Javna pokretna mreža – završni ispit

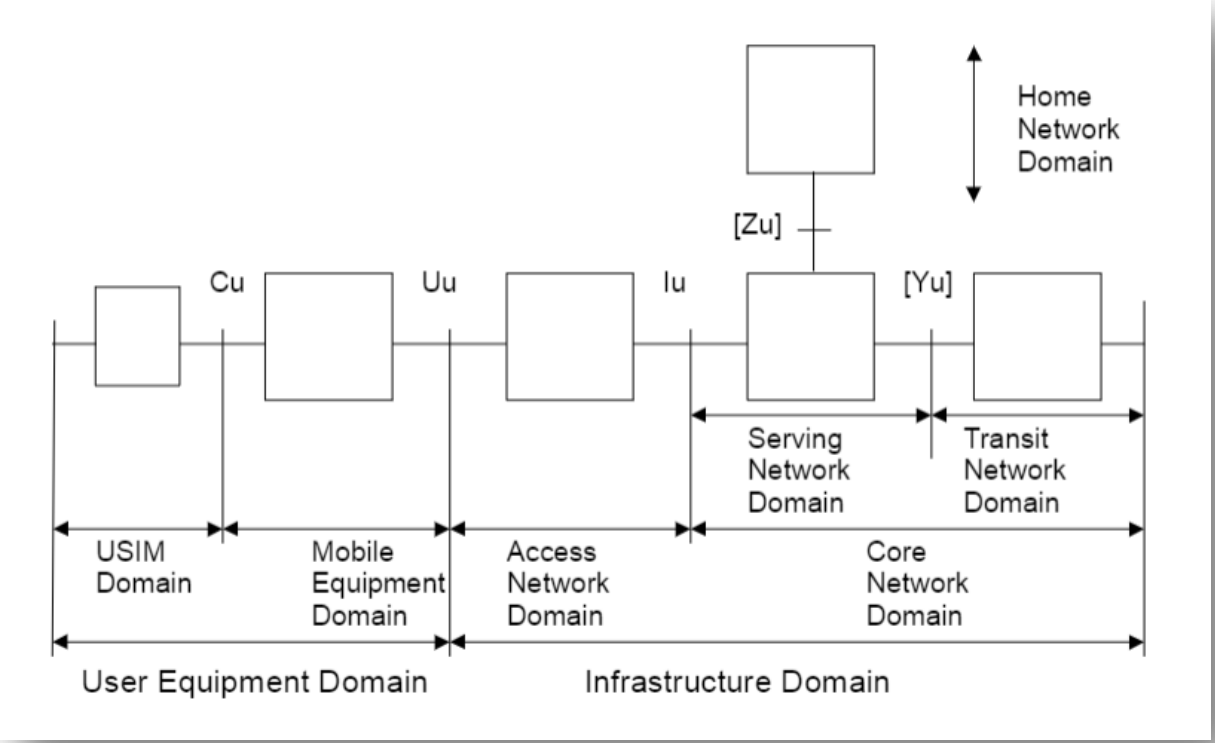
- koncept ne kontinuirane emisije – postupak gašenja emisije odašiljača u trenucima pauza u govoru
  - koristi se VAD (Voice Activity Detection)
  - smanjenje potrošnje baterije MS-a i smanjenje interferencijskih smetnji u radijskoj vezi
  - uvodi se komforni šum kako sugovornik ne bi pomislio da je veza prekinuta
  - osnovni problem: razlika između govora i šumova
- modovi rada MS-a:
  - dedicated mode – stanje u kojem mobilna postaja ima aktivnu vezu s mrežom i zauzima fizički kanal, koji sadrži barem 2 logička kanala
    - mreža daje sve važne parametre za podržavanje i kontrolu veze, kao i podatke o ćeliji kojoj se veza ostvaruje
  - idle mode – stanje u kojem je MS upaljena, ali je u stanju mirovanja, nema ostvarenu aktivnu vezu s mrežom
    - MS mora u određenom ritmu pratiti tzv. paging kanal, kako bi mogla primiti dolazni poziv
    - MS i u idle stanju može promijeniti ćeliju; ta se promjena razlikuje od promjene ćelije za vrijeme trajanja poziva – prekapčanja
    - u idle stanju mobilna stanica sama odlučuje o promjeni čelije
- upravljanje pokretljivošću – HLR i VLR
  - mreža nadzire uključivanje i isključivanje MS-a
  - nakon uključivanja MS-a slijedi:
    - utvrđivanje u kojoj se ćeliji trenutno nalazi
    - provjera autentičnosti i identiteta opreme
    - registracija lokacijske informacije u VLR-u
  - registracija se obavlja periodički i nakon promijene lokacije
- LAI (Location Area Identity) – jedinstveni identifikacijski broj lokacijskog područja
  - LAC – Location Area Code
  - BTS šalje svim MS-ovima putem BCCH kanala LAI
  - ako MS primi nepoznati LAI, znači da je promijenila lokacijsko područje te traži obnovu podataka o svojoj lokaciji (mijenjaju se podaci u HLR i VLR)
  - upućivanje poziva MS-u:
    - na osnovu MSRN pronalazi se MSC nadležan za pozivani MS
    - upitom područnom VLR-u dobiva se LAI
    - upućuje se skupni (paging) poziv preko svim područnih BTS-ova na koji se javlja pozivana MS
- slučajni pristup u GSM mreži
  - potaknut od strane mreže (paging poziv)

    - potaknut od MS-a (IMSI Attach, IMSI Detach, ažuriranje lokacije, odlazni poziv, SMS)
    - postupak:
        - MS šalje kratki burst preko zajedničkog kontrolnog kanala RACH koristeći Slotted Aloha načelo
        - BSC vraća Immediate Assignment (AGCH) poruku koja uključuje:
            - parametri dodijeljenog fizičkog kanala (frekvencija nositelja, vremenski odsječak) u kojem je smješten pridruženi SDCCH kanal
            - parametar Timing Advance
        - MS nakon toga šalje poruku na dodijeljenom SDCCH kanalu indicirajući razlog pristupanja mreži
- komunikacija se tijekom poziva šifrira (chipering)
- dolazni poziv – GMSC pronalazi HLR koji je zadužen za pozivani MS preko IMSI broja
    - potom od VLR-a traži TMSI koji se dalje koristi u komunikaciju

UMTS

- Universal Mobile Telecommunication System
- IMT-200 – u SAD-u
- uz pokretljivost terminala, riješena je osobna pokretljivost te pokretljivost, prenosivost i transparentnost usluga
- zahtjevi:
    - do 144 kbit/s u svim uvjetima, do 384 kbit/s na otvorenom prostoru, do 2 Mbit/s u zatvorenom prostoru
    - komutacija kanala i paketa
    - simetrični i asimetrični prijenos
    - kvaliteta govora usporediva s onom u fiksnoj mreži
    - više istodobnih usluga
    - integracija s fiksnom mrežom
    - koegzistencija s GSM-om
    - brzi pristup internetu u pokretu
- zahtjevi na usluge:
    - fleksibilnost – kretanje između različitih mreža
    - pristup uslugama bez obzira na pristupnu mrežu u kojoj se MS nalazi
    - prilagođenje usluge s obzirom na korišteni terminal
    - dostupnost usluge s obzirom na lokaciju
    - upravljanje profilom usluge bez obzira na lokaciju i pristupnu mrežu
- domena – predočuje skup funkcija pojedinog elementa UMTS mreže
    - međusobno odvojene referentnim točkama
    - USIM Domain (UMTS SIM) – podaci i procedure za nedvosmislenu i sigurnu identifikaciju osobe
    - Mobile Equipment Domain
        - pokretna oprema ME

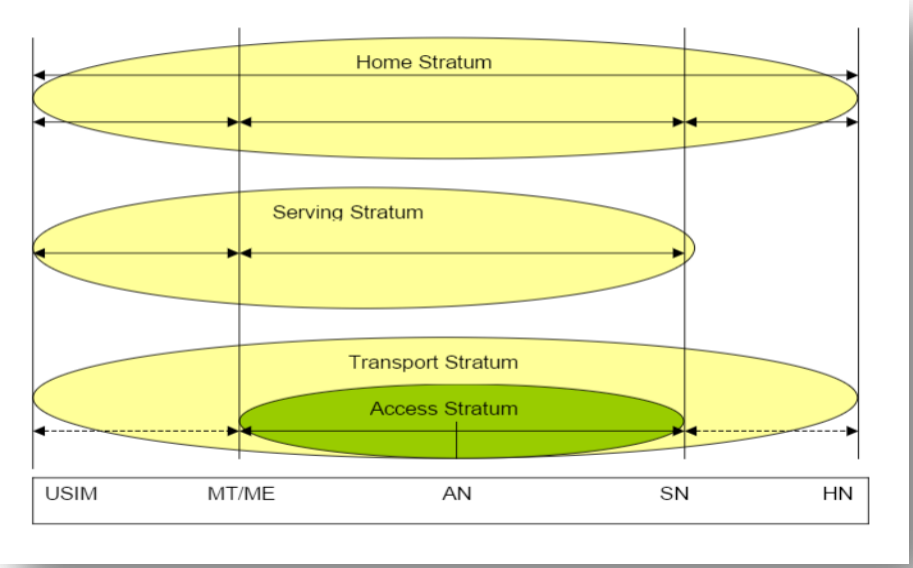
    - radijski prijenos MT (Mobile Termination) + Aplikacija TE (Terminal Equipment)
- Access Network Domain – pristup jezrenoj mreži
- Core Neetwork Domain – upravljanje lokacijskom informacijom i uslugama
    - transfer korisničke i upravljačke informacije



Slika 1. UMTS Domene

- stratum – predočuje funkcijsku komunikaciju između domena
    - funkcije i protokoli
    - vrste:
        - transportni stratum – transport korisničkih podataka i mrežne signalizacije
            - određuje fizikalni format prijenosa
            - šifriranje podataka na radijskom sučelju
        - pristupni stratum – dio transportnog stratuma
            - protokoli između UE i UTRAN
            - prijenos podataka na radijskom sučelju
            - upravljanje radijskim sučeljem
        - uslužni stratum – funkcije pridružene uslugama
            - protokoli za usmjeravanje i prijenos informacija
        - domaći stratum – protokoli i funkcije za pretplatničke podatke i usluge
            - usklađivanje korisničkih specifičnih informacija
            - pristup korisnički specifičnim informacijama i uslugama
        - aplikacijski stratum – aplikacijski procesi za krajnje korisnike
            - protokoli i funkcije mogu biti izvan standarda UMTS

- protokoli i funkcije od pokretne opreme, preko pristupne, uslužne, tranzitne mreže do krajnjeg korisnika

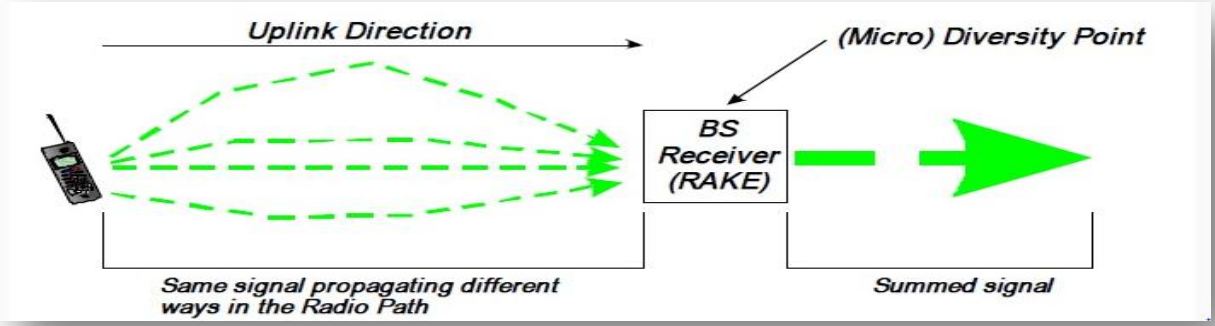


Slika 2. Stratumi

UTRAN

- UMTS Radio Access Network
- zemaljski radijski pristup
- UTRAN i GSM mreža mogu koegzistirati i biti spojeni na istu jezgrenu mrežu
- karakteristike:
  - širokopojasni višestruki pristup u kodnoj podjeli (WCDMA)
  - veći kapacitet i bolja pokrivenost
  - mogućnost varijabilne brzine prijenosa
  - prikladnost za paketski i kanalski prijenos
  - višestruke istodobne usluge u jednom terminalu
  - hijerarhijsko strukturiranje ćelija
- funkcije:
  - sustavna kontrola pristupa
  - sigurnost i privatnost
  - upravljanje i kontrola radijskih resursa
  - kontrola radijskog pristupa i veze između korisničke opreme i mreže
  - prijenos korisničkih podataka između korisničke opreme i mreže
- RNS (Radio Network Subsystem) – osnovni element UTRAN-a
  - sadrži:
    - RNC (Radio Network Controller)
      - CRNC (Controlling RNC)
      - SRNC (Serving RNC)
      - DRNC (Drifting RNC, prihvatni)

    - Node B – radijski primopredajni dio
        - pokriva više ćelija (3-6)
        - upravljanje radijskim resursima
        - modulacija (podržava FDD, TDD, CDMA)
        - fizikalni i transportni kanali
        - korekcija pogrešaka
        - povezivanje poziva s UE
        - sakupljanje prometnih podataka
- CDMA – Code Division Multiple Access
    - korisnici dijele isti frekvencijski spektar u isto vrijeme, a razlikuju se po dodijeljenim kodovima
    - svaki uređaj koristi čitavi frekvencijski pojas UMTS sustava cijelo vrijeme
    - svakoj MS dodjeljuje se jednoznačni kod (Chip Sequence)
    - „1“ u prijenosu se zamjenjuje sa Chip Sequence, a „0“ sa komplementom od Chip Sequence
    - soft handover – meko prebacivanje poziva
        - nema prekida veze prilikom prebacivanja bazne stanice
        - korisnik ima vezu sa više baznih stanica istovremeno
    - WCDMA – širokopojasni višestruki pristup s kodnom podjelom
        - podrška više simultanih nosilaca i varijabilne brzine prijenosa u svakoj vezi
        - FDD – 1920-1980 MHz (up), 2110-2170 MHz (down) – otvoren prostor
        - TDD – 1900-1920 MHz i 2010-2025 MHz – zatvoren prostor
        - širina frekvencijskog pojasa – 5 MHz
            - omogućava višestazni diverziti korištenjem rake prijamnika (Rake Reciever)
                - mikro diverziti
                    - višestazni dolazni signal se na Rake prijamniku dekodira tako da se dekodira svaka komponenta pojedinačno, a onda se kombiniraju kako bi se izvukao maksimum iz signala
                    - povećava omjer signal šum
                    - višestazni signal – signal koji dolazi do prijamnika umnožen i po različitim putanjama, s određenim kašnjenjem



Slika 3. Mikro diverziti

        - makro diverziti
            - isti tok podataka se šalje preko različitih fizičkih kanala
            - uzlazna veza: UE šalje podatke istovremeno različitim baznim postajama (Node B)
            - silazna veza: prijam istog toka podataka iz više susjednih ćelija s različitim raspršnim kodovima
    - prošireni frekvencijski spektar – raspršeni spektar
        - prije odašiljanja se uskopojasni signal raspršri preko širokog frekvencijskog pojasa (zadržavajući gustoću snage konstantnom)
        - u prijamniku se signal vraća u izvorni uskopojasni originalni oblik
        - manja osjetljivost na uskopojasne interferencije i prigušenje
        - nema fiksnog ograničenja kapaciteta (broja korisnika)
        - nedostatak: povećanje razine interferencije od drugih pretplatnika
    - omogućava dinamički promjenjive dimenzije ćelije
        - kod UMTS-a je veličina ćelije u uskoj vezi s njezinim kapacitetom
            - veličina ćelije ovisi o odnosu signal/šum – zbog veće snage emitiranja udaljenih korisnika i broja aktivnih korisnika nastaju interferencije u istoj ćeliji zbog ostalih korisnika u ćeliji, kao i iz drugih ćelija, što rezultira disanjem ćelija – cell breathing
                - konstantna promjena veličine geografskog područja pokrivanja bazne postaje na temelju količine prometa unutar ćelije
                - kad je ćelija preopterećena, korisnici se prebacuju u susjedne ćelije
                - povećanjem broja korisnika, smanjuje se veličina ćelije
- jezgrena mreža:
    - dio s komutacijom kanala – izveden iz GSM-a
    - dio s komutacijom paketa – izveden iz GPRS-a
- IMS (Internet Multimedia Subsystem) – omogućuje preusmjeravanje prometa
    - komutacija kanala – Internet
    - komutacija paketa – PSTN, ISDN
    - integracija interneta i ćelijskih mreža
    - pružanje usluga u stvarnom vremenu
    - višemedijske sjednice između više korisnika
    - ahitektura
        - aplikacijski sloj – odvaja sadržaj i usluge od povezivanja i pristupa
            - aplikacijski poslužitelji - AS
                - IMS AS – prisutnost, poruke, grupe
                - SIP AS – usluge temeljene na protokolu SIP
            - IP Multimedia – Service Switching Function (IM SSF)
                - poslužitelj za povezivanje IMS-a s uslugama koje su bile razvijene za GSM
        - upravljački sloj – zajednička IP temeljna struktura
            - elementi baze podataka
                - HSS – Home Subscriber Server

        - nadležni S-CSCF
    - elementi upravljanja
        - funkcija za upravljanje sjednicom poziva CSCF (Call Session Control Function)
        - P-CSCF
            - posrednički SIP poslužitelj
            - prva dodirna točka između terminala i IMS mreže
            - registracija i autentifikacija korisnika
            - uspostavlja sigurnu asocijaciju s UE
            - naplata
        - S-CSCF
            - središnji upravljački čvor
            - SIP poslužitelj, upravlja sjednicom
            - osluškuje AS-ove koji sudjeluju u komunikaciji
            - usmjerava SIP poruke
            - više S-CSCF-ova u mreži
        - I-CSCF (Interrogating CSCF)
            - upitni CSCF
            - definira domenu, njegova adresa se nalazi u DNS-u
            - prva točka u vlastitoj mreži za kontakte iz gostujuće ili vanjske mreže
            - usmjerava SIP zahtjeve za nadležni S-CSCF
    - elementi sučelja s upravljačkom razinom
        - MGCF – Media Gateway Control Function
            - funkcija upravljanja medijskim pristupnikom
        - BGCF – Brearout Gateway Control Function
            - funkcija za upravljanje pristupnikom za prebacivanje veze
            - SIP poslužitelj
            - usmjerava na temelju pozivnog broja
        - SGW – Signaling Gateway
            - signalizacijski pristupnik
        - IMS MGW
    - elementi resursa
        - MRF – Media Resources Function
            - manipulacija medijskim tokovima
            - Controller – MRFC
                - obavlja upravljanje vezama s više sudionika
            - Processor – MRFP
                - distributer medija prema mreži
    - element sučelja na razini mreže
        - MGW – Media Gateway
- sloj povezivosti
    - UE se može povezati na IMS preko različitih pristupnih mreža

- Tunneling protokol se u UMTS-u uvodi i između UTRAN-a i SGSN-a
- SIP
  - osnovna ideja: omogućiti pozivanje korisnika u sjednicu pomoću jedinstvene adrese, neovisno o trenutnom položaju:
    - [sip:]<user>@(<host>|<domain>)
  - omogućava osobnu pokretljivost korisnika
  - primjeri sjednica: poziv u internetskoj telefoniji, distribucija višemedijskog sadržaja, višemedijska konferencija
  - entiteti:
    - korisnički agent – UA
      - klijent i poslužitelj
    - poslužitelji:
      - posrednički poslužitelj
        - SIP usmjeritelj
        - prima SIP poruke od UA ili posredničkog poslužitelja
      - poslužitelj za preusmjeravanje
        - preslikava SIP adrese
        - ne prosljeđuje zahtjeve već samo vrača adresu odgovarajućeg SIP poslužitelja
      - registar
        - razlučivanje adrese, povezivanje korisnika s njegovom trenutnom lokacijom
    - SIP poruke: INVITE, ACK, CANCEL, BYE
    - odgovori – statusni kodovi – standardni osim što kod SIP-a ima i kod 6xx koji označava globalnu pogrešku
  - SIGTRAN – Signaling Transport
    - skup protokola koji omogućavaju prijenos signalizacije SS7 preko IP mreže
    - tri komponente:
      - protokol za adaptaciju
      - Common Signaling Transport Protocol (SCTP)
        - podržava skup pouzdanih prijenosnih funkcija za prijenos signalizacije
      - Internetski protokol IP

Ključne razlike između UMTS i GSM		
	WCDMA	GSM
širina kanala	5 MHz CDMA	200 kHz TDMA
ponavljanje frekvencija	1	nakon 4-12 ćelija
prekapčanje veze	istovremena komunikacija s više baznih postaja	komunikacija s ćelijom se prekida pri spajanju na novi BS
frekvencijski diverziti	Rake prijamnik demodulira signale višestaznog širenja	interferencija i feding reduciraju se skakanjem frekvencija
kapacitet sustava	soft, ovisi o opterećenju ćelija i interferenciji	hard, ovisi o faktoru ponavljanja frekvencija
kontrola snage	1,5 kHz	2 Hz (vrlo sporo)
procedura traženja ćelije	korištenjem sinkronizacijskog kanala i PN koda	pretraživanjem frekvencija nositelja
diverziti emitiranja	podržan u silaznoj vezi	nije podržan

Slika 4. Razlike između GSM-a i UMTS-a

Evolucija ćelijskih sustava

- HSCSD – High Speed Circuit Switched Dana
  - novi software
  - istovremeno korištenje nekoliko vremenskih odsječaka (moguće svih 8, u praksi 4)
  - prednost: jednostavan za primjenu, konstantna kvaliteta
  - nedostatak: kanali blokirani za prijenos govora, skupa naplata usluge
- GPRS
  - uvodi novi PDCH kanal koji može biti dodijeljen permanentno ili privremeno vremenskom odsječku TDMA okvira
  - dinamičko i fleksibilno pridruživanje prometnih kanala i dodjela više od jednog vremenskog odsječka po okviru
  - prednost: korak bliže prema UMTS, fleksibilnost
  - nedostatak: veća investicija
  - brzine ovise o kodiranju i broju odsječaka, a idu do 171.2 kbit/s
  - uvodi četiri različita načina kodiranja – razlikuju se u parametrima blokovskog i konvolucijskog kodiranja
    - blokovski koder – dodaje fire code (detekcija pogrešaka) od 40 ili 16 bita, kodira USF (Uncoded Uplink State Flag) koristeći 3, 6 ili 12 bita i dodaje 4 tail bita
    - konvolucijski koder – razlika je u omjerima koda
- EDGE
  - novi modulacijski postupak (8 PSK) s 3 bita po simbolu

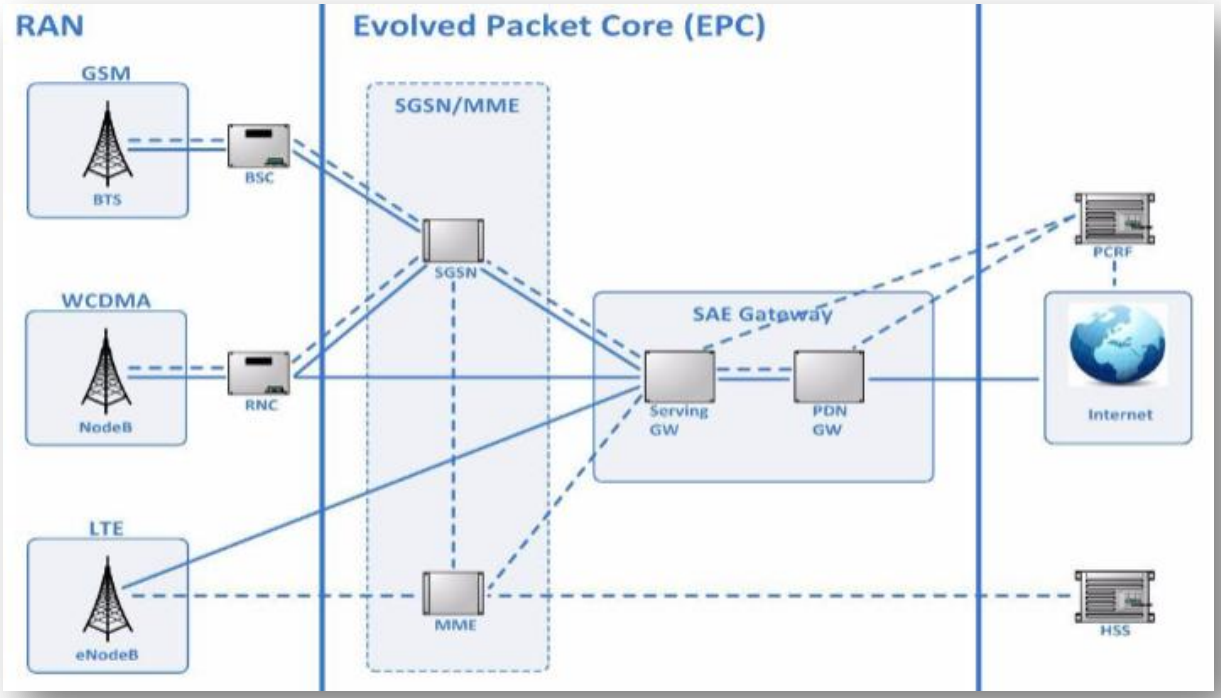
- različite klase kodiranja
- maksimalna brzina 43 kbit/s po kanalu
- prednost:
  - povećanje prijenosnog kapaciteta
  - iskorištavanje postojećih frekvencijskih pojaseva
  - zadržavanje postojeće infrastrukture
- nedostatak:
  - nužna bolja kvaliteta signala u odnosu na onu koju nudi GSM mreža
  - velike brzine nisu dostupne svuda u ćeliji
  - signal je vrlo osjetljiv na interferencije i smetnje
  - potrebna promjena softvera i hardvera u pristupnoj mreži kao i prilagodba mobilnih postaja
- definira ukupno 9 postupaka koji se razlikuju u modulaciji, kodiranju i načinu zaštite od pogrešaka – primjena ovisi o parametrima radijske veze i kvaliteti signala
  - četiri se baziraju na GMSK modulaciji
  - pet preostalih bazira se na 8PSK modulaciji
- novi prometni kanali – E-TCH/F (Enchanched Circuit Switched Data)
  - E-TCH/F 28.8
  - E-TCH/F 32.0
  - E-TCH/F 43.2

- prednosti 3G i 4G mreža u odnosu na prijašnje generacije:
  - tehnologija radijskog sučelja – OFDMA, CDMA
  - širina frekvencijskog pojasa kanala – 5-20 MHz
  - korištenje MiMo tehnologije – Multiple Input Multiple Output
    - prijem/predaja višestrukih neovisnih tokova podataka između odašiljača i prijemnika
- HSPA – 3.5G
  - High Speed Packet Access
  - HSPA+ – kanal širine 10 MHz
  - Node B preuzima određene funkcionalnosti od RNC-a
  - adaptivna modulacija i kodiranje
    - koristi se povratna informacija od korisničkog terminala kako bi se utvrdila najbolja modulacijska tehnika i kodirajuća shema za zadane uvjete u kanalu
    - terminal komunicira s više čvorova B i definira listu baznih stanica koje je moguće koristiti za komunikaciju (FCSS – Fair Scheduling and Fast Cell Site Selection)
    - odabire ćeliju sa najboljim karakteristikama
  - kraći TTI (Transmission Time Interval) koji reducira kašnjenja i poboljšava praćenje brzih varijacija karakteristika kanala
    - određuje vrijeme zauzeća kanala
    - definira se za svakog korisnika posebno
    - varijabilna duljina okvira – ovisno o vrsti prometa
    - dva terminala – isti kanal s različitim TTI

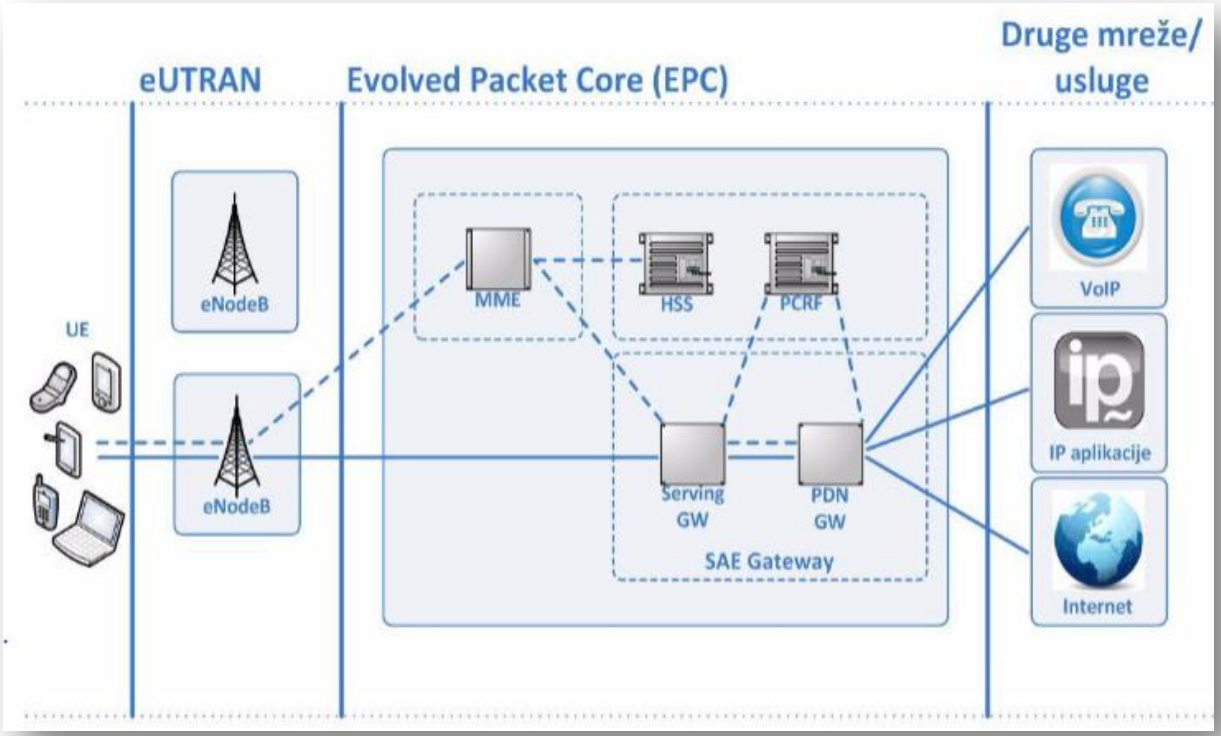
- brza adaptacija linkova – učinkovitija modulacija i kodiranje kanala
- dinamičko raspoređivanje kanala, dinamička promjena kapaciteta – prioritet imaju oni s boljom kvalitetom signala
  - korisnicima koji se nalaze u području s boljim uvjetima doznačuje se veći kapacitet prijenosne mreže i veće prijenosne brzine čime se postiže efikasnije zauzeće kanala
  - dodijeljeni kapacitet ovisi o broju korisnika koji se nalaze unutar istog područja
- brza retransmisija
- uz QPSK koristi se i 16-QAM modulacija s 4 bita po simbolu
- MiMo – antenski diveerziti
- 14.4 Mbit/s – u praksi 7.2 Mbit/s
- HSPA (HSUPA/HSDPA) – uplink i downlink
- nadogradnja potrebna samo u pristupnom dijelu mreže (RNC i Node B)

- HSPA
  - poboljšanje radijskih performansi
  - optimizacijski postupci za dodatno smanjenje kašnjenja u prijenosu podataka te povećanje kapaciteta
  - paketski prijenos govora i podataka
  - potpuno iskorištenje mogućnosti višestrukog pristupa WCDMA
  - 42 Mbit/s (down), 11.5 Mbit/s (up) – u praksi duplo manje brzine
  - prvi korak prema pristupnoj mreži LTE te novoj jezgrenoj mreži SAE (System Architecture Evolution) – all IP
- LTE – 4G
  - Long Term Evolution
  - širina kanala od 1.25 MHz do 20 MHz
    - 100 Mbit/s u dolaznom smjeru i 50 Mbit/s u odlaznom smjeru (326 Mbit/s, 86 Mbit/s)
  - više usluga, niže cijene pojednostavljenje arhitekture, otvorena sučelja
  - vrijeme odziva RTT (Round Trip Time) manje od 10 ms
  - smanjenje broja mrežnih elemenata
  - koegzistencija sa GSM i UMTS
  - OFDMA u dolaznom smjeru, a SC-FDMA u odlaznom smjeru
  - MiMo – višestruke antene, više paralelnih strujanja podataka prema pojedinom korisniku
  - all IP
  - dodjela frekvencijskih resursa u dolaznom i odlaznom smjeru definirana blokovima širine 180 kHz
  - nova jezgrena mreža – EPC (Envolved Packet Core)
    - podržava pristupnu mrežu E-UTRAN uz smanjenje broja mrežnih elemenata
    - pojednostavljene funkcionalnosti, smanjenje kašnjenja
    - mogućnosti povezivanja i prekapčanja s fiksnim i ostalim bežičnim pristupnim tehnologijama

- LTE + SAE = 4G EPS (Envolved Packet System)
- MME (Mobility Menagment Entity)
  - temeljni čvor jezgrene mreže
  - brine o signalizacijskim porukama koje se izmjenjuju između UE i čvorova jezgrene mreže
  - nadležan za velik broj Node B
  - funkcionalnosti:
    - sigurnost
    - autentifikacija
    - prekapčanje poziva
    - dodjela mrežnih resursa
    - upravljanje pristupom, sjednicom i vezom
    - upravljanje lokacijom terminala u mirovanju
  - služi samo za razmjenu signalizacije
- čvorovi prilaza – SAE Gateway
  - S-GW (Serving Gateway)
    - tunelira podatke prema P-GW
    - prati kretanje korisničkog terminala između čvorova eNodeB pristupne mreže
    - upravljanje pokretljivošću
    - brine o uspostavi veze s korisnicima drugih mreža
  - P-GW (Packet Data Network Gateway)
    - usmjerava podatke od jezgrenog dijela mreže prema ostalim mrežama
    - dodjela IP adrese korisničkim uređajima
    - naplata
    - pružanje usluga s određenom kvalitetom
- HSS (poslužitelj domaćih pretplatnika)
  - baza podataka koja sadrži podatke o pretplatnicima, njihovim profilima, uslugama, ograničenjima i ostalim parametrima bitnim za pružanje usluga
- čvor za upravljanje resursima i terećenjem (Policy Control and Charging Rules Function – PCRF)
  - terećenje, autorizacija, pružanje usluge a obzirom na pretplatnički profil, provođenje pravila operatora i sl.



Slika 5. LTE/SAE arhitektura



Slika 6. Napredni LTE (LTE-A)

- pristup internetu – prilikom uključivanja UE u mrežu, čvor MME kreira UE kontekst u kojem su zapisane karakteristike veze i mogućnosti korisničkog terminala dobivene na temelju korisničkog profila preuzetog iz HSS-a, IP adresa
  - uspostava veze UE – P-GW:
    - UE inicira i uspostavlja vezu s eNodeB
    - UE šalje zahtjev za uspostavom IP veze s čvorom P-GW
    - eNodeB uspostavlja logičku vezu s MME
    - MME ažurira lokaciju UE u HSS i od HSS dobiva pretplatničke podatke
    - MME inicira uspostavu veze između S-GW i P-GW
    - P-GW dodjeljuje IP adresu UE
    - MME uspostavlja vezu između eNodeB i S-GW
    - aktivira se UE kontekst
- VoLTE
  - prijenos govora putem pokretne mreže temeljene na IP protokolu
  - arhitektura se temelji na IMS-u (IP Multimedia Subsystem)
  - problem: veliki broj signalizacijskih poruka kod prijenosa govora
- povezivanje s WLAN mrežama
  - ne omogućava pokretljivost korisnika
  - pristup internetu velikim brzinama
  - PDG (Packet Dana Gateway) – provodi registraciju korisnika spojenih na WLAN
    - lokalna IP adresa – javna IP adresa
    - sadrži informacije o usmjeravanju podataka za korisnike spojene preko mreže WLAN na Internet
  - WAG (WLAN Access Gateway) – osigurava vezu s internetom preko odgovarajućeg PDG-a
    - vatrozid
    - generira informacije o naplati
- Mobile TV
  - velik broj simultanih konekcija
  - pokretno više-odredišno razašiljanje
  - triple play u pokretnom telefonu – govor, video, podaci
  - novi čvor u jezgrenoj mreži – centar za više-odredišno razašiljanje
  - zauzimanje mrežnih resursa ne ovisi o broju korisnika koji traže uslugu već isključivo o broju različitih sadržaja koji se nude
- femto ćelije – bežične pristupne točke male snage, rade u licenciranom dijelu spektra
  - služe za spajanje standardnih pokretnih uređaja na mrežu pokretnog operatora preko DSL-a ili širokopojasnog kabelskog pristupa

Sigurnost pokretne mreže

- identifikacija korisnika i opreme:
  - MSISD – dodjeljuje mrežni operator
  - IMSI – dodjeljuje mrežni operator
  - IMEI – dodjeljuje proizvođač opreme
    - 15 znamenki
    - trajno zapisan u memoriji pokretnog uređaja i ne može se promijeniti
  - MSISDN i IMSI su međusobno odvojeni čime je ostvarena bolja sigurnost i tajnost korisnika
- tajni ključ – Ki
  - jedinstven, 128 bita
  - osiguranje komunikacije na zračnom sučelju
  - ne izmjenjuje se kroz mrežu već se izravno upisuje u SIM i AUC
  - algoritmi A3 i A8
- pohrana identifikacije i ključeva:
  - SIM – IMSI, MSISDN, Ki, algoritmi A3 i A8
  - HLR – IMSI, MSISDN
  - AUC – Ki
  - EIR – IMEI
- autentičnost pretplatnika
  - poznavanje IMSI-a omogućuje lažno predstavljanje i neovlašten pristup mreži jer je IMSI jednoznačno povezan s MSISDN-om
  - zaštita: provjera autentičnosti SIM-a prilikom zahtjeva za registracijom
    - HLR od AUC-a traži Ki i generira pet trojki
      - trojka – RAND, SRES, Kc
        - RAND – 128 bitni slučajni broj
        - SRES = A3(RAND, Ki), 32 bita
        - Kc – 64 bita, generiran pomoću Ki, ključ za šifriranje
      - MSC odabire jednu trojku
- autentičnost opreme
  - gubitak ili krađa pokretne opreme
  - zaštita: kompromitiranom MS-u ne omogućuje se autentifikacija
    - kompromitiranom SIM-u se zabranjuje pristup mreži
- anonimnost pretplatnika
  - dohvaćanjem IMSI na zračnom sučelju, može se ustanoviti pretplatnikova lokacija i pratiti kretanje
  - zaštita: nakon provjere identiteta pretplatnika, VLR mu dodjeljuje privremeni identitet TMSI čime se smanjuje upotreba IMSI na zračnom sučelju
- tajnost komunikacije
  - prisluškivanje na zračnom sučelju
  - zaštita: šifriranje podataka na zračnom sučelju

- algoritam A5, sjednički ključ Kc
  - svaka komunikacija – drugi ključ
  - šifriranje se obavlja koristeći algoritam A5 i ključ Kc
- algoritam A8 – zapisan je na SIM-u
  - služi za generiranje 64 bitnog ključa Kc
  - Kc = A8 (RAND, Ki)

GPRS

- identifikacija i autentifikacija slične kao kod GSM-a
  - SGSN vrši autentifikaciju i šifriranje podataka pomoću sigurnosnih algoritama i ključeva koji su prilagođeni paketskom prijenosu podataka
  - umjesto TMSI koristi se TLLI (Temporary Logical Link Identity) i RAI (Routing Area Identity)
  - sedam GPRS algoritama (GEA) za zaštitu komunikacijskog kanala i podataka
  - mrežna sigurnost – vatrozid

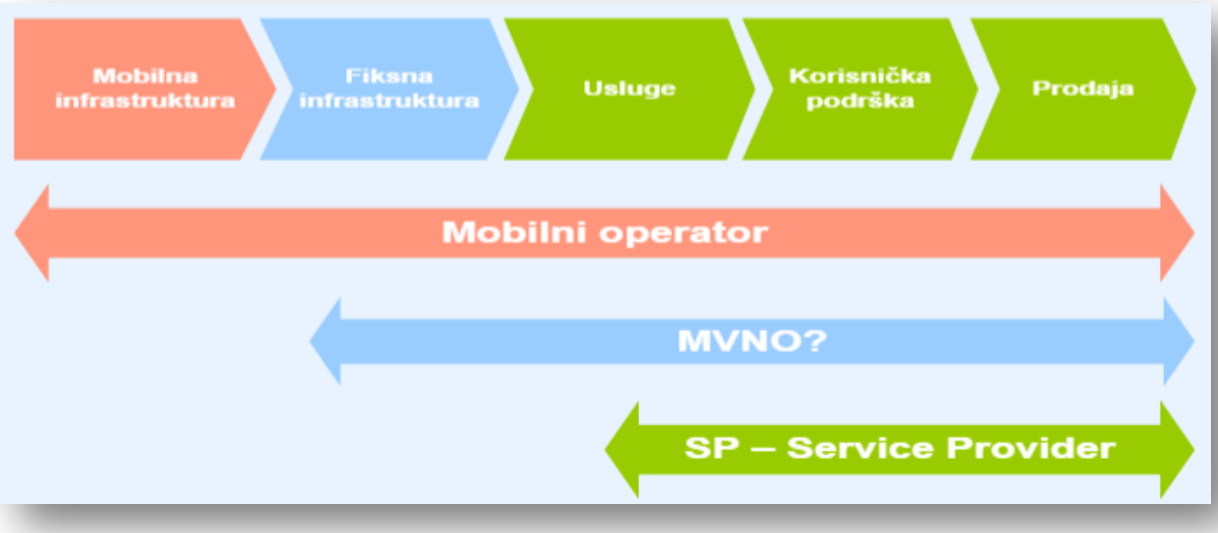
UMTS

- sigurnosne skupine
  - sigurnost mrežnog pristupa
  - sigurnost domene operatora
  - sigurnost korisničke opreme
  - sigurnost aplikacija
- za razliku od GMS kod kojeg se provodi samo autentifikacija korisnika, u UMTS mreži se provodi uzajamna identifikacija korisnika i mreže
  - postupak autentifikacije uključuje:
    - slučajni broj – RAND
    - XRES
    - ključ šifriranja - Kc
    - ključ integriteta – IK
    - autentifikacijski token za mrežnu autentifikaciju (AUTN)
- tajnost komunikacije – provjera cjelovitosti i poboljšani postupak autentifikacij
  - provjera cjelovitosti provjerava se između UE i RNC-a
  - ključevi za šifriranje se duži nego kod GSM-a
  - UMTS Integrity Algorithm – UIA, f9 algoritam za provjeru cjelovitosti
  - algoritam f8 – šifriranje korisničkih i signalizacijskih podataka
    - računaju se zaštitni bitovi i provodi XOR operacija između tako izračunatog slijeda i podataka koji se šalju
    - na odredištu se na isti način računaju zaštitni bitovi i provodi XOR operacija iz čega se dobiva poslani podatak
- mrežna sigurnost – komunikacija čvorova u jezgrenoj mreži obavlja se preko sigurnosne inačice MAP (Mobile Application Part) protokola – MAP sec

- zaštita na aplikacijskom sloju, dodavanje posebnih sigurnosnih zaglavlja koja štite poruke
- IPsec
  - sigurnosni prilazi- SEG-ovi
  - IPsec ESP tunel
  - AES protokol
- usmjerivači, vatrozidi, posrednički poslužitelji za filtriranje prometa

Virtualni operator pokretne mreže

- MVNO – Mobile Virtual Network Operator
- nudi pokretne usluge korisnicima
  - ne posjeduje koncesiju frekvencijskog spektra
  - ne posjeduje vlastitu infrastrukturu
  - mrežnim operatorima koji posjeduju koncesiju plača korištenje njihove pokretne mreže
- vitrualni operator je zapravo preprodavač usluga pokretne mreže, kupuje usluge od mrežnih operatora na veliko pa ih preprodaje svojim korisnicima
- prednosti – minimalno ulaganje i konkurentnost
- nedostaci
  - nude osnovne usluge na teritorijalno ograničenom području
  - ne nude usluge prelaženja (roaminga)
  - ne nude korisnicima posebne ponude i pogodnosti
- davatelj usluge
  - service provider
  - nudi određene usluge
  - nema mrežnu infrastrukturu, ali posjeduje potrebnu opremu (poslužitelje)



Slika 7. Odnos mobilnog operatora, MVNO-a i davatelja usluga

- kategorije MVNO:
  - četiri tipa prema rastućoj neovisnosti
  - MVNO-1
    - u potpunosti preuzima mrežnu infrastrukturu od svog operatora
    - pruža osnovne usluge
    - nizak trošak ulaganja, mali rizik poslovanja
  - MVNO-2
    - posjeduje određene čvorove pokretne mreže (HLR)
    - vlastite SIM kartice za korisnike
    - nudi neke dodatne usluge
  - MVNO-3
    - posjeduje djelomično vlastitu infrastrukturu (MSC, HLR)
    - nudi niz dodatnih naprednih usluga
    - vlastita podrška za inteligentnu mrežu
    - vlastite usluge
  - MVNO-4
    - posjeduje vlastitu infrastrukturu (MSC, HLR, GMSC)
    - podržava vlastito usmjeravanje prometa (GMSC)
- primjeri – automobilska tvrtka, aviokompanija
  - u HR: Bonbon, Multiplus, Telco Grupa, ZABA, Tomato
- virtualni omogućitelj pokretne mreže – MVNE (Mobile Virtual Network Enabler)
  - nema izravan kontakt s korisnicima
  - nudi tehničku infrastrukturu (HLR, SMS-C, MMS-C, SGSN, GGSN)
  - usluge naplate
  - administracija
  - podrška za bazne postaje
  - niz pokretnih usluga
  - primjer HR – Aspider Soulutins