió per multiplexació de temps.

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 tipologia de la xarxa.

TISPAN TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) i SPAN (Services and Protocols for Advanced Networks). És una organització fundada per l'ETSI per a l'estandardització de xarxes fixes i convergència amb Internet.

TLM-FE Transport Location Management Functional Entity. Funció de gestió de localització en transport (xarxa d'accés) en el model de referència del NACF de la ITU-T.

T-MGF Trunk Media Gateway Function. Funcionalitat de passarel·la de mitjans amb enllaços de xarxa troncal de telefonia tradicional en el model de referència de l'ETSI-TISPAN per a la subcapa de processament de transport.

TMG-FE Trunking Media Gateway Functional Entity. Funció de passarel·la de mitjans de xarxa de circuits dins del model de referència de la ITU-T en la subcapa de processament de transport (xarxa troncal).

ToS Type of Service. Paràmetre que indica el tipus de servei inclòs en la capçalera IP.

TRC-FE Transport Resource Control Functional Entity. Funció de control de recursos de transport dins del model de referència de la ITU-T en la subcapa de control de transport.

TRE-FE Transport Resource Enforcement Functional Entity. Funció d'aplicació de recursos de transport dins del model de referència de la ITU-T en la subcapa de processament de transport.

TrGW Transition Gateway. Funció de passarel·la fronterera entre dues xarxes troncals, utilitzada en la subcapa de processament de transport en el model de referència del 3GPP.

TUP-FE Transport User Profile Functional Entity. Entitat que emmagatzema els perfils d'usuari a escala de xarxa de transport en el model de referència del NACF de la ITU-T.

UAAF User Authentication and Authorization Function. Funció d'autenticació i autorització de l'usuari en la xarxa de transport (xarxa d'accés) en el model de referència del NASS de l'ETSI-TISPAN.

UDP User Datagram Protocol. Protocol de capa 4 per a l'enviament de paquets sense confirmació.

UE Equip d'usuari. Pot contenir un o més TE.

UMTS Universal Mobile Telecommunications System. Sistema universal de telecomunicacions mòbils de tercera generació de la ITU, successor del sistema GSM.

UNI User-Network Interface. Defineix la frontera de l'àmbit estrictament d'usuari i de l'àmbit de la xarxa d'accés o servei.

UPSF User Profile Subscription Function. Base de dades que emmagatzema la informació de subscripció d'un usuari juntament amb informació d'autenticació i autorització a escala de servei (model de referència de l'ETSI-TISPAN).

URI Uniform Resource Identifier. Esquema d'identificació d'usuari.

USIW-FE User Signalling Interworking Funcional Entity. Element del model de referència de la ITU-T en la capa de control de servei la funció del qual és adaptar o traduir la senyalització de tots aquells terminals d'usuari que no suporten el protocol SIP d'IMS.

UTRAN UMTS Terrestrial Radio Access. Definició de la xarxa ràdio d'UMTS segons el 3GPP.

VLAN ID Virtual Local Area Network Identifier. Identificador de xarxa local virtual, utilitzat en un commutador per a dividir-se en diversos commutadors virtuals amb menys boques.

VoIP Voice over IP. Servei de veu que s'ofereix sobre una xarxa de commutació de paquets basada en el protocol.

WiMAX Worldwide Interoperability for Microwave Access. Conjunt d'estàndards de xarxes metropolitanes sense fil de la família IEEE 802.16.

XDSI Xarxa Digital de Serveis Integrats.

xDSL x Digital Subscriber Line. Família de tecnologies d'accés a Internet de banda ampla basades en la digitalització del bucle d'abonat telefònic.

XML eXtensible Markup Language. És un llenguatge de marques desenvolupat pel World Wide Web Consortium (W3C) que permet definir la gramàtica de llenguatges específics per a estructurar documents grans.

x-RACF Resource and Admission Control Function. Funció pertanyent al RACS dins del model de referència de l'ETSI-TISPAN encarregat del control dels recursos de la xarxa de transport (A-RACF s'aplica a la xarxa d'accés i C-RACF a la xarxa troncal).

XTC Xarxa Telefònica Commutada.

Bibliografia

ITU-T Recomendación Y.2012 (04/2010). *Functional requirements and architecture of next generation networks*.

ITU-T Recomendación Y.2014 (03/2010). *Network attachment control functions in next generation networks*.

ETSI-TISPAN Recomendación ES 282 004 v3.4.1 (2010-03). *NASS Functional Architecture*.

ETSI-TISPAN Recomendación TS 183 020 v1.1.1 (2006-03). *NASS - Roaming in TISPAN - Interface Protocol Definition*.

ITU-T Recomendación Y.2111 (11/2011). *Resource and admission control functions in next generation networks*.

ETSI-TISPAN Recomendación ES 282 003 v3.5.1 (2011-04). *RACS Functional Architecture*.

ITU-T Recomendación Y.2018 (09/2009). *Mobility management and control framework and architecture within the NGN transport stratum*.

3GPP Recomendación TS 23.203 v11.5.0 (2012-03). *Policy and charging control architecture*.

ETSI-TISPAN Recomendación ES 282 001 V3.4.1 (2009-09). *NGN Functional Architecture*.

ETSI-TISPAN Recomendación ES 123 517 8.0.0 (2007-12). *IP Multimedia Subsystem*.

3GPP Recomendación TS 23.228 v11.4.0 (2012-03). *IP Multimedia Subsystem (IMS)*.

3GPP Recomendación TS 29.214 v11.0.0 (2011-03). *Policy and Charging Control over Rx reference point*.

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

Annex

Resum de punts de referència del model de referència de la ITU-T

A continuació mostrem un resum de tots els punts de referència que apareixen en l'arquitectura de referència de la ITU-T que s'han mostrat al llarg d'aquest document.

1) Punts de referència del NACF

La taula següent mostra una descripció dels punts de referència que esmenta la ITU-T i la seva recomanació sobre el protocol per a implementar-ho.

Taula 4. Punts de referència del NACF

Nom	Entitats que interconnecta	Protocol	Descripció
T-U1	CPE i AR-FE	<sense especificar>	Utilitzat pel CPE per a iniciar sessió en capa 2.
TC-T1	AR-FE i AM-FE	<sense especificar>	Utilitzat pel NACF per a finalitzar sessió capa 2 i detectar adhesió a la xarxa d'un CPE.
Na	AM-FE i TAA-FE	<sense especificar>	Utilitzat per l'AM-FE per a intercanviar missatges de procés d'autenticació del CPE.
Nd	AM-FE i NAC-FE	<sense especificar>	Utilitzat per l'AM-FE per a intercanviar missatges d'assignació d'adreça IP.
Nb	TAA-FE i TUP-FE	<sense especificar>	Utilitzat pel TAA-FE per a accedir a la base de dades de perfils QoS i credencials.
Ni	TAA-FE (proxy) i TAA-FE	<sense especificar>	Utilitzat pel TAA-FE (proxy) en la xarxa visitada per a accedir a la base de dades de perfils QoS i credencials de la xarxa original.
Nc	TAA-FE i TLM-FE	<sense especificar>	Utilitzat pel TAA-FE per a transferir la informació de subscripció de transport de l'usuari autenticat.
Ne	NAC-FE i TLM-FE	<sense especificar>	Utilitzat pel NAC-FE per a transferir la informació d'assignació d'adreçament IP i paràmetres d'identificació de xarxa d'accés.
Ng	TLM-FE i TLM-FE	Diameter	Utilitzat pel TLM-FE local per a itinerància.
Ru	TLM-FE i PD-FE(RACF)	Diameter	Utilitzat per a transferir informació d'identificació en xarxa d'accés i perfil de QoS de l'usuari al RACF.
Nx	TLM-FE i HGWC-FE	Diameter	Utilitzat per a transferir informació de subscripció i informació de seguretat del TLM-FE a l'HGWC-FE
S-TC1	TLM-FE i Funcions Control Servei (SCF)	Diameter	Utilitzat per l'SCF per a sol·licitar informació de localització de l'usuari, i també reportar a l'SCF esdeveniments relacionats amb l'adhesió de l'usuari a la xarxa.
TC-Ux	HGWC-FE i CPE	<sense especificar>	Utilitzat per al monitoratge i configuració remota de la passarel·la domèstica.
M1	TLM-FE i MLM-FE	<sense especificar>	Utilitzat per a transferir a l'MLM-FE paràmetres de mobilitat.

Nom	Entitats que interconnecta	Protocol	Descripció
M2	TLM-FE i HDC-FE	<sense especificar>	Utilitzat per a transferir a l'HDC-FE paràmetres de mobilitat.
M13	TLM-FE i NID-FE	<sense especificar>	Utilitzat per a transferir al NID-FE paràmetres de mobilitat.

2) Punts de referència del NACF

La taula següent mostra una descripció dels punts de referència que esmenta la ITU-T i la seva recomanació sobre el protocol o protocols per a implementar-ho.

Taula 5. Punts de referència del RACF

Nom	Entitats que interconnecta	Protocol	Descripció
Rs	Funcions de Control de Servei (SCF) i PD-FE	Diameter	Utilitzat per l'SCF per a la sol·licitud de recursos de QoS i informe d'esdeveniments de capa de transport.
Ri	PD-FE i PD-FE	Diameter	Utilitzat per un PD-FE d'un altre domini per a la sol·licitud de recursos de QoS i informe d'esdeveniments de capa de transport al PD-FE. També usat per a itinerància en la reserva de recursos.
Rd	PD-FE i PD-FE	Diameter	Utilitzat per un PD-FE del mateix domini per a la sol·licitud de recursos de QoS i informe d'esdeveniments de capa de transport al PD-FE adjacent.
Rw	PD-FE i PE-FE	Diameter, H.248	Utilitzat pel PD-FE per a instal·lar polítiques de QoS i usat pel PE-FE per a sol·licitar recursos (mode *pull*).
Rt	PD-FE i TRC-FE	Diameter	Utilitzat pel PD-FE per a sol·licitar control d'admissió al TRC-FE sobre disponibilitat de recursos.
Rp	TRC-FE i TRC-FE	Diameter	Utilitzat per un TRC-FE del mateix domini per a la sol·licitud de control d'admissió de recursos al TRC-FE adjacent.
Rn	TRC-FE i TRE-FE	<sense especificar>	Utilitzat pel TRC-FE per a aplicar les decisions del control d'admissió de disponibilitat de recursos.
Rc	TRC-FE i subcapa Processament Transport	COPS, SNMP	Utilitzat pel TRC-FE per a captar informació de topologia i estat de recursos de la xarxa.
Ru	PD-FE i TLM-FE (NACF)	Diameter	Utilitzat pel PD-FE per a obtenir del NACF informació de subscripció.
Ro	PD-FE i HDC-FE (MMCF)	<sense especificar>	Utilitzat per l'HDC-FE per a funcions de mobilitat.
Rm	PD-FE i MPM	<sense especificar>	Utilitzat per a transferir informació de monitoratge a l'MPM.
Rh	PD-FE i CGPE-FE	COPS	Utilitzat per a instal·lar polítiques de QoS en la passarel·la residencial.
Rh'	PD-FE i CGPD-FE	<sense especificar>	Utilitzat per a sol·licitar control d'admissió de recursos en la passarel·la residencial.

3) Punts de referència de l'MMCF

La taula següent mostra una descripció dels punts de referència que esmenta la ITU-T i la seva recomanació sobre el protocol per a implementar-ho.

Taula 6. Punts de referència de l'MMCF

Nom	Entitats que interconnecta	Protocol	Descripció
M1	TLM-FE i MLM-FE	<sense especificar>	Utilitzat per a transferir a l'MLM-FE paràmetres de mobilitat (p. ex., IP temporal assignada).
M2	TLM-FE i HDC-FE	<sense especificar>	Utilitzat per a transferir a l'HDC-FE paràmetres de mobilitat (p. ex., associacions de seguretat amb l'equip d'usuari).
M3	CPE i MLM-FE	<sense especificar>	Utilitzat per a transferir a l'MLM-FE actualitzacions de localització del CPE.
M4	CPE i HDC-FE	<sense especificar>	Utilitzat pel CPE per a notificar esdeveniments de mobilitat i utilitzat per a enviar al CPE ordres des de l'HDC-FE d'indicació de canvi a una altra xarxa.
M5	CPE i NID-FE	<sense especificar>	Utilitzat per a enviar al CPE ordres des del NID-FE d'informació de xarxes candidates.
M6	HDC-FE i L2HE-FE	<sense especificar>	Utilitzat per l'HDC-FE per a executar la transferència en capa 2.
M7	HDC-FE i L3HE-FE	<sense especificar>	Utilitzat per l'HDC-FE per a executar la transferència en capa 3.
M8, Ro	HDC-FE i PD-FE (RACF)	<sense especificar>	Utilitzat per l'HDC-FE per a reservar recursos en la xarxa d'accés quan l'equip d'usuari es mou a una altra xarxa.
M9	MLM-FE i MLM-FE	<sense especificar>	Utilitzat per a intercanviar registres de mobilitat entre dues MLM-FE.
M10	MLM-FE i HDC-FE	<sense especificar>	Utilitzat per a intercanviar indicacions i notificacions de transferència.
M11	HDC-FE i NID-FE	<sense especificar>	Utilitzat per l'HDC-FE per a aconseguir informació sobre altres xarxes d'accés en les quals es fa una transferència.
M12	NID-FE i NIR-FE	<sense especificar>	Utilitzat pel NID-FE per a aconseguir informació sobre altres xarxes d'accés.
M13	TLM-FE i NID-FE	<sense especificar>	Utilitzat per a transferir al NID-FE paràmetres de mobilitat.

Resum de punts de referència del model de referència de l'ETSI-TISPAN

A continuació mostrarem un resum de tots els punts de referència que apareixen en l'arquitectura de referència de l'ETSI-TISPAN que s'han mostrat al llarg d'aquest document.

1) Punts de referència del NASS

La taula següent mostra una descripció dels punts de referència que esmenta l'ETSI-TISPAN per al NASS i la seva recomanació sobre el protocol per a implementar-ho.

Taula 7. Punts de referència del NASS

Nom	Entitats que interconnecta	Protocol	Descripció
e1	UE i ARF i AMF	<sense especificar>	Utilitzat per l'UE per a iniciar sessió en capa 2 i detectar adhesió en la xarxa d'un UE.
a3	AMF i UAAF	<sense especificar>	Utilitzat per l'AMF per a intercanviar missatges de procés d'autenticació de l'UE.
a1	AMF i NACF	<sense especificar>	Utilitzat per l'AMF per a intercanviar missatges d'assignació d'adreça IP.
e5	UAAF (proxy) i UAAF	Radius	Utilitzat per l'UAAF (proxy) en la xarxa visitada per a accedir a la base de dades de perfils QoS i credencials de la xarxa original.
a4	UAAF i CLF	<sense especificar>	Utilitzat per l'UAAF per a transferir la informació de subscripció de transport de l'usuari autenticat.
a2	NACF i CLF	<sense especificar>	Utilitzat pel NACF per a transferir la informació d'assignació d'adreçament IP i paràmetres d'identificació de xarxa d'accés.
e2	CLF i CLF	Diameter	Utilitzat pel CLF local per a itinerància.
e2	CLF i CNGCF	Diameter	Utilitzat per a transferir informació de subscripció i informació de seguretat des del CLF a CNGCF.
e2	CLF i AF	Diameter	Utilitzat per l'AF per a sol·licitar informació de localització de l'usuari, i també reportar a l'AF esdeveniments relacionats amb l'adhesió de l'usuari a la xarxa.
e4	CLF i A-RACF (RACS)	Diameter	Utilitzat per a transferir informació d'identificació en xarxa d'accés i perfil de QoS de l'usuari al RACS.
e3	CNGCF i CNG	<sense especificar>	Utilitzat per al monitoratge i configuració remota de la passarel·la domèstica.

2) Punts de referència del RACS

La taula següent mostra una descripció dels punts de referència que esmenta l'ETSI-TISPAN i la seva recomanació sobre el protocol per a implementar-ho.

Taula 8. Punts de referència del RACF

Nom	Entitats que interconnecta	Protocol	Descripció
Gq'	AF i SPDF	Diameter	Utilitzat per l'AF per a la sol·licitud de recursos de QoS i informe d'esdeveniments de capa de transport.
Ri'	SPDF i SPDF	Diameter	Utilitzat per un SPDF d'un altre domini per a la sol·licitud de recursos de QoS i informe d'esdeveniments de capa de transport a l'SPDF. També usat per a itinerància en la reserva de recursos.
Rd'	SPDF i SPDF	Diameter	Utilitzat per un SPDF del mateix domini per a la sol·licitud de recursos de QoS i informe d'esdeveniments de capa de transport a l'SPDF adjacent.
Ia	SPDF i BGF	H.248	Utilitzat per l'SPDF per a instal·lar polítiques de QoS en el BGF.
Rq	SPDF i x-RACF	Diameter	Utilitzat per l'SPDF per a sol·licitar control d'admissió a l'x-RACF sobre perfil de subscripció i disponibilitat de recursos.

Nom	Entitats que interconnecta	Protocol	Descripció
Rr	x-RACF i x-RACF	Diameter	Utilitzat per un x-RACF del mateix domini per a la sol·licitud de control d'admissió de recursos a l'x-RACF adjacent.
Re	x-RACF i RCEF	Diameter	Utilitzat per l'x-RACF per a aplicar les decisions del control d'admissió de disponibilitat de recursos.
e4	A-RACF i CLF (NASS)	Diameter	Utilitzat per l'A-RACF per a obtenir del NASS informació de subscripció.
Rf	(SPDF, x-RACF) i Funcions de Facturació	Diameter	Utilitzat per a transferir informació de facturació.

3) Punts de referència del model PCC

La taula següent mostra una descripció dels punts de referència que esmenta el 3GPP i la seva recomanació sobre el protocol per a implementar-ho.

Taula 9. Punts de referència del model PCC

Nom	Entitats que interconnecta	Protocol	Descripció
Rx	AF i PCRF	Diameter	Utilitzat per l'AF per a la sol·licitud de recursos de QoS i informe d'esdeveniments de capa de transport.
S9	V-PCRF i H-PCRF	Diameter	Utilitzat per un PCRF d'un altre domini per a la sol·licitud de recursos de QoS (visitat) per a itinerància en la reserva de recursos.
Gx	PCRF i PCEF	Diameter	Utilitzat pel PCRF per a instal·lar les regles PCC (establiment d'IP CAN *bearer* i assignació de fluxos de dades de servei). També usat per a informar d'esdeveniments de capa de transport.
Gxx	PCRF i BBERF	Diameter	Utilitzat pel PCRF per a instal·lar les regles PCC (establiment d'IP CAN *bearer* i assignació de fluxos de dades de servei). També usat per a informar d'esdeveniments de capa de transport.
Sp	PCRF i SPR	Diameter	Utilitzat pel PCRF per a obtenir de l'SPR informació de subscripció.
Gy	PCEF i OCS	Diameter	Utilitzat per a transferir informació de facturació en línia (prepagament).
Gz	PCEF i OFCS	Diameter	Utilitzat per a transferir informació de facturació fora de línia (postpagament).

4) Punts de referència del component IMS

La taula següent mostra una descripció dels punts de referència per al subsistema IMS que s'esmenten en els models de la ITU-T, l'ETSI-TISPAN i el 3GPP i també la recomanació sobre el protocol per a implementar-ho.

Taula 10. Punts de referència del nucli IMS

Nom	Entitats que interconnecta	Protocol	Descripció
Gq', Rx i Rs (S-TC2, S-TC3, S-TC4, S-TC5)	P-CSCF (o IBCF per a l'ETSI) i Control d'Admissió de Recursos (RACF, RACS i PCRF)	Diameter	Utilitzat pel P-CSCF (o també IBCF per l'ETSI) per a la sol·licitud de recursos de QoS i informe d'esdeveniments de capa de transport.

Nom	Entitats que interconnecta	Protocol	Descripció
Gm i S-U1	UE i P-CSCF	SIP	Interfície entre UE i P-CSCF per a intercanviar missatges de senyalització SIP d'IMS (Registre, Control de Sessions i Transaccions).
Mw	Entre CSCF	SIP	Utilitzat pels CSCF per a reenviar-se senyalització SIP de registre o control de sessió (originada des d'un UE o destinada a aquest) entre ells segons els seus criteris d'encaminament.
Mx	CSCF o BGCF i IBCF	SIP	Utilitzat pels CSCF o el BGCF i el o els IBCF per a reenviar-se senyalització SIP de registre o control de sessió quan va destinada a un nucli IMS d'un altre operador o hi ve.
Mr	S-CSCF o MRFC	SIP	Utilitzat per l'S-CSCF quan necessita activar serveis de transport.
Mp, S-T1	MRFC i MRFP (subcapa de Processament de Transport)	H.248	Utilitzat per l'MRFC per a controlar els recursos multimèdia de l'MRFP d'acord amb les demandes de l'AS i l'S-CSCF.
Mi	S-CSCF i BGCF	SIP	Utilitzat per l'S-CSCF quan l'S-CSCF vol redirigir la sessió SIP a una xarxa externa que no és NGN (XTC/XDSI o H323).
Mj	BGCF i MGCF	SIP	Utilitzat pel BGCF per a transferir la sessió SIP una vegada ha seleccionat l'MGCF (passarel·la a XTC/XDSI) pel qual treu aquesta sessió. En aquest cas l'MGCF es troba en el mateix domini que el BGCF.
Mk	BGCF i MGCF (remot)	SIP	Utilitzat pel BGCF per a transferir la sessió SIP una vegada ha seleccionat l'MGCF (passarel·la a XTC/XDSI) pel qual es treu aquesta sessió. En aquest cas l'MGCF es troba en un domini diferent que el BGCF.
Mg	MGCF i I-CSCF o S-CSCF	SIP	Utilitzat per l'MGCF per a reenviar missatges de sessions SIP entrants des d'XTC/XDSI cap a l'I-CSCF o S-CSCF.
Mn, S-T4	MGCF i T-MGF (o IMS-GW segons 3GPP)	H.248	Utilitzat per l'MGCF per a controlar els recursos en canals de veu/vídeo del T-MGF (o IMS-MGF segons 3GPP) en la seva connexió amb la xarxa XTC/XDSI.
Mm (3GPP)	CSCF locals i CSCF remots	SIP	Utilitzat per a reenviar missatges de sessions SIP a altres servidors SIP o xarxes IP externes (altres dominis).
Ma, A-S7	I-CSCF i AS	SIP	Utilitzat per l'I-CSCF per a reenviar peticions SIP a l'AS amb serveis públics d'identitats (PSI).
ISC, A-S4	S-CSCF i AS	SIP	Utilitzat per l'S-CSCF i l'AS per a reenviar i rebre peticions SIP.
Cx	S-CSCF o I-CSCF i UPSF	Diameter	Utilitzat per l'S-CSCF i l'I-CSCF per a consultar a l'UPSF informació d'autenticació i autorització d'usuari, perfil de subscripció, localització (S-CSCF assignat).
Dx	S-CSCF o I-CSCF i SLF	Diameter	Utilitzat per l'S-CSCF i l'I-CSCF per a consultar l'SLF sobre la localització de l'UPSF que conté la informació de subscripció d'un usuari.

Nom	Entitats que interconnecta	Protocol	Descripció
Ib (ETSI)	IBCF i IWF	<sense especificar>	Utilitzat per l'IBCF per a sol·licitar a l'IWF la traducció del protocol SIP de sessió a un altre protocol.
Iw (ETSI)	IWF i altres xarxes IP	<sense especificar>	Utilitzat per l'IWF per a la conversió de la senyalització de sessió.
Ic, Ici	IBCF i altres xarxes NGN	SIP	Utilitzat per l'IBCF per a intercomunicar dos dominis IMS. Ici (3GPP) és una especialització de l'Ic.
Ie (ETSI), S-T3 (ITU-T)	MGCF i SGW	<sense especificar>	Utilitzat per l'MGCF per a intercanviar senyalització SS7 sobre IP amb l'SGW.
Ix, S-T5 (ITU-T)	IBCF i TrGW	<sense especificar>	Utilitzat per l'IBCF per a controlar el TrGW (p. ex., controlar les traduccions NAT).
Rc, A-S1	AS i MRB	<sense especificar>	Utilitzat per l'AS per a sol·licitar recursos multimèdia a l'MRB.
Cr (3GPP)	AS i MRFC	<sense especificar>	Utilitzat per l'AS per a controlar els mitjans sense passar per l'S-CSCF.
Mr' (3GPP)	AS i MRFC	SIP	Utilitzat per l'AS per a control de sessió sense passar per l'S-CSCF.

5) Punts de referència dels components d'emmagatzematge d'informació de subscripció

La taula següent mostra una descripció dels punts de referència per al subsistema IMS que s'esmenten en els models de la ITU-T, l'ETSI-TISPAN i el 3GPP i també la recomanació sobre el protocol per a implementar-ho.

Taula 11. Punts de referència dels components de magatzematge d'informació de subscripció

Nom	Entitats que interconnecta	Protocol	Descripció
Cx	S-CSCF o I-CSCF i UPSF	Diameter	Utilitzat per l'S-CSCF i l'I-CSCF per a consultar a l'UPSF informació d'autenticació i autorització d'usuari, perfil de subscripció, localització (S-CSCF assignat).
Dx	S-CSCF o I-CSCF i SLF	Diameter	Utilitzat per l'S-CSCF i l'I-CSCF per a consultar l'SLF sobre la localització de l'UPSF que conté la informació de subscripció d'un usuari.
Sh	AS i UPSF	Diameter	Utilitzat per l'AF per a consultar a l'UPSF informació d'autenticació i autorització d'usuari, perfil de subscripció, localització (S-CSCF assignat).
Dh	AS i SLF	Diameter	Utilitzat per l'AF per a consultar l'SLF sobre la localització de l'UPSF que conté la informació de subscripció d'un usuari.