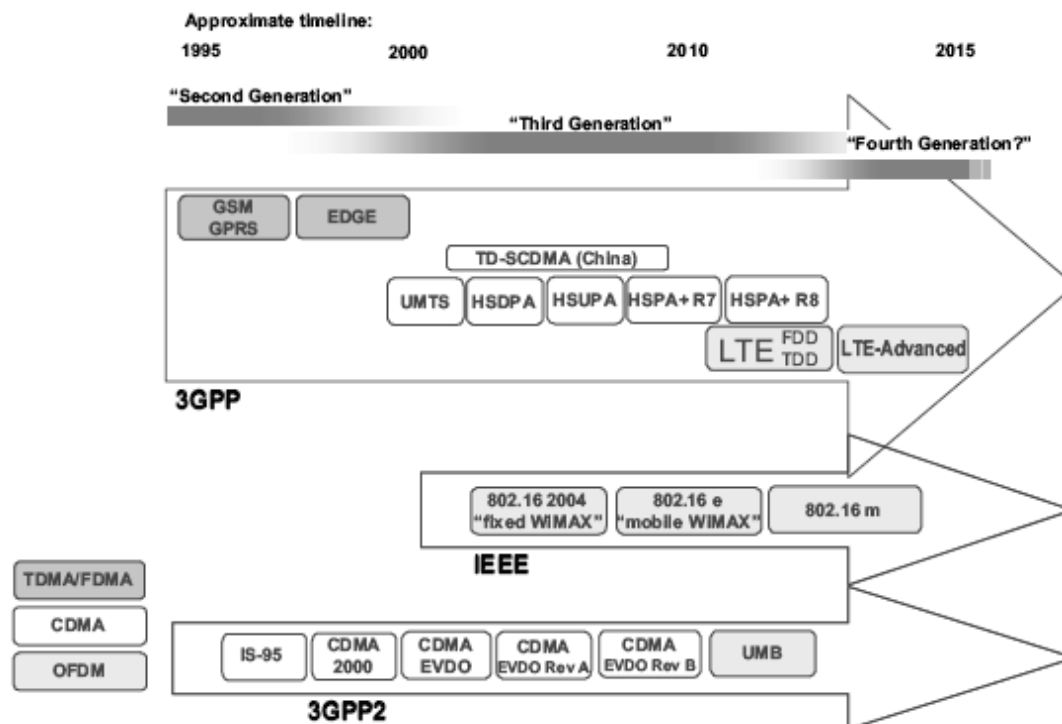


Curs 9 SC - LTE (Long Term Evolution). Arhitectura sistemului

LTE (Long Term Evolution) și EPC (Evolved Packet Core network) sunt cele mai noi tehnologii în telecomunicațiile mobile, fiind în faza de implementare și testare în multe țări.



LTE este o continuare a tehnologiilor GSM și UMTS. În cadrul 3GPP, LTE poate fi privit ca o finalizare în tendința de extindere a serviciului de voce către o interfață multi-service. Acest lucru a fost un obiectiv-cheie și pentru UMTS sau GPRS - EDGE, dar cu LTE s-a dorit evoluția tehnologiei de acces radio, presupunând că toate serviciile sunt bazate pe pachete comutate și nu sisteme de circuite comutate, așa cum este cazul tehnologiilor anterioare. În plus, LTE constituie și o evoluție a aspectelor non-radio ale sistemului complet, conform cu 'System Architecture Evolution' (SAE), care include Evolved Packet Core (EPC). Împreună, LTE și SAE formează Evolved Packet Core (EPC), cu comutație de pachete atât în rețeaua de bază cât și în cea de acces radio.

Introducere. Sistemul SAE (System Architecture Evolution) din standardul 3GPP

O dată cu evoluția interfeței radio, s-a constatat că și arhitectura de rețea trebuie să evolueze în paralel. Ceea ce a condus la această evoluție a fost în primul rând dorința de a optimiza serviciul de comutație de pachete în rețeaua mobilă, optimizarea interfeței radio devenind un factor secundar.

În tehnologia HSPA (High Speed Packet Access) deja s-a demonstrat că toate funcționalitățile radio pot fi grupate împreună într-un singur nod, numit NodeB, acest lucru deschizând o serie de oportunități. Întreaga arhitectură a rețelei mobile devine mai "plată", adică drumul unui apel spre destinație trece prin cat mai puține noduri, cu mai puține procesări.

Sistemul SAE a fost proiectat după următoarele criterii:

- optimizarea serviciilor de tip comutație de pachete, eliminarea suportului pentru modul de operare de tip comutație de circuit;
- suport optimizat pentru un throughput mai mare, fiind necesar pentru o creștere a ratei de bit la utilizatorul final;
- îmbunătățirea timpului de răspuns pentru activarea și instalarea purtătoarei;
- reducerea întârzierilor de pachete;
- simplificarea sistemului în întregime, comparat cu sistemele 3GPP existente și alte sisteme celulare;
- interoperarea optimizată cu alte rețele de acces de tip 3GPP;
- interoperarea optimizată cu alte rețele de acces wireless.

Multe dintre aceste criterii implică necesitatea dezvoltării unei arhitecturi plate. Arhitectura plată cu mai puține noduri implicate în furnizarea serviciului mobil, reduce întârzierile și îmbunătățește performanța. Dezvoltarea către această direcție a început încă de la “Release 7”, unde conceptul de “Direct Tunnel” permite ca nivelul de “User Plane (UP)” să omită nodul SGSN și plasarea funcționalităților de RNC în NodeB-ul de HSPA. Fig. 1 arată acești pași de evoluție, unde se poate observa cum s-a ajuns pe parcurs la arhitectura SAE.

Se pare că unele idei de perfecționare au condus la dezvoltarea arhitecturii în direcții complet diferite. De exemplu, interoperarea optimizată cu diferite noduri de acces radio implică necesitatea de a introduce un set de noi funcționalități și chiar noi interfețe pentru suportul unor protocoale specifice, dar aceasta împiedică însă păstrarea mai simplă a arhitecturii. De aceea, specificațiile arhitecturale ale 3GPP au fost împărțite în următoarele două direcții:

- **Îmbunătățiri ale GPRS pentru accesul de tip E-UTRAN:** Se descriu arhitectura și funcționalitățile în mediul 3GPP de bază, cu E-UTRAN și toate celelalte noduri de acces radio tip 3GPP, definind procedurile de interoperare dintre ele. Numitorul comun pentru aceste noduri de acces radio este folosirea protocolului GTP (GPRS Tunneling Protocol) ca protocol de mobilitate în rețea;
- **Îmbunătățiri arhitecturale pentru acces radio de tip non-3GPP:** Se descriu arhitectura și funcționalitățile pentru interoperarea cu noduri de acces radio non-3GPP, de exemplu CDMA2000 HRPD (High Packet Rate Data). Funcționalitatea de mobilitate este bazată pe protocoale de tip IETF, de exemplu MIP (Mobile Internet Protocol) și PMIP (Proxy MIP); tot în aceste specificații se descrie și rețeaua E-UTRAN adaptată pentru acest mediu de protocol.

În continuare se descrie arhitectura sistemului 3GPP în cele mai posibile scenarii de dispunere (deployment): a) scenariul de bază doar cu E-UTRAN; b) scenariul cu operatorul; c) de tip 3GPP cu noduri de acces radio 3GPP deja existente (moștenite) și E-UTRAN; d) E-UTRAN cu noduri de acces radio non-3GPP având un exemplu de interoperare cu CDMA2000.

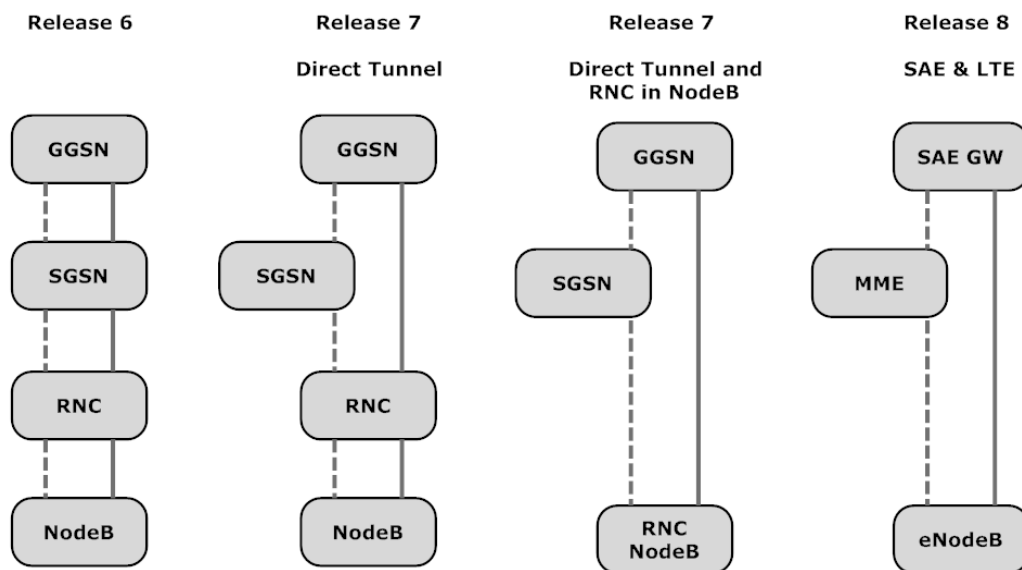


Fig.1. Evoluția arhitecturii 3GPP către o arhitectură “plată”

1.1 Configurația arhitecturii de sistem pentru rețeaua de acces radio E-UTRAN

În Fig. 2 este prezentată arhitectura și elementele de rețea din configurația în care este implicată rețeaua de acces radio E-UTRAN. Nodurile logice și conexiunile dintre ele reprezintă configurația arhitecturii de bază. Aceste elemente și funcționalitățile lor sunt necesare în toate cazurile în care este implicat E-UTRAN. Celelalte configurații arhitecturale, descrise în paragrafele următoare, includ funcții adiționale. Figura arată și împărțirea în 4 domenii de nivel înalt:

- 1) domeniul dispozitivelor mobile;
- 2) domeniul rețelei de acces radio E-UTRAN (Evolved-UMTS Radio Access Network);
- 3) domeniul rețelei EPC (Evolved Packet Core);
- 4) domeniul de servicii.

Domeniile dispozitivelor mobile, E-UTRAN și EPC împreună formează nivelul de conectivitate IP, această parte a sistemului mai numindu-se și EPS (Evolved Packet System).

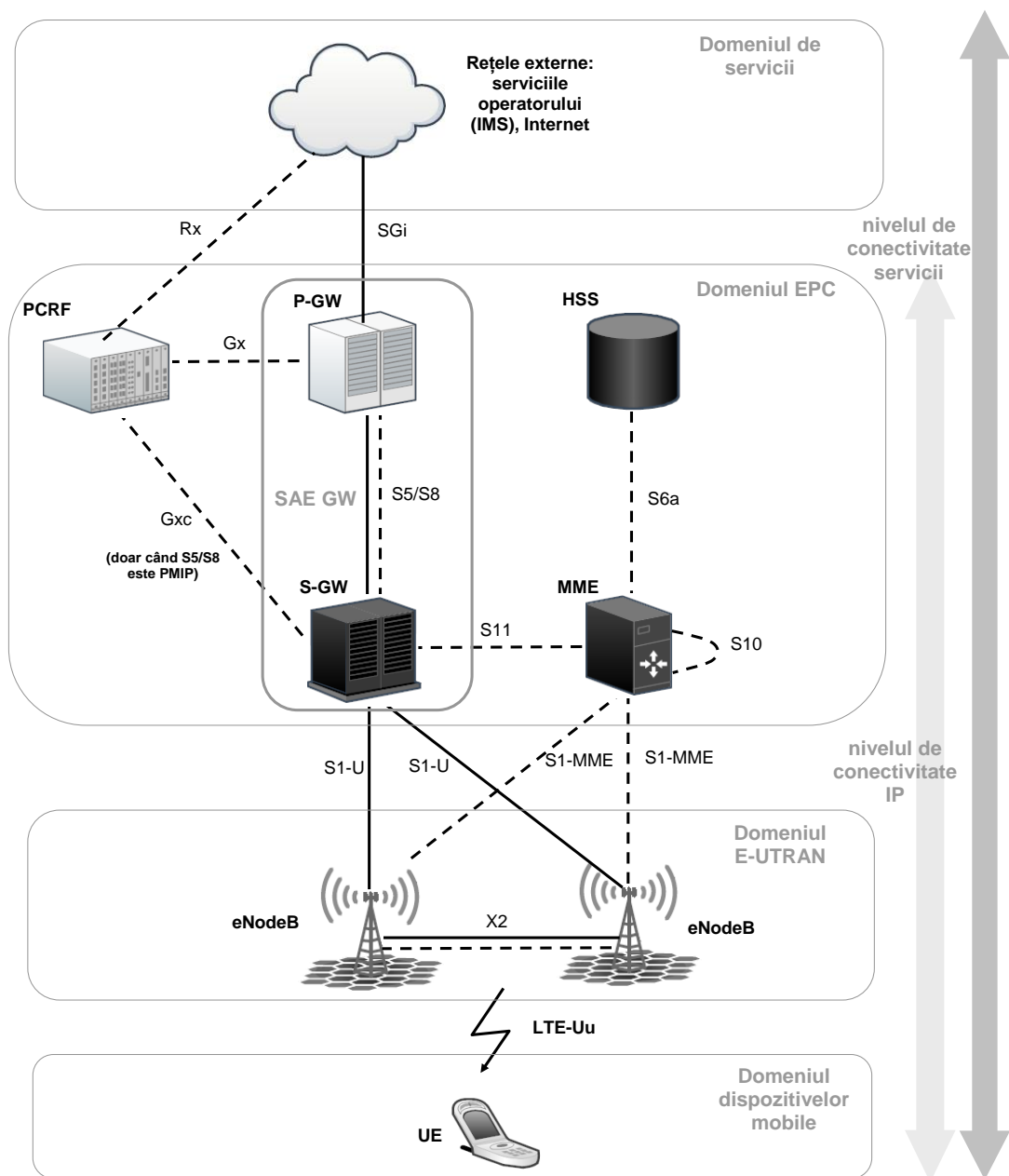


Fig. 2. Arhitectura sistemului EPC pentru rețeaua E-UTRAN

Funcția principală a acestui nivel este de a furniza conectivitate bazată pe IP și este optimizat doar pentru acest scop, toate serviciile fiind oferite peste nivelul de IP. Nodurile de tip comutație de circuit și interfețele existente în arhitecturile 3GPP precedente nu mai sunt prezente în E-UTRAN și EPC. Tehnologiile IP sunt dominante și în rețeaua de transport, unde totul este proiectat astfel încât să funcționeze peste transportul de IP. Sistemul IMS (IP Multimedia Sub-System) este un exemplu bun de mecanism de servicii ce poate fi folosit în nivelul de conectivitate de servicii pentru furnizarea serviciilor peste nivelul de conectivitate IP. De exemplu, pentru a oferi serviciul de voce, IMS poate furniza VoIP și conectivitate la rețele cu comutație de circuite PSTN și ISDN prin nodurile de tip Media Gateway pe care le controlează.

Dezvoltarea în E-UTRAN este concentrată în jurul unui singur nod, numit eNodeB (evolved NodeB), toate funcțiile radio fiind integrate în acest nod. eNodeB este punctul

terminal pentru toate protocoalele de tip radio. Ca rețea, E-UTRAN este pur și simplu o plasă (*mesh*) de eNodeB-uri conectate între ele prin interfața X2.

Una dintre marile schimbări arhitecturale în aria rețelei Core Network este faptul că EPC nu conține domeniul de comutație de circuit și pe acest nivel nu necesită conectivitate directă la rețelele tradiționale cu comutație de circuit ISDN sau PSTN. Ca funcționalitate, EPC este echivalent cu domeniul de comutație de pachete din rețelele 3GPP existente, însă există schimbări semnificative în dispunerea funcțiilor, de aceea majoritatea nodurilor și arhitectura sunt considerate a fi total noi.

Atât în Fig. 1 cât și în Fig. 2 apare elementul denumit SAE GW (System Architecture Evolution – Gateway). În Fig. 2 acesta reprezintă combinația a două gateway-uri, S-GW (Serving Gateway) și P-GW (Packet Data Network Gateway), folosite pentru tratarea nivelului UP (User Plane) din rețeaua EPC. Implementarea lor împreună, într-un singur nod SAE GW reprezintă faptul că există numai un singur scenariu de dispunere, dar standardele precizează o interfață între ele și toate operațiile au fost definite pentru cazul în care ele sunt dispuse separat.

Configurația arhitecturii sistemului de bază și funcționalitatea ei sunt documentate în specificația 3GPP TS 23.401. Acest document descrie și funcționarea pentru cazul în care interfața S5/S8 folosește protocolul GTP. Când interfața S5/S8 utilizează protocolul PMIP, funcționalitatea acestor interfețe este puțin diferită, fiind nevoie și de interfața Gxc, care se află între PCRF (Policy and Charging Resource Function) și S-GW. Diferențele arhitecturale sunt marcate în TS 23.401 și toate funcțiile adiționale sunt descrise în detaliu în specificația 3GPP TS 23.402.

1.1.1 Elementele logice în configurația arhitecturii sistemului de bază

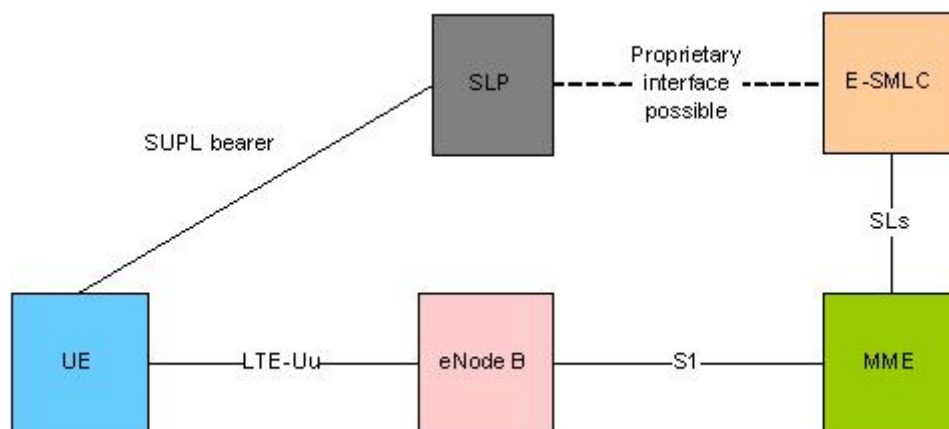
Acest paragraf descrie elementele logice de rețea din arhitectura de bază.

1.1.1.1 Dispozitivul mobil (UE – User Equipment)

UE reprezintă dispozitivul mobil ce poate fi un “smart phone”, “data card” (asemănător cu cele folosite în rețelele 2G sau 3G) sau poate fi integrat într-un laptop. UE conține modulul USIM (Universal Subscriber Identity Module) ce este separat de restul componentelor UE, acest modul adeseori fiind denumit și Echipament Terminal (TE-Terminal Equipment). USIM este, de fapt, o aplicație inclusă într-un smartcard numit UICC (Universal Integrated Circuit Card).

USIM este folosit pentru identificarea și autentificarea utilizatorului și pentru generarea cheilor de securitate folosite pentru protejarea transmisiei pe interfața radio.

Ca funcționare, UE este o platformă utilizată pentru aplicații de comunicație, aceasta transmițând semnalizări către rețeaua LTE/EPC pentru instalarea, menținerea și ștergerea legăturilor de comunicație folosite de către utilizator. Aici sunt incluse funcții de “mobility management”, de exemplu “handover”, sau raportarea locului unde se află terminalul mobil. UE poate furniza interfața de utilizare pentru aplicații client de VoIP, pentru crearea apelului de voce.



Arhitectura în EPS, raportată la poziția UE față de E-UTRAN

1.1.1.2 E-UTRAN Node B (eNodeB)

Singurul nod prezent în rețeaua E-UTRAN este nodul E-UTRAN Node B (numit eNodeB). eNodeB este o stație radio de bază ce controlează toate funcțiile specifice radio din partea fixă a sistemului. Stațiile de bază eNodeB sunt distribuite peste tot în aria de acoperire a rețelei, fiecare eNodeB fiind dispus lângă antenele radio.

Funcțional, eNodeB se comportă ca un “*bridge* - punte” de nivel 2 (OSI) între UE și rețeaua EPC (prin faptul că este punctul de terminare al tuturor protocoalelor radio către UE) prin comutarea datelor între conexiunea radio și conectivitatea IP corespunzătoare din rețeaua EPC. În acest rol, eNodeB are următoarele activități: cifrarea/decifrarea datelor de tip UP (User Plane) (datele din planul utilizator) și compresia/decompresia antetului (*header*-ului) de IP, cu avantajul că nu trebuie transmise în mod repetat aceleași date sau date secvențiale în header-ul de IP.

eNodeB este responsabil pentru mai multe funcții de tip CP (Control Plane) (funcții specifice planului de control), fiind responsabil și pentru managementul resurselor radio (RRM-Radio Resource Management), ce implică următoarele activități:

- controlul utilizării interfețelor radio, ce include, de exemplu, operațiunea de alocare a resurselor bazată pe cereri;
- prioritizarea și programarea traficului în funcție de Calitatea Serviciului (QoS – Quality of Service) cerută;
- monitorizarea constantă a situației de utilizare a resurselor.

În plus, eNodeB are un rol important în managementul mobilității (*MM-Mobility Management*).

eNodeB-ul controlează și analizează măsurătorile nivelului de semnal radio făcute de către echipamentul utilizator UE, efectuează măsurători similare și ia decizii de *handover* pentru a trece dispozitivele mobile dintr-o celulă în alta. Această operațiune include și activități de transmitere (interschimbare) a semnalizării de *handover* între celelalte eNodeB-uri și MME (*Mobility Management Entity*).

Atunci când un nou dispozitiv mobil UE se activează în zona de acoperire a eNodeB-ului și cere conexiune către rețeaua EPC, eNodeB-ul este responsabil pentru rutarea acestei cereri către MME-ul care servea înainte acest UE. De asemenea, face selecția unui nou MME, dacă ruta către MME-ul de dinainte nu mai este valabilă sau informația de rutare este absentă.

Fig. 3 arată toate tipurile de conexiuni pe care eNodeB-ul le are în relație cu celelalte noduri logice înconjurătoare și descrie sumar funcțiile principale din aceste interfețe.

În toate tipurile de conexiuni, eNodeB-ul poate să aibă relații one-to-many sau many-to-many. eNodeB-ul poate servi mai multe dispozitive mobile UE aflate în aria lui de acoperire, dar fiecare UE este conectat doar la un singur eNodeB la un moment dat.

eNodeB-ul va trebui să fie conectat însă la acele eNodeB-uri vecine care vor fi implicate în operațiunea de *handover*. Atât MME-urile cât și S-GW-urile se pot asocia (pooling), ceea ce înseamnă faptul că eNodeB-ul poate fi în conexiune cu mai multe MME-uri și S-GW-uri, dar fiecare UE este servit la un moment dat doar de către un singur MME și un singur S-GW. eNodeB-ul trebuie să urmărească aceste asocieri. Această asociere nu se va schimba niciodată din punctul de vedere al unui singur eNodeB, pentru că doar MME-ul sau S-GW-ul pot să se schimbe în cazul unui *handover* inter-eNodeB.

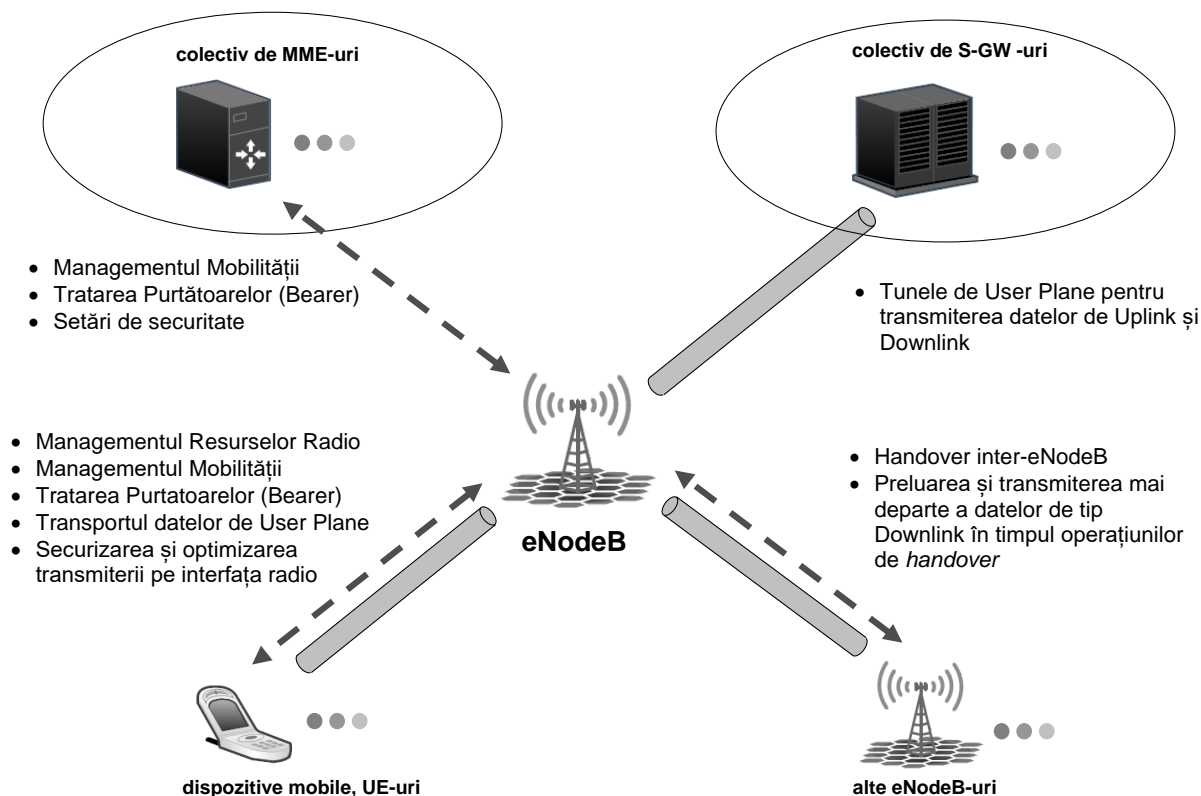


Fig. 3. Conexiunile eNodeB-ului cu alte noduri logice și descrierea funcționalităților de bază

1.1.1.3 Mobility Management Entity (MME)

Nodul MME (Mobility Management Entity) este elementul principal de control în rețeaua EPC. În premisa operatorului de rețea, MME este un server care se află într-un loc securizat. MME funcționează numai pe Nivelul de Control (CP-Control Plane) și nu este implicat în calea de transmisie a datelor de Nivel Utilizator (UP-User Plane). În plus față de interfețele terminate la MME, în arhitectura ilustrată în Fig. 4, MME-ul mai are și o conexiune logică directă de tip CP cu dispozitivul mobil UE, această conexiune fiind folosită drept canal principal de control între dispozitivul mobil UE și rețeaua EPC.

În continuare sunt descrise funcțiile principale ale MME-ului și configurația arhitecturii de sistem de bază:

- **Autentificare și Securitate:** Când un dispozitiv mobil UE se înregistrează în rețea prima dată, MME-ul inițiază autentificarea prin efectuarea următorilor pași:

- a) află identitatea permanentă a UE-ului de la rețeaua precedent vizitată sau chiar de la UE și face comparația între răspunsul primit de la UE cu cel primit de la rețeaua de origine (*home network*). Această funcție este necesară pentru a asigura faptul că dispozitivul UE este chiar cine susține că este. Detaliile autentificării EPS-AKA sunt definite în standardul 3GPP TS 33.401, “Security Architecture (Release 8)”. MME-ul poate repeta procedura de autentificare când este nevoie sau în mod periodic;
 - b) MME-ul calculează cheia de cifrare și cheia de protecție a integrității pentru dispozitivului mobil UE folosind cheia principală (*master key*) primită în vectorul de autentificare de la rețeaua de origine; astfel, va controla setările corespunzătoare în E-UTRAN pentru planurile UP și CP în mod separat. Aceste funcții sunt folosite pentru protejarea comunicării de ascultări nelegitime și de la alterarea ei de către părți terțe neautorizate;
 - c) Pentru a proteja confidențialitatea dispozitivului mobil UE, MME va aloca pentru fiecare UE o identitate temporară numită GUTI (Globally Unique Temporary Identity), tocmai pentru a reduce necesitatea transmiterii identității permanente a UE-ului (IMSI-International Mobile Subscriber Identity) pe interfața radio. Identificatorul GUTI poate fi re-alocat în mod periodic, tocmai pentru a evita urmărirea neautorizată a dispozitivului mobil UE.
- **Managementul Mobilității:** MME-ul înregistrează și urmărește localizarea tuturor dispozitivelor mobile UE în aria lui de servire. Când un UE se înregistrează prima dată în rețea, MME-ul va crea o înregistrare pentru UE și va semnaliza HSS-ul din rețeaua de origine a UE-ului cu localizarea curentă a acestui dispozitiv mobil. MME-ul va cere instalarea resurselor corespunzătoare, atât în eNodeB cât și în S-GW-ul pe care îl va selecta pentru UE.
MME-ul urmărește în continuare localizarea UE-ului, ori la nivelul eNodeB-ului, dacă UE rămâne conectat (însemnând că este activ în comunicație), ori pe nivelul de Tracking Area (TA), ce reprezintă un grup întreg de eNodeB-uri (în cazul în care UE-ul intră în stare pasivă, astfel că nu mai este necesară menținerea unei căi de date active/interconectate).
MME-ul controlează alocarea și eliberarea resurselor bazându-se pe schimbarea modului de activitate a UE-ului.
MME-ul participă și cu semnalizarea de control în cazul *handover*-ului unui UE activ între eNodeB-uri, S-GW-uri sau MME-uri.
MME este implicat în toate schimbările de eNodeB, deoarece acum nu mai exista un Radio Network Controller (ca în arhitecturile precedente) care să ascundă majoritatea acestor evenimente. Un UE pasiv va raporta localizarea lui în mod periodic, ori când se deplasează către o altă Tracking Area (Arie de Urmărire). În cazul în care sunt recepționate date destinate unui UE pasiv de la rețele externe, MME-ul va fi și el anunțat despre acest fapt, el cerând la rândul lui de la eNodeB-uri (din TA-ul în care UE este momentan înregistrat) să anunțe (prin *paging*) UE-ul corespunzător despre sosirea datelor.
- **Administrarea profilului și a conectivității la serviciu:** în momentul în care UE se înregistrează în rețea, MME-ul este responsabil pentru a obține profilul de înregistrare al UE-ului de la rețeaua de origine. MME-ul va stoca această informație pentru durata de timp în care servește UE-ul corespunzător. Acest profil descrie ce tipuri de conexiuni PDN (Packet Data Network) pot fi alocate pentru UE în momentul atașării lui la rețea. MME-ul va instala în mod automat purtătoarea inițială (*default bearer*), care va asigura conectivitatea IP de bază. Această conectivitate include atât suportul

pentru semnalizarea CP (Control Plane) cu eNodeB cât și semnalizarea CP cu S-GW. Mai târziu, ar putea să fie necesară implicarea MME-ului pentru alocarea purtătoarelor dedicate pentru a suporta furnizarea serviciilor care sunt tratate prioritar. MME-ul poate primi și cererea pentru a alocă o purtătoare dedicată, de la S-GW în cazul în care cererea provine din domeniul operatorului de servicii, ori cererea poate veni direct de la UE în cazul în care acesta necesită o conexiune pentru un serviciu care nu este cunoscut în domeniul operatorului de servicii și astfel nici nu se poate iniția de acolo.

Fig. 4 arată conexiunile MME-ului cu celelalte noduri logice înconjurătoare și descrie sumar funcțiile de bază ale acestor interfețe.

În principiu, MME poate fi conectat la orice alt MME din sistem, dar în mod tipic conectivitatea este limitată doar la un singur operator de rețea. Conectivitatea distantă între MME-uri poate fi folosită atunci când un UE care a călătorit departe în modul oprit se înregistrează la un nou MME, care va trebui să obțină identitatea permanentă și IMSI-ul UE-ului de la MME-ul anterior înregistrat/vizitat. Conexiunea inter-MME cu MME-urile vecine este folosită în cazul *handover*-urilor.

Trebuie să fie suportată conectivitatea la mai multe HSS-uri. HSS-ul se află în rețeaua de origine a fiecărui utilizator și ruta către acesta poate fi aflată pe baza IMSI-ului. Fiecare MME va fi configurat să controleze un set de S-GW-uri sau eNodeB-uri. Atât S-GW-urile cât și eNodeB-urile pot fi la rândul lor conectate și la alte MME-uri.

După cum s-a mai precizat, MME-ul poate servi un număr de UE-uri în același timp, pe când fiecare UE se va conecta doar la un singur MME la un moment dat.

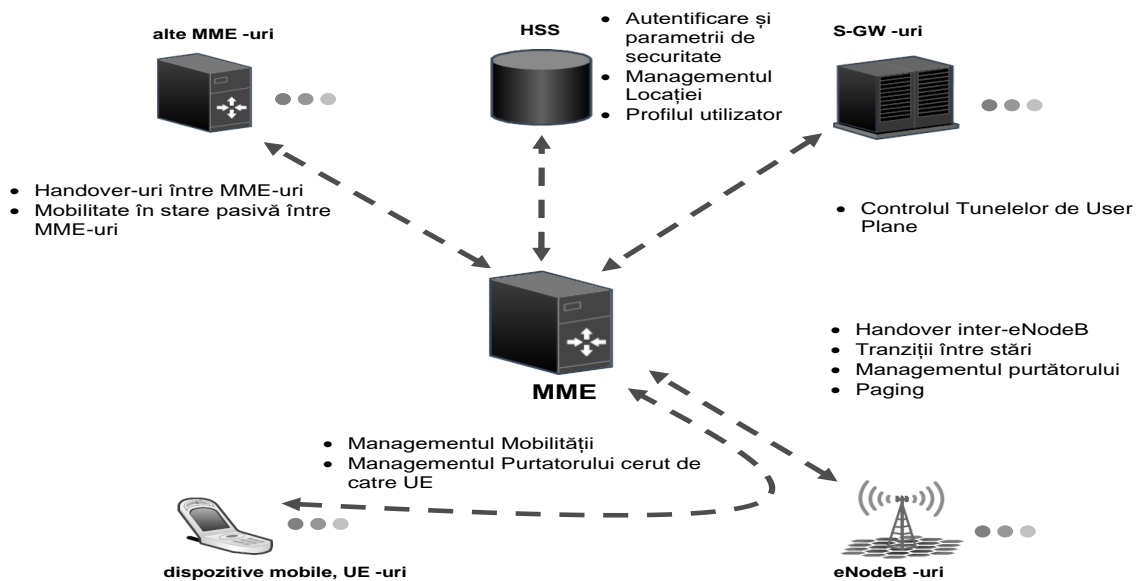


Fig. 4. Conexiunile MME-ului cu alte noduri logice și descrierea funcționalităților de bază

1.1.1.4 Serving Gateway (S-GW)

În configurația arhitecturii sistemului de bază, funcția de bază pentru S-GW o reprezintă managementul tunelului de UP (User Plane) și comutația. S-GW-ul face parte din infrastructura de rețea administrată central în premisa operatorului de rețea.

Atunci când pe interfața S5/S8 se folosește protocolul GTP, nodul S-GW va avea tunele pe toate interfețele lui de UP. Maparea între fluxurile de IP și tunelele GTP se face în P-GW, iar S-GW nu va trebui să fie conectat la PCRF. Tot controlul se face în legătură cu tunelele

GTP, iar acest control poate veni ori de la MME ori de la P-GW. Când interfața S5/S8 folosește protocol PMIP, S-GW-ul va efectua maparea între fluxurile IP din S5/S8 și tunelele GTP din interfața S1-U, conectându-se și la PCRF ca să obțină informația de mapare.

S-GW-ul are un rol minor în partea de control. Este responsabil doar pentru resursele lui, pe care le alocă pe baza cererilor venite de la MME, P-GW sau PCRF, dar, în schimb, contribuie la activitățile de alocare, modificare și ștergere de purtătoare pentru UE. Dacă interfața S5/S8 este bazată pe PMIP, datele în această interfață vor fi fluxuri de IP în tunele pentru fiecare UE, pe când dacă se folosește GTP pe interfața S5/S8, fiecare purtătoare va avea tunelul propriu de GTP. Așadar, la S-GW cu PMIP, S5/S8 este responsabil pentru legarea purtătoarei, de exemplu maparea fluxurilor de IP pe interfața S5/S8 către purtătoarele de pe interfața S1. Această funcție este numită BBERF (Bearer Binding and Event Reporting Function) în S-GW, adică Funcția de Interconectare de Purtătoare și Raportare de Evenimente.

Indiferent de unde a pornit semnalizarea de purtătoare, BBERF-ul întotdeauna primește informația de “legare a purtătoarei” de la PCRF.

Pe durata mobilității printre eNodeB-uri, S-GW-ul se comportă ca o ancoră locală de mobilitate. MME comandă S-GW-ul să comute tunelul de la un eNodeB la altul. MME poate și să ceară de la S-GW alocarea resurselor de tunelare pentru transmiterea de date, atunci când este nevoie de transmiterea datelor de la eNodeB-ul sursă către eNodeB-ul destinație în timpul în care UE face *handover*. Scenariile de mobilitate includ și varianta în care se face schimbarea de la un S-GW la altul, iar MME-ul respectiv controlează această schimbare, prin ștergerea tunelelor din S-GW-ul vechi și crearea lor în noul S-GW.

Pentru toate fluxurile de date ale unui UE care se află în modul conectat, S-GW-ul transmite datele între eNodeB și P-GW. Când un UE se află în modul inactiv, resursele în eNodeB sunt eliberate și calea de date se termină în S-GW. Dacă S-GW-ul recepționează pachete de date de la P-GW pe orice astfel de tunel, el le va colecta într-un *buffer* (tampon de memorie) și va cere MME-ului să inițieze anunțarea (*paging*) dispozitivului mobil UE despre acest eveniment (sosirea pachetelor). Această anunțare va determina UE-ul să se re-conecteze la rețea, iar în momentul în care și tunelele sunt re-conectate, pachetele colectate în *buffer* vor fi trimise mai departe la UE. S-GW-ul monitorizează datele din tunele și poate chiar să colecteze date pentru a le folosi în contabilitate și taxarea utilizatorului. S-GW are și funcție de Interceptare Legală, ce înseamnă capacitatea de a transmite datele monitorizate ale utilizatorilor către autorități pentru investigație.

Fig. 5 arată cum S-GW-ul este conectat la celelalte noduri logice și descrie funcțiile principale din aceste interfețe. Toate interfețele trebuie să fie dispuse în configurația “una la mai multe”, văzute din punctul de vedere al S-GW-ului. Un S-GW poate servi doar o anumită arie geografică cu un set limitat de eNodeB-uri, pe lângă acesta putând exista un set limitat de MME-uri ce controlează acea arie. S-GW-ul poate fi capabil să se conecteze la orice P-GW din întreaga rețea deoarece P-GW-ul nu se schimbă în timpul mobilității, pe când S-GW-ul poate fi realocat atunci când UE-ul se află în mișcare. În legătură cu conexiunile asociate unui singur UE, S-GW-ul se află în semnalizare doar cu un singur MME. Dacă unui UE îi este permis să se conecteze la mai multe PDN-uri (rețele de date de tip pachet) prin diferite P-GW-uri, atunci S-GW-ul trebuie să se conecteze separat la fiecare din acele P-GW-uri. Dacă interfața S5/S8 este bazată pe PMIP, S-GW-ul trebuie să se conecteze la un PCRF pentru fiecare P-GW în parte, pe care UE-ul îl folosește la respectivul moment.

Fig. 5 arată și cazul de transmitere indirectă a datelor, unde datele UP sunt transmise între eNodeB-uri prin S-GW-uri. Nu există un nume specific de interfață între S-GW-uri, deoarece formatul este exact același ca și în interfața S1-U, iar S-GW-urile implicate pot considera că ele comunică în mod direct cu un eNodeB. Acesta ar fi cazul în care se face

transmitere indirectă de date printr-un singur S-GW, de exemplu ambele eNodeB-uri pot fi conectate la același S-GW.

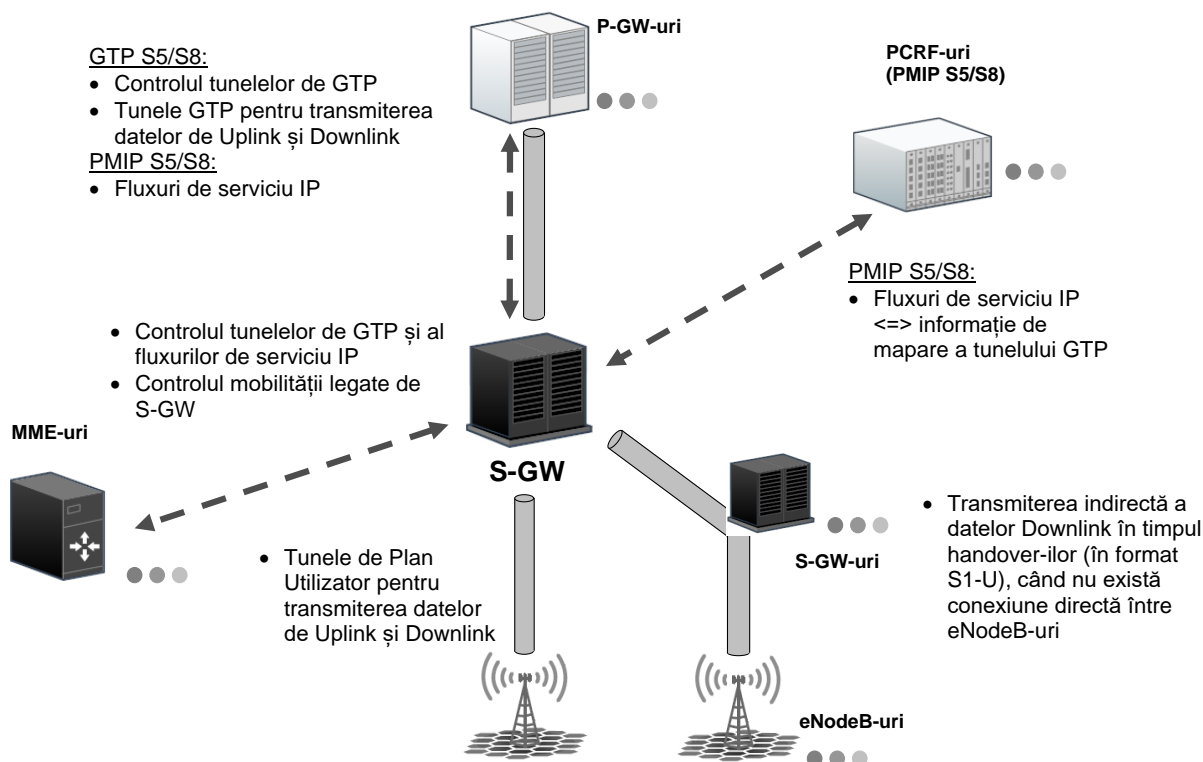


Fig. 5. Conexiunile S-GW-ului la alte noduri logice și descrierea funcțiilor de bază

1.1.1.5 Packet Data Network Gateway (P-GW) (Poarta pentru Rețeaua de Date de tip Pachet)

Packet Data Network Gateway (P-GW, sau abreviat altfel ca PDN-GW) este router-ul de margine (*edge router*) între sistemul EPS și rețelele externe de date în format pachet. Este ancora de mobilitate la nivelul cel mai înalt din sistem și în general se comportă ca punct de atașare IP pentru dispozitivul mobil UE, executând funcții de selecție și filtrare a traficului. Similar cu S-GW, P-GW-urile sunt menținute în clădirea operatorului de rețea într-un loc central.

În mod tipic, P-GW-ul este cel care alocă adresa IP pentru dispozitivul mobil UE, iar UE folosește această adresă pentru comunicarea cu alte sisteme gazdă IP din rețelele externe. Poate fi posibil ca PDN-ul extern la care este conectat UE-ul să alocă adresa IP care va fi folosită de către UE și atunci P-GW-ul va tunela tot traficul către acea rețea.

Adresa IP este întotdeauna alocată numai în momentul în care UE cere o conexiune la PDN. P-GW-ul execută și funcționalitatea de DHCP (Dynamic Host Configuration Protocol) sau poate interoga un server extern de DHCP pentru a furniza adresa IP pentru UE. Mai mult decât atât, standardele mai descriu și funcția de auto-configurare dinamică. Doar IPv4 sau IPv6 sau ambele tipuri de adrese pot fi alocate, depinzând de necesitate, iar UE-ul poate semnaliza dacă vrea să primească adresele în semnalizarea de atașare sau dorește să efectueze configurarea adresei numai după ce nivelul de legătură este conectat.

P-GW-ul include PCEF, fapt ce arată că poate să execute funcții de selecție și filtrare așa cum este cerut de către setul de reguli pentru UE și de către serviciul furnizat, așadar va colecta și raporta informațiile de taxare corespunzătoare.

Traficul de Nivel Utilizator (UP-User Plane) între P-GW și rețelele externe se găsește sub forma pachetelor IP ce aparțin diverselor fluxuri de servicii IP. Dacă interfața S5/S8 către S-GW este bazată pe protocolul GTP, atunci P-GW-ul efectuează maparea între fluxurile de date IP către tunelele GTP, care reprezintă de fapt purtătoarele.

P-GW-ul creează purtătoarele pe baza cererilor venite prin PCRF sau de la S-GW, care de fapt transmit informație de la MME. În al doilea caz, s-ar putea ca P-GW-ul să aibă nevoie să interacționeze cu PCRF pentru a cere informațiile corespunzătoare de control de politici, în cazul în care acestea nu sunt configurate local în P-GW. Dacă însă interfața S5/S8 este bazată pe PMIP, atunci P-GW-ul mapează toate fluxurile de servicii IP venite de la rețelele externe și care aparțin unui singur UE, la un singur tunel GRE (Generic Routing Encapsulation), iar toate informațiile de control sunt interschimbate doar cu PCRF. P-GW are și funcție de monitorizare a fluxurilor de date pentru scopuri de contabilitate și de interceptare legală.

P-GW-ul este ancora de mobilitate de cel mai înalt nivel din sistem. Când un UE se deplasează de la un S-GW la altul, purtătoarele trebuie să fie comutate în P-GW. P-GW-ul va primi o indicație pentru a comuta fluxurile la noul S-GW.

Fig. 6 arată conexiunile P-GW-ului cu nodurile logice înconjurătoare și descrie funcțiile principale în aceste interfețe. Fiecare P-GW poate fi conectat la una sau mai multe PCRF-uri, S-GW-uri și rețele externe. Pentru un anumit UE ce este asociat cu P-GW, există un singur S-GW, însă trebuie să fie suportate conexiuni către mai multe rețele externe și respectiv la mai multe PCRF-uri, dacă și conectivitatea la mai multe PDN-uri este suportată printr-un singur P-GW.

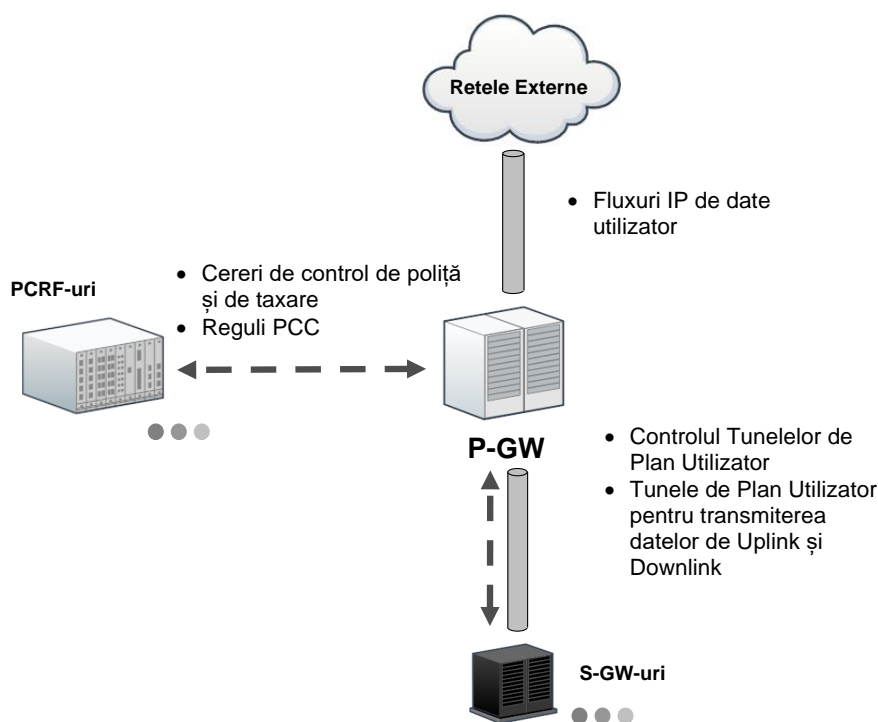


Fig. 6. Conexiunile S-GW-ului la alte noduri logice și descrierea funcțiilor de bază

1.1.1.6 Policy and Charging Resource Function (PCRF)

PCRF (Policy and Charging Resource Function - Funcția de Politici și Taxare pentru Resurse) este elementul de rețea responsabil pentru Control de Politici și de Taxare (PCC –

Policy and Charging Control). Ia decizii despre cum să se trateze serviciile din punctul de vedere al QoS-ului (Calității Serviciilor) și furnizează informații către PCEF-ul (Policy and Charging Enforcement Function) aflat în P-GW, iar dacă e cazul și către BBERF-ul aflat în S-GW pentru a se putea stabili purtătoarele și politicile corespunzătoare.

PCRF face parte din framework-ul PCC definit în standardul 3GPP TS 23.203, '*Policy and Charging Control architecture (Release 8)*'. El este un server care, în general, este dispus împreună cu alte elemente de CN (Core Network) în centrele de comutare ale operatorului de rețea.

Informațiile furnizate de PCRF către PCEF se numesc reguli PCC. PCRF-ul va trimite reguli PCC oricând este stabilită o nouă purtătoare. Stabilirea de purtătoare este necesară, de exemplu, atunci când UE-ul se atașează inițial la rețea și se stabilește purtătoarea implicită și ulterior, atunci când se stabilesc una sau mai multe purtătoare dedicate. PCRF-ul va fi în stare să furnizeze reguli PCC bazate pe cererile venite de la P-GW și de la S-GW în cazul PMIP, ca și în cazul de atașare, pe baza cererilor venite de la Funcția de Aplicație (AF – Application Function) ce se află în Domeniul de Servicii.

În acest scenariu, UE semnalizează în mod direct cu Domeniul de Servicii, de exemplu cu IMS (*IP Multimedia Subsystem*) și AF-ul trimite informația de QoS la PCRF. Aceasta va rezulta într-o decizie PCC și astfel se trimit regulile PCC către P-GW, iar informația de mapare a purtătoarei către S-GW, în cazul PMIP S5/S8. Purtătoarele de EPC sunt stabilite pe baza acestor informații.

Conexiunile între PCRF și celelalte noduri sunt ilustrate în Fig. 7. Fiecare PCRF poate fi asociat cu una sau mai multe AF-uri, P-GW-uri și S-GW-uri. Doar un singur PCRF este asociat la fiecare conexiune PDN.

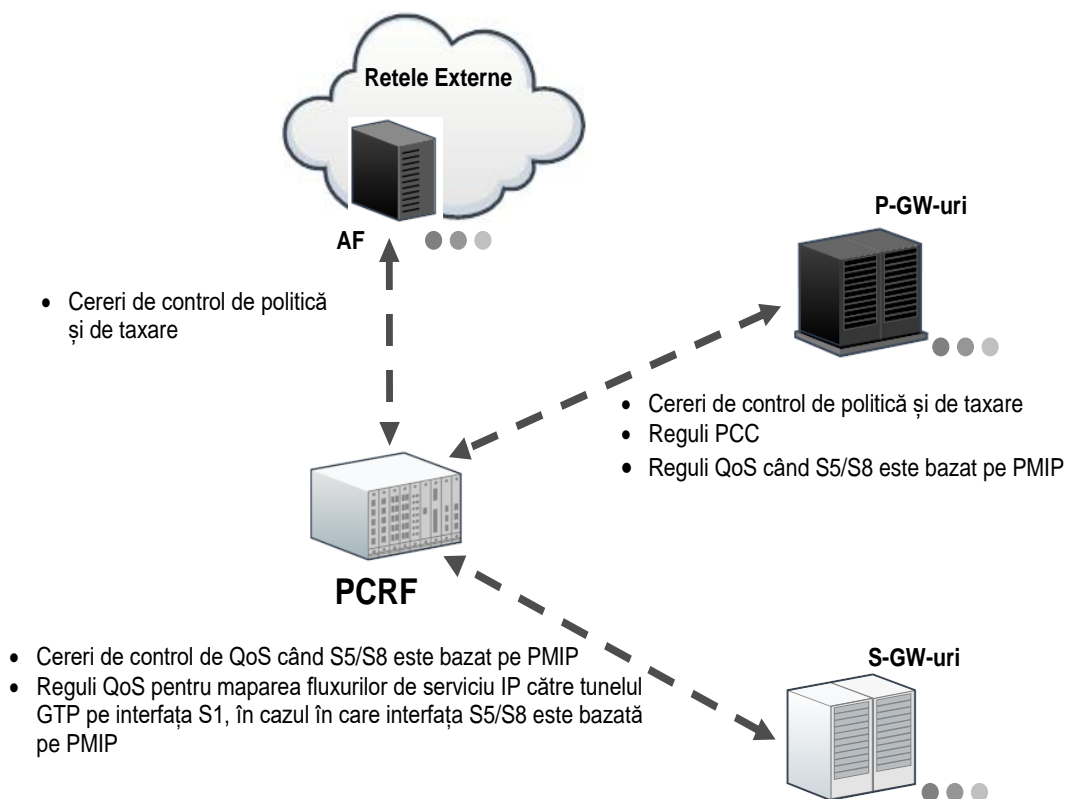


Fig. 7. Conexiunile PCRF-ului cu alte noduri logice și descrierea funcțiilor de bază

PCEF (Policy and Charging Enforcement Function) – Funcția de aplicare a politicilor și a taxării) este elementul funcțional care cuprinde aplicarea politicilor și urmărește funcționalitățile de bază pentru taxare. Ea este localizată în P-GW și controlează traficul de plan utilizator la GW și calitatea serviciilor, oferind totodată detectarea și contabilizarea datelor precum și activități de taxare online sau offline.

1.1.1.7 Home Subscriber Server (HSS)

Serverul de Origine al Abonaților – HSS (Home Subscription Server) este depozitul datelor permanente de abonat, conținând o bază de date administrată central în clădirea operatorului de rețea. Este folosit și pentru înregistrarea localizării curente a utilizatorului la nivelul nodului de control din rețeaua vizitată, de exemplu MME.

HSS-ul stochează copia de bază a profilului abonatului, ce conține informații despre serviciile care sunt aplicate pentru acel utilizator, informații despre conexiunile PDN permise și informații despre faptul că roaming-ul către o anumită rețea vizitată este permis sau nu. Pentru suportul mobilității între Noduri de Access Radio non-3GPP, HSS mai înregistrează și identitățile acelor P-GW-uri care sunt în folosință la momentul respectiv. Cheia permanentă, ce este folosită pentru calculul vectorilor de autentificare, este stocată în Centrul de Autentificare (AuC – Authentication Center), ce face parte în mod tipic din HSS. HSS-ul interacționează cu MME pentru toate semnalizările legate de aceste funcții.

HSS-ul va trebui să fie capabil să se conecteze la toate MME-urile din întreaga rețea, unde UE-ul său are permisiunea să se deplaseze. Pentru fiecare UE, înregistrările din HSS vor arata un singur MME ce îl deservește la un moment dat, iar când un nou MME raportează faptul că a preluat servirea UE-ului, HSS șterge locul MME-ului anterior.

1.1.1.8 Domeniul de Servicii

Domeniul de servicii poate include diferite sub-sisteme, ce pot include la rândul lor mai multe noduri logice. Mai jos sunt enumerate tipurile de servicii ce sunt puse la dispoziție, o descriere scurtă despre fiecare gen de servicii și tipul de infrastructură necesară pentru furnizarea lor:

- Serviciu de operator bazat pe IMS (IP Multimedia Subsystem) - este un mecanism de serviciu pe care operatorul îl poate folosi la furnizarea de servicii prin utilizarea protocolului SIP (Session Initiation Protocol). IMS are arhitectura definită de către 3GPP;
- Servicii de operator non-IMS: - arhitectura serviciilor non-IMS nu este definită în standarde. Operatorul pur și simplu poate plasa în rețeaua lui un server, iar UE-urile se pot conecta la acesta printr-un protocol ce este suportat de către o aplicație din UE. Un exemplu ar fi serviciul de *streaming* video furnizat de către un server de *streaming*;
- Alte servicii ce nu sunt furnizate de către operatorul de rețea mobilă, de exemplu

servicii furnizate prin internet: această arhitectură nu este descrisă în standardele 3GPP, ea depinzând numai de serviciul corespunzător. O configurație tipică ar fi aceea când UE-ul se conectează la un server din internet, de exemplu la un web server pentru servicii de navigație web, sau la un server SIP pentru accesul la serviciul de telefonie internet VoIP.

Deplasarea/Călătoria (Roaming) este o facilitate (împreună cu mecanismul aferent) importantă, cu ajutorul căreia operatorii își pot pune la dispoziție propria rețea abonaților altei rețele. Deplasarea se realizează, în mod tipic, între operatorii ce deservește arii diferite, de exemplu țări diferite. Termenii “origine” și “vizitat” sunt folosiți ca prefix împreună cu alți termeni arhitecturali pentru a descrie de unde provine abonatul și respectiv pe unde călătorește.

Specificațiile 3GPP SAE (System Architecture Evolution) definesc interfețele ce pot fi folosite între operatori și considerații adiționale ce sunt necesare atunci când se trece granița unui operator. În plus față de conectivitate între rețele, călătoria/deplasarea are nevoie ca operatorii să cadă de comun acord despre mai multe lucruri ce se află pe nivelul de servicii, de exemplu care sunt serviciile ce vor fi disponibile unui abonat în călătorie, cum vor fi realizate aceste servicii și cum se va ține contabilitatea, respectiv taxarea acestor servicii.

Acordul se numește “Acord de Călătorie” (Roaming Agreement) și poate fi făcut direct între operatori, sau printr-un broker. Specificațiile 3GPP nu acoperă aceste laturi ale călătoriei mobile și operatorii ce folosesc tehnologii 3GPP discută aspectele acestora într-un forum privat numit Asociația GSM (GSM Association), ce a publicat diverse recomandări pentru acoperirea acestor cerințe.

Călătoria definită pentru SAE este bazată pe principii foarte similare cu cele din arhitecturile 3GPP anterioare. Rețeaua de acces radio E-UTRAN se află întotdeauna în rețeaua vizitată, însă datele pot fi dirijate (rutate) ori către rețeaua de origine, ori pot să evadeze (break out) către rețele externe direct de la rețeaua vizitată. Acest aspect deosebește două modele de călătorie suportate în SAE, ce sunt definite ca:

- Modelul de dirijare din rețeaua de origine (dirijare, rutare efectuată de către rețeaua de origine). P-GW, HSS și PCRF se află în rețeaua operatorului de origine, iar S-GW, MME și rețelele radio se află în rețeaua operatorului vizitat. În această configurație de călătorie, interfața între P-GW și S-GW se numește S8, pe când aceeași interfață este numită S5 în cazul în care S-GW și P-GW se află în aceeași rețea de origine. Interfețele S5 și S8 sunt echivalente din punct de vedere tehnic. Când interfața S8 este bazată pe protocolul GTP, arhitectura de călătorie este cea din figura 12 (interfața Gxa nu se aplică cu GTP). Când interfața S8 folosește protocolul PMIP, PCRF-ul va fi despărțit în nod de origine și în nod vizitat, cu interfața S9 între ele. Acest scenariu este ilustrat în figura 12 în partea stângă. Modelul de dirijare din rețeaua de origine se aplică în același mod și pentru Nodurile de Access Radio 3GPP moștenite (provenite din arhitecturi anterioare), singura diferență fiind că SGSN-ul se afla în rețeaua vizitată;

- Modelul de evadare locală. În acest model, ilustrat în partea dreaptă a Fig., P-GW se află în rețeaua vizitată, iar HSS-ul se află în rețeaua de origine. Dacă se folosește control dinamic de politici, vor fi încă două PCRF-uri implicate, una în rețeaua de origine și cealaltă în rețeaua vizitată. În funcție de serviciile cărui operator se folosesc, PCRF-ul din rețeaua acelui operator este conectat la AF. Cu aceste constrângeri, modelul de evadare locală va funcționa și cu nodurile de acces radio 3GPP moștenite.

