Preddiplomski studij

Javna pokretna mreža

9.

Komunikacija porukama

Sigurnost pokretne mreže

WAP

AIPN, LTE

Ak.g. 2007./2008.

Svibanj 2008.

Sadržaj predavanja

- Komunikacija porukama
- Sigurnost pokretne mreže
- Bežični aplikacijski protokol
- Evolucija mreže nakon 3G
- Prijenosi preko mreže IP

Preddiplomski studij

Komunikacija porukama

Ak.g. 2007./2008.

Svibanj 2008.

Komunikacija porukama

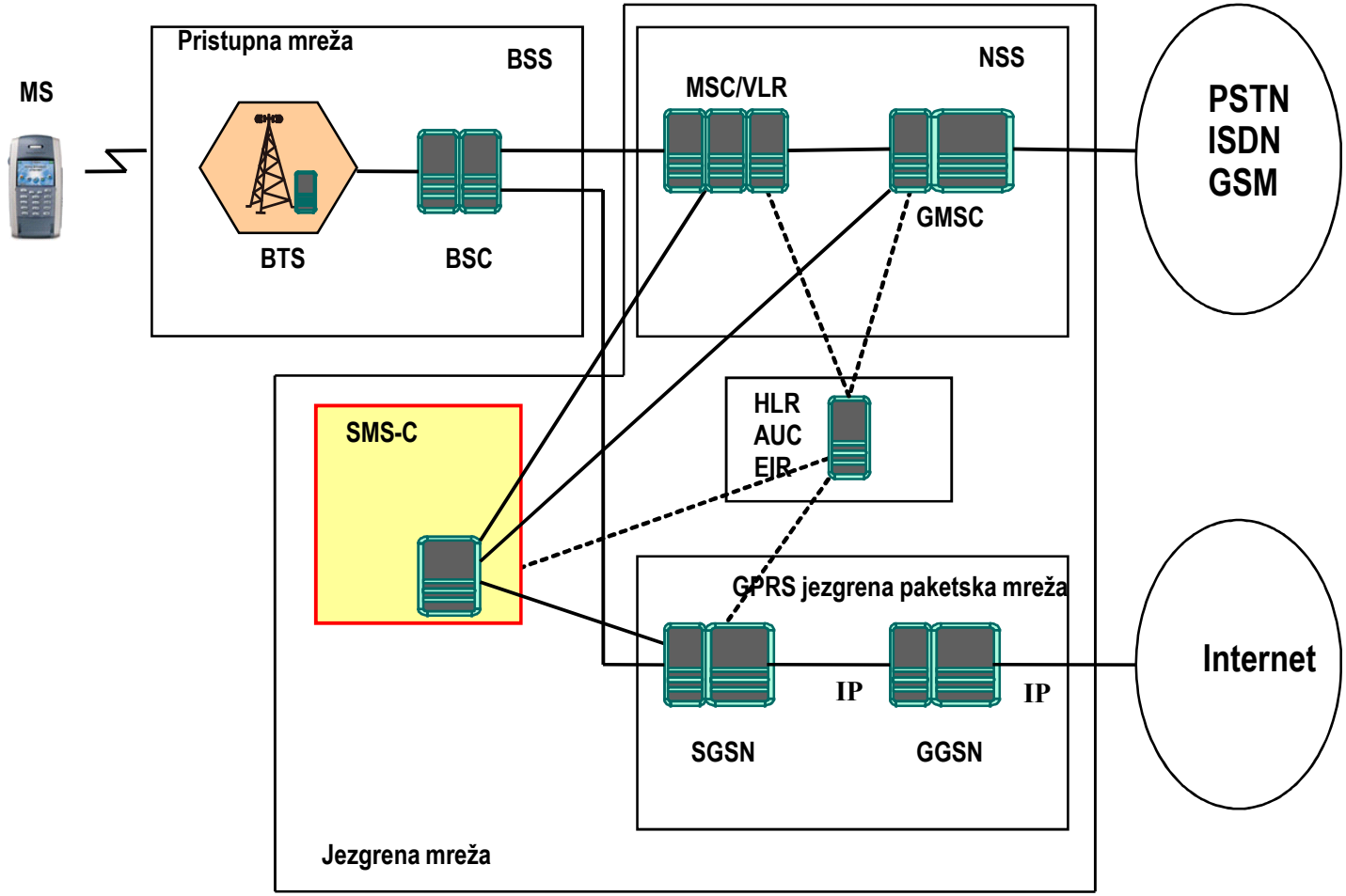
- Usluga kratkih poruka (*Short Messaging Service*, SMS)
- Poboljšana usluga izmjene poruka (*Enhanced Messaging Service*, EMS)
- Usluga višemedijskih poruka *(Multimedia Messaging Service*, MMS)

SMS usluga

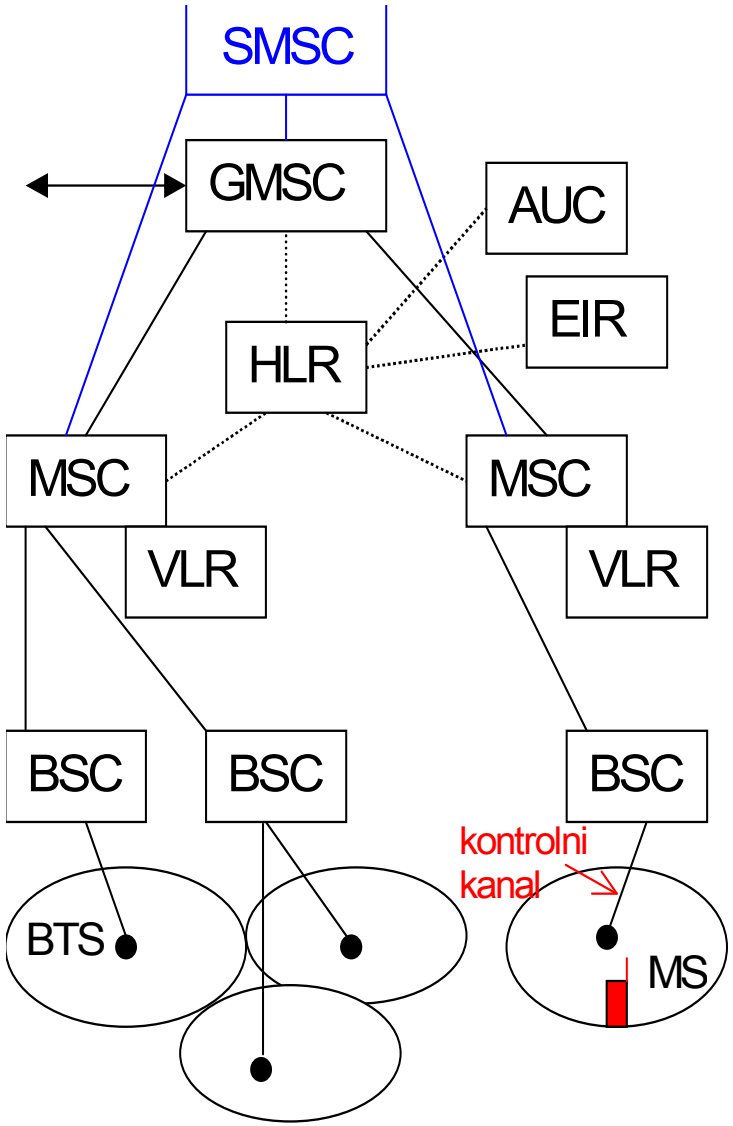
- Uvodi se posebni centar za uslugu kratkih poruka (*Short Message Service Centre*, SMS-C)
  - Primanje i slanje SMS pruka od/prema pokretnoj postaji
  - Zadržava poruku dok ne dobije poruku o primitku ili dok ne istekne definirano vrijeme valjanosti poruke
- Duljina poruke je 160 znakova, uz mogućnost ulančavanja

- EMS proširuje sadržaj poruke
  - Uz tekst, točkaste slike i kratke melodije

Arhitektura za podršku SMS usluge



Usluga kratkih poruka



SMS (i EMS)

- Poruke se prenose kontrolnim kanalom u pristupnoj mreži
- Poruke prihvaća, pohranjuje i prosljeđuje SMSC (*SMS Centre*)

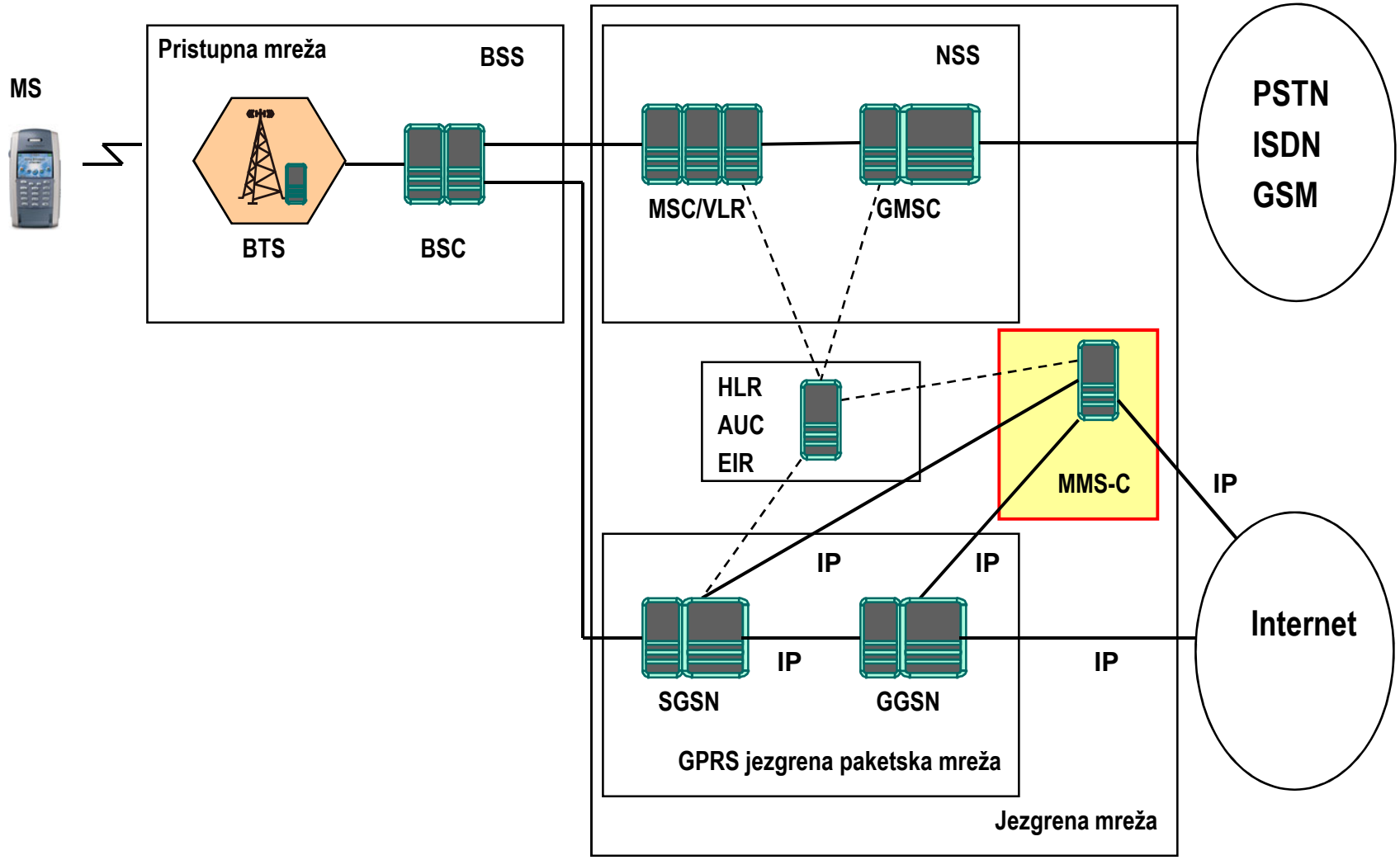
MMS usluga

- Usluga razmjene poruka bogatog sadržaja
  - Zahtijeva veće brzine prijenosa podataka
  - Formatirani tekst, crtež, slika u boji, animacija, audio i video sadržaji

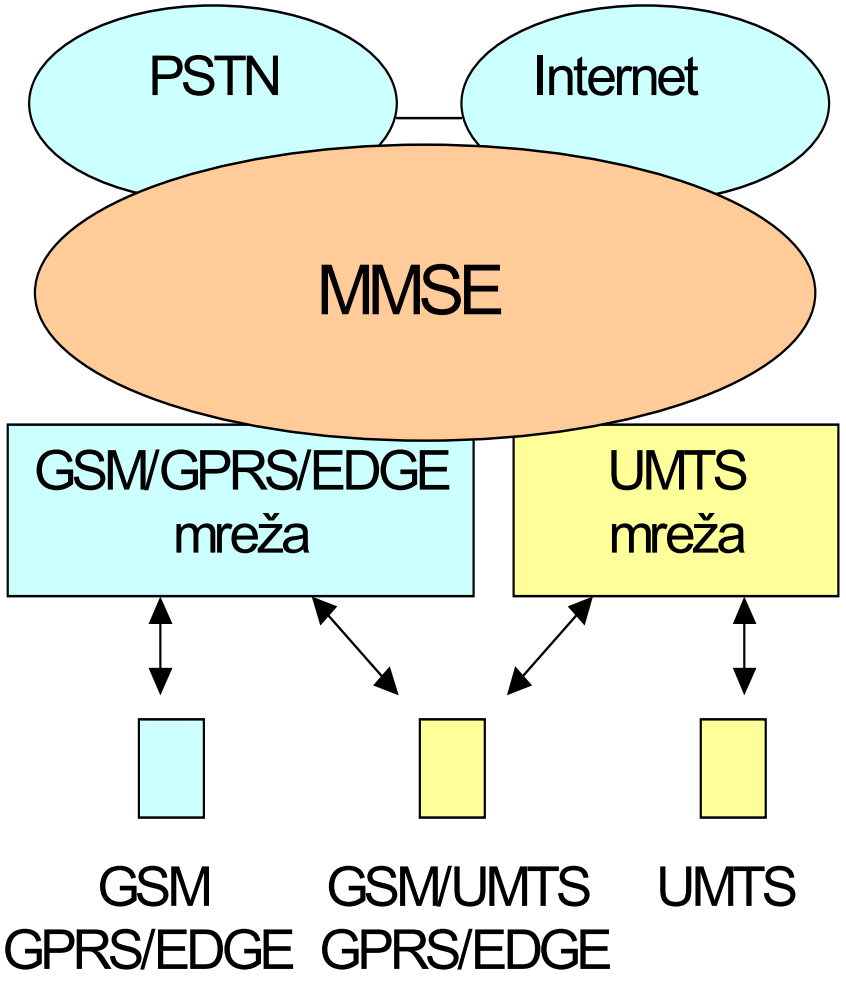
- Prijenos MMS poruka temelji se na WAP (*Wireless Application Protocol*) protokolima

- Uvodi se centar za izmjenu višemedijskih poruka (*Multimedia Messaging Service Center*, MMS-C)

Arhitektura za podršku MMS usluge



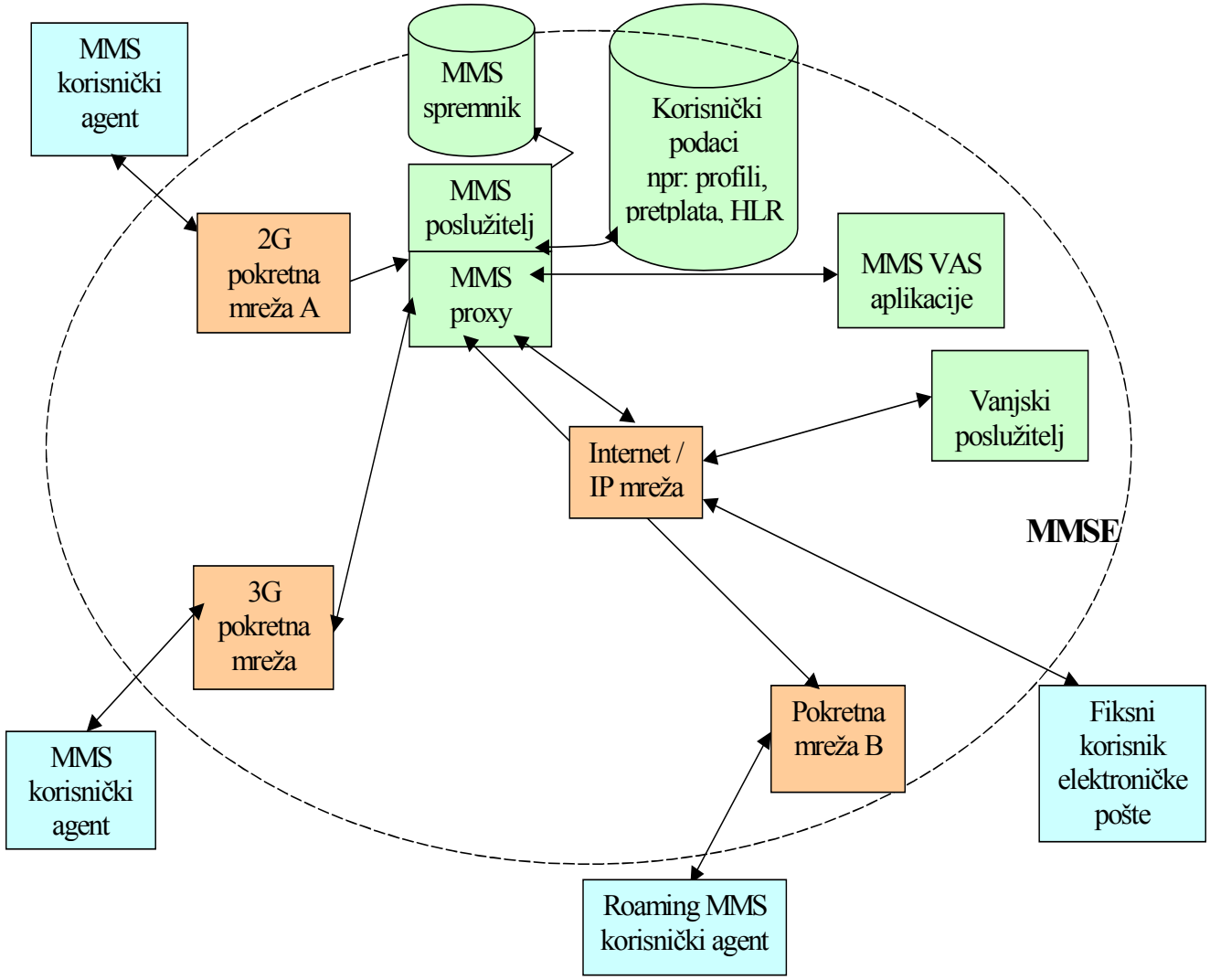
Izmjena višemedijskih poruka (1)



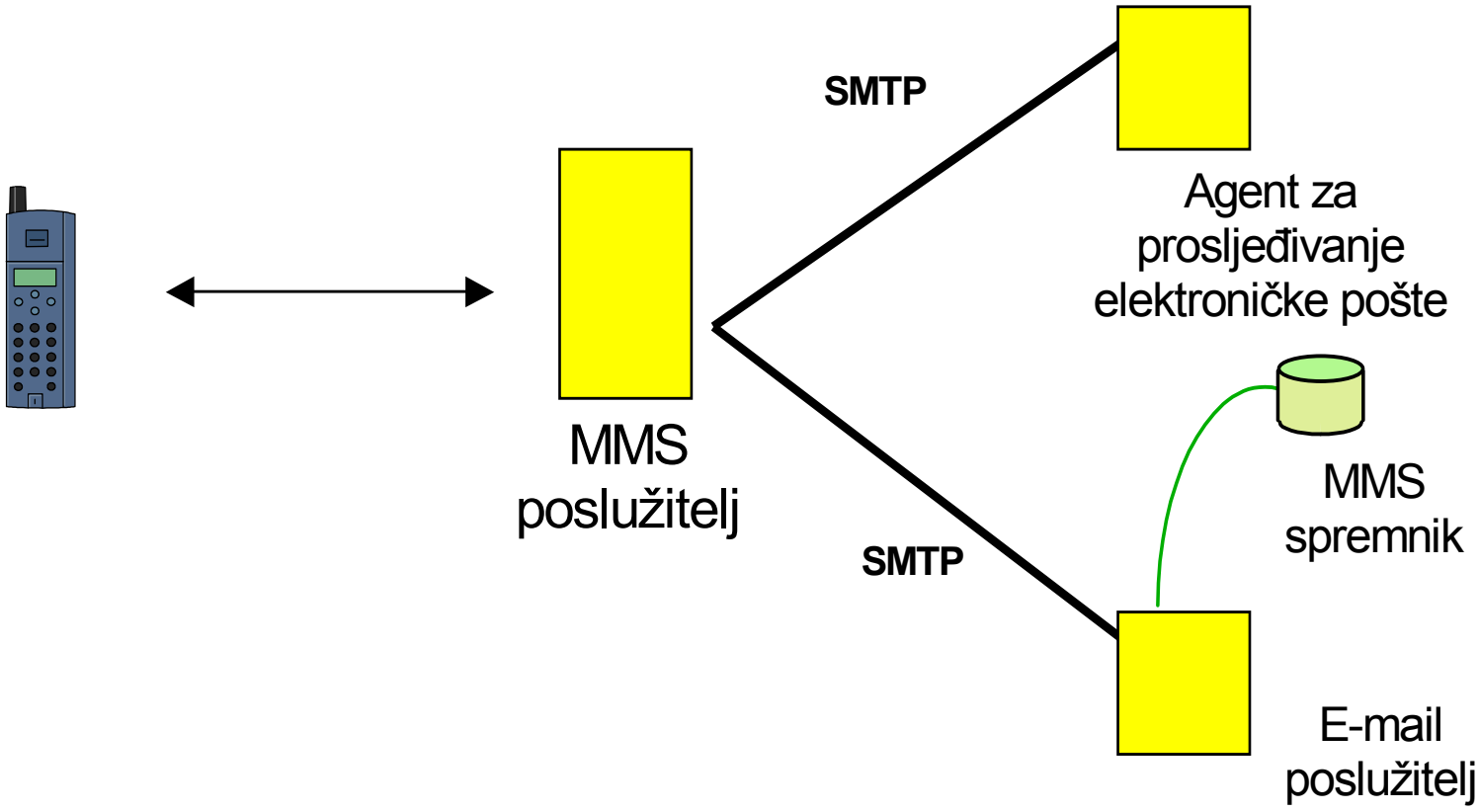
MMSE

Multimedia Messaging Service Environment

Izmjena višemedijskih poruka (2)



Primjer: MMS – E-mail



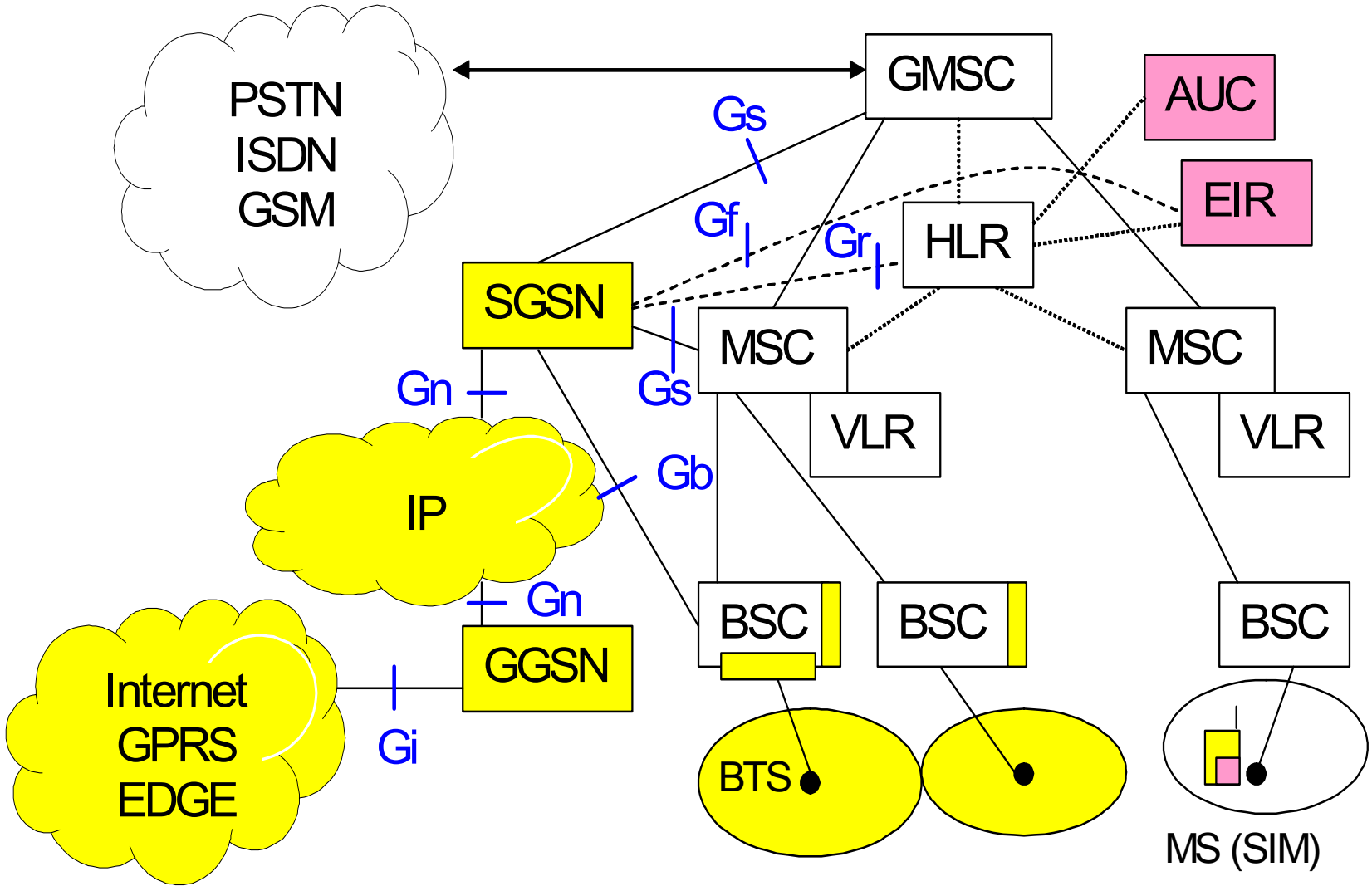
Preddiplomski studij

Sigurnost pokretne mreže

Ak.g. 2007./2008.

Svibanj 2008.

Sigurnost u mreži GSM



Identifikacija korisnika i opreme

MSISDN (*Mobile Subscriber* ISDN) number

- pozivni broj pokretnog pretplatnika
- dodjeljuje mrežni operator

IMSI (*International Mobile Subscriber Identity*)

- međunarodni identitet pokretnog pretplatnika
- dodjeljuje mrežni operator

IMEI (*International Mobile Equipment Identity*)

- međunarodni identitet pokretne opreme
- dodjeljuje proizvođač opreme

Tajni ključ

K_i

- jedinstven, 128 bita
- osiguranje komunikacije na zračnom sučelju (MS-BTS)
- ne izmjenjuje se kroz mrežu, već se izravno upisuje u SIM i AUC
- algoritmi A3 (SRES) i A8 (Kc) za sigurnosni vektor

Pohrana identifikacije i ključa

SIM (*Subscriber Identity Module*)

- MSISDN, IMSI
- Ki, algoritmi A3 i A8

HLR (*Home Location Register*)

- MSISDN, IMSI

AUC (*Authentication Centre*)

- Ki

EIR (*Equipment Identity Register)*

- IMEI

Autentičnost pretplatnika (1)

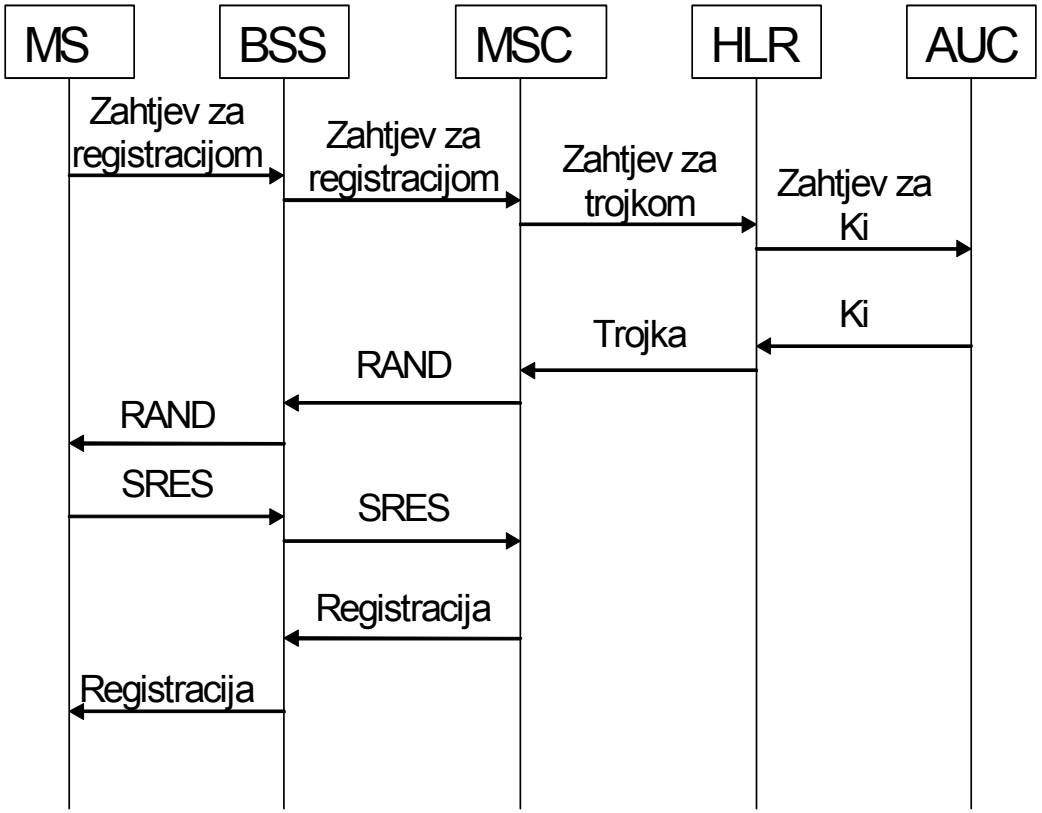
Sigurnosna prijetnja

- poznavanje IMSI omogućuje lažno predstavljanje i neovlašteni pristup mreži, jer IMSI je jednoznačno povezan s MSISDN

Zaštita

- provjera autentičnosti SIM-a prigodom zahtjeva za registracijom
- pretpostavke:
  - sigurni BSS, MSC, VLR i AUC
  - povjerenje između BTS i BSC, BSC i MSC, MSC i HLR te HLR i AUC

Autentičnost pretplatnika (2)



(RAND, SRES, Kc)

RAND – slučajni broj,128 bita

SRES – odgovor na RAND generiran s Ki, 32 bita

Kc – sjednički ključ (tajnost), generiran s Ki, 64 bita

HLR generira 5 trojki

MSC odabire jednu trojku

MSC uspoređuje SRES-ove

Autentičnost opreme

Sigurnosna prijetnja

- gubitak ili krađa pokretne opreme

Zaštita

- prijava gubitka ili krađe opreme mrežnom operatoru zapisuje se u EIR:
  - kompromitiranom MS ne omogućuje se autentifikacija
- i HLR :
  - kompromitiranom SIM-u zabranjuje se pristup mreži

Anonimnost pretplatnika

Sigurnosna prijetnja

- mreža upotrebljava IMSI za obradu poziva i usluga
- IMSI je jednoznačno povezan s MSISDN
- dohvaćanjem IMSI na zračnom sučelju može se ustanoviti pretplatnikova lokacija i pratiti kretanje

Zaštita

- nakon provjere autentičnosti pretplatnika, mreža mu dodjeljuje privremeni identitet TMSI (*Temporary Mobile Subscriber Identity*), čime se smanjuje upotreba IMSI na zračnom sučelju
- preslikavanje IMSI-TMSI provode VLR i MSC

Tajnost komunikacije

Sigurnosna prijetnja

- prisluškivanje na zračnom sučelju

Zaštita

- šifriranje podataka na zračnom sučelju:
  - algoritam A5 (u MS)
  - sjednički ključ Kc (svaka komunikacija novi Kc)

Preddiplomski studij

Bežični aplikacijski protokol

Ak.g. 2007./2008.

Svibanj 2008.

Bežični aplikacijski protokol - WAP

WAP (Wireless Application Protocol)

Namjena

Pretraživanje informacija na Internetu

- WWW na pokretnom telefonu

Dodatne usluge

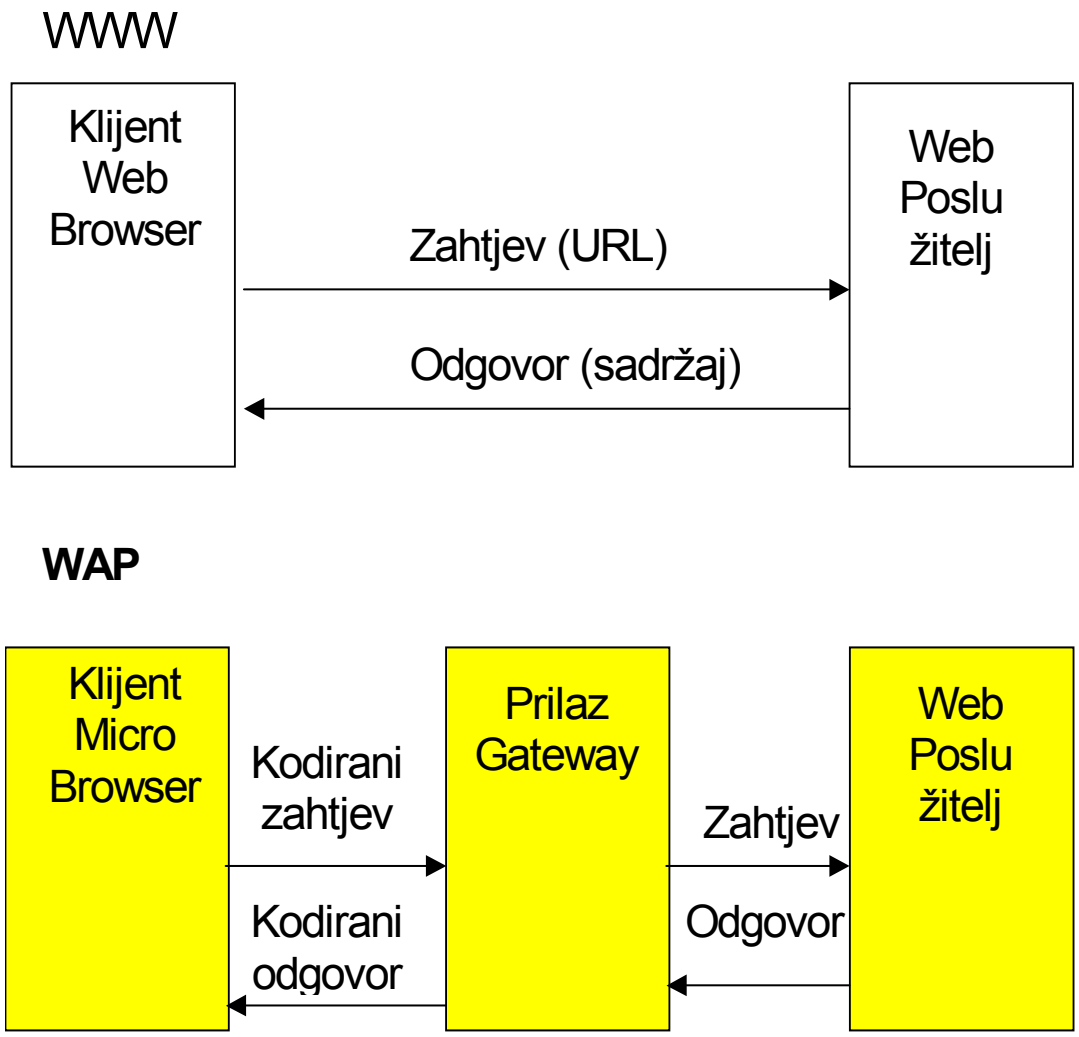
- označavanje pristiglih poruka (e-mail, govorne poruke, odabrane informacije, ...)

m-trgovina

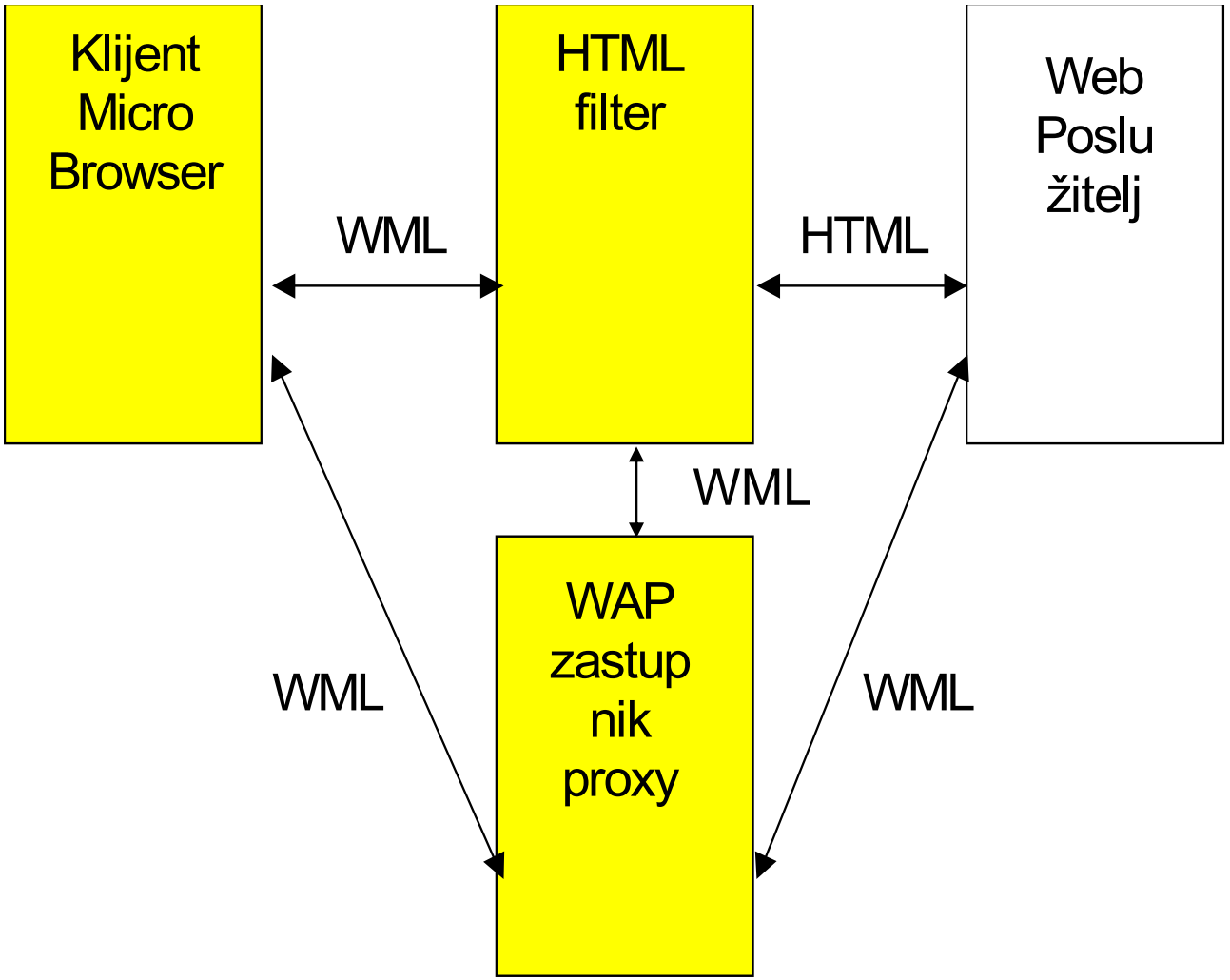
- rezervacija, narudžba, plaćanje

MMS

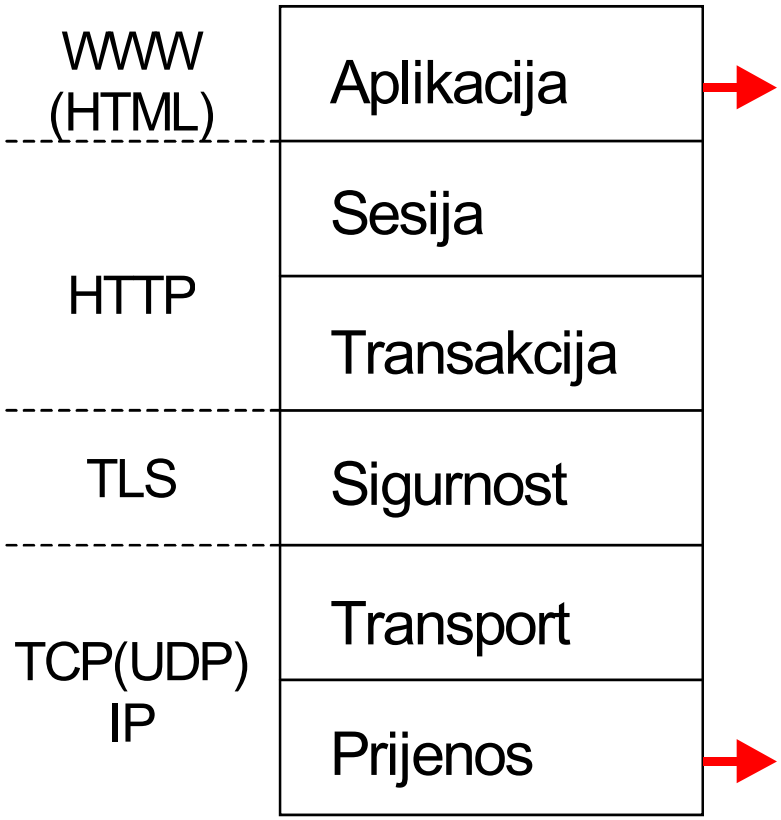
Primjer: WWW - WAP (1)



Primjer: WWW – WAP (2)



Arhitektura WAP-a

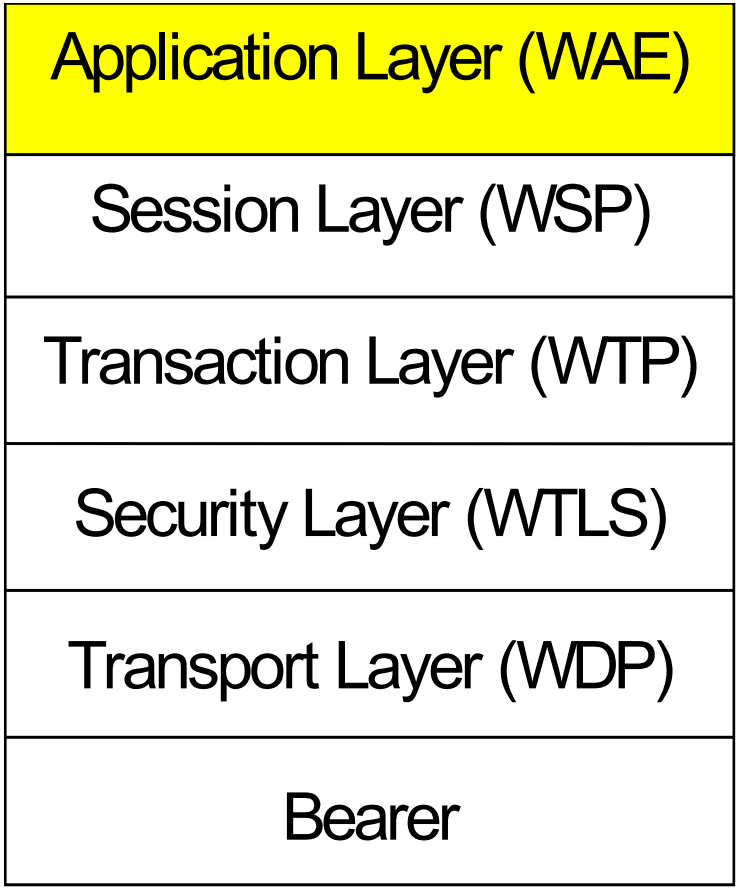


Micro Browser, MMS, ….

Komunikacijski protokoli prilagođeni uvjetima u pokretnoj mreži i mogućnostima korisničkih uređaja

GSM, GPRS, EDGE,UMTS

WAP - aplikacijski sloj

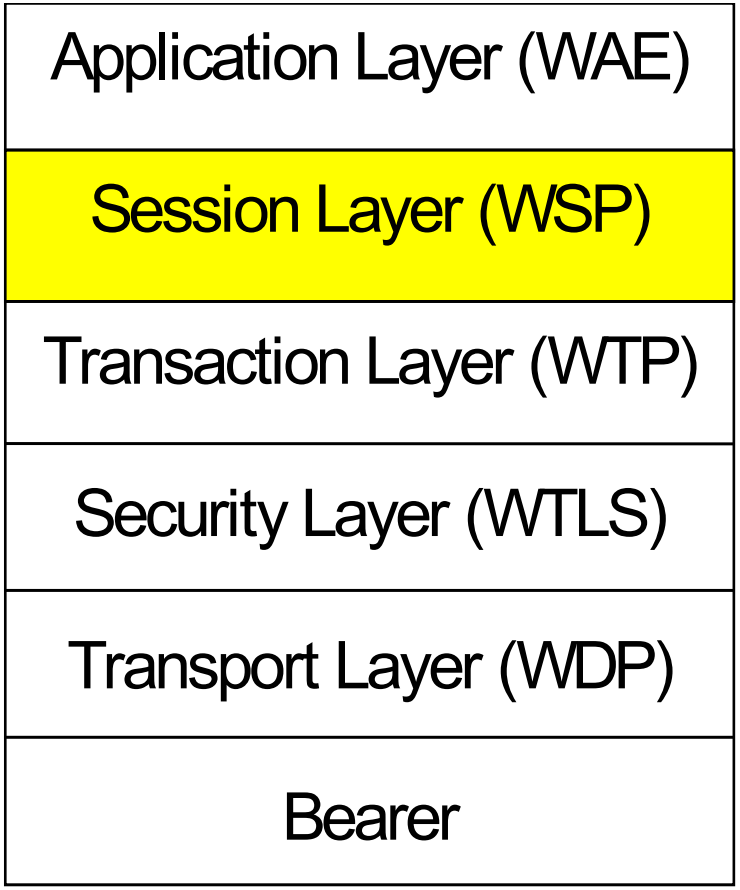


Bežično aplikacijsko okružje

WAE (Wireless Application Environment)

- MMS
- izgradnja aplikacija i usluga za kombinaciju WWW i pokretne telefonije
- WML (Wireless Markup Language) - sličan HTML-u, optimiziran za ručne naprave

WAP - sloj sjednice (sesije)

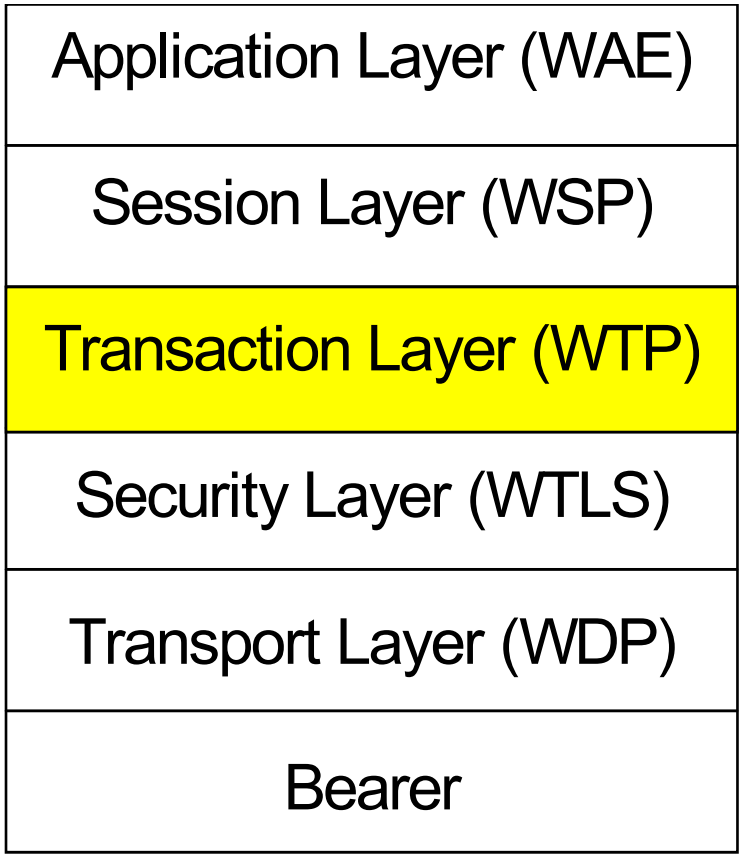


Bežični sjednički protokol

WSP (Wireless Session Protocol)

- optimiziran za mreže s malom propusnosti i velikim kašnjenjem
- klijenta preko WAP proxy na WWW (HTTP)

WAP - transakcijski sloj

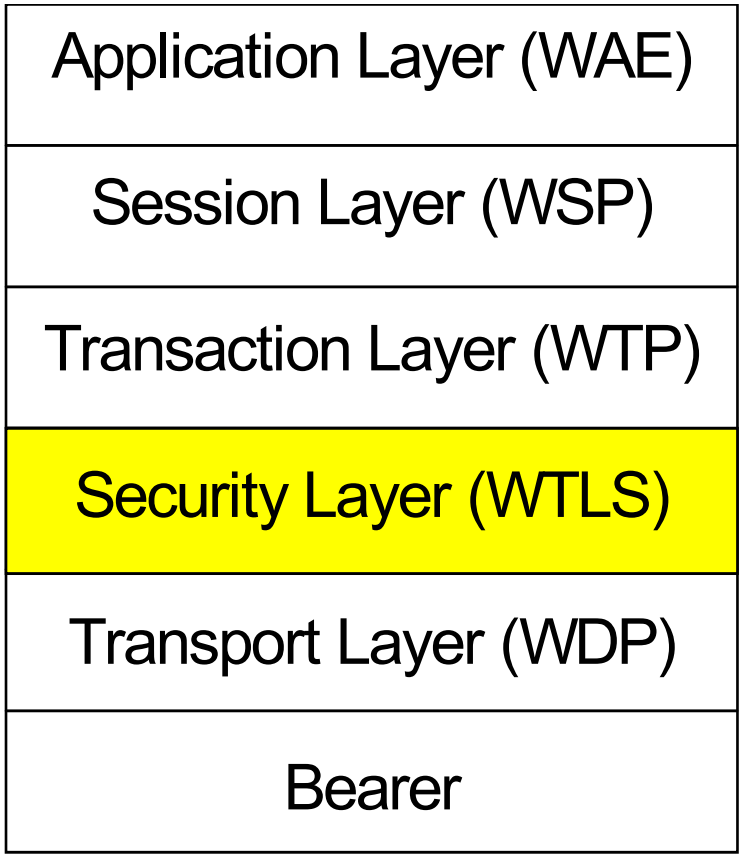


Bežični transakcijski protokol

WTP (Wireless Transaction Protocol)

- optimiziran za ugradnju u uređaj ograničenih mogućnosti (“thin client”)
- Jednosmjerno: zahtjev, dvosmjerno: zahtjev-odgovor

WAP – sigurnosni sloj

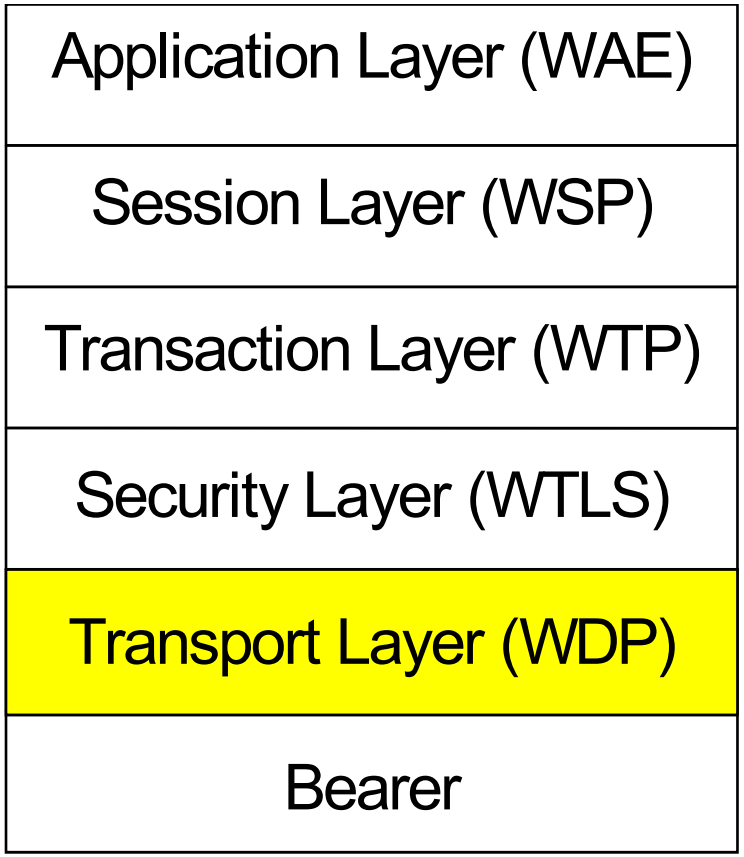


Sigurnost bežičnog transportnog sloja

WTLS (Wireless Transport Layer Security)

- zasnovan na TLS (Transport Layer Security), optimiziran za uskopojasni kanal
- funkcije: integritet podataka, privatnost, autentifikacija, otkrivanje i odbacivanje neprovjerenih podataka
- može se izostaviti!

WAP - transportni sloj



Bežični datagramski protokol

WDP (Wireless Datagram Protocol)

- omogućuje višim slojevima rad u različitim bežičnim mrežama

GSM, GPRS, EDGE,UMTS

Preddiplomski studij

Evolucija mreže nakon 3G

All-IP mrežni koncept

Long Term Evolution (LTE)

Prijenosi mrežom IP

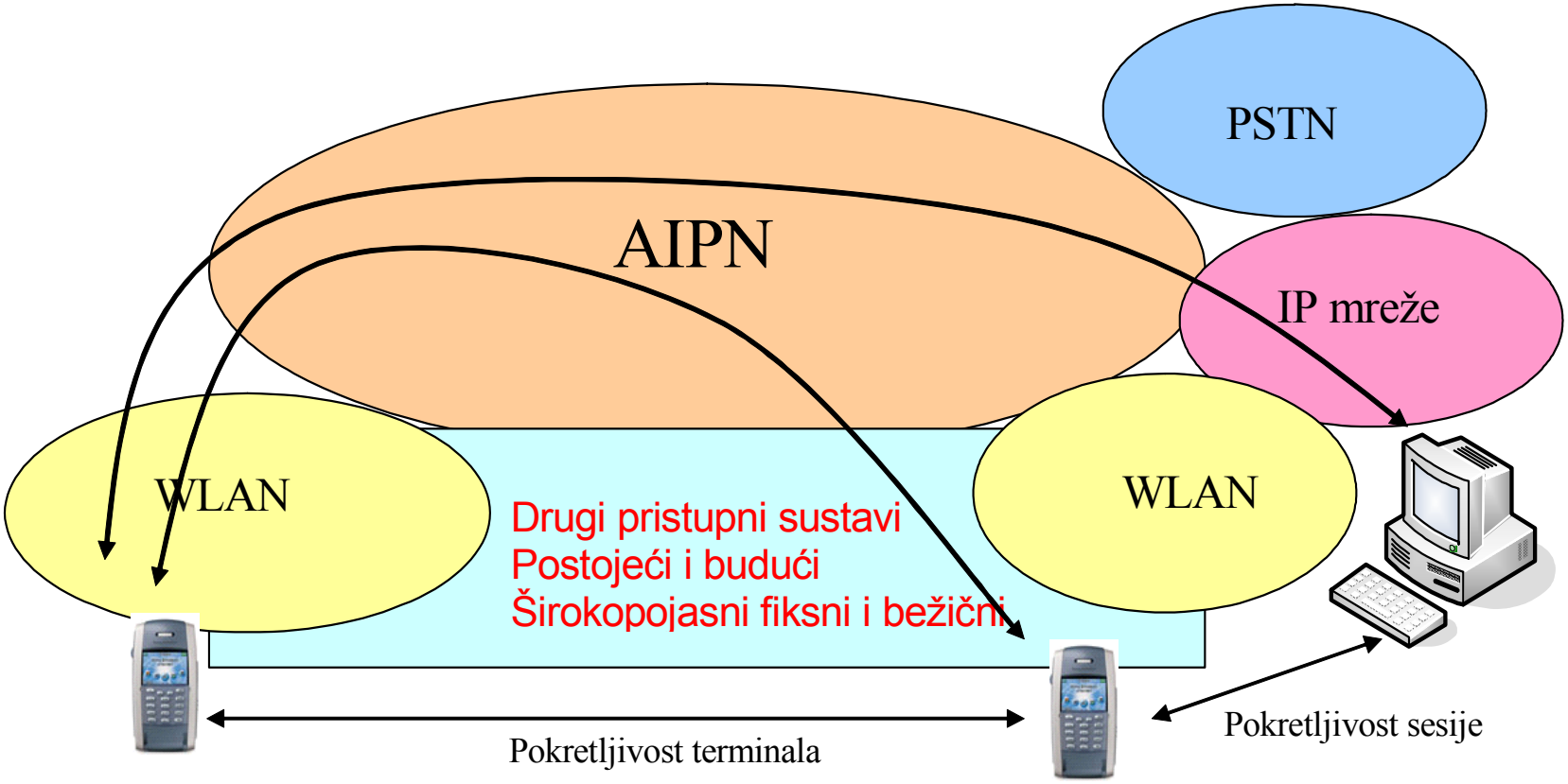
Ak.g. 2007./2008.

Svibanj 2008.

All-IP koncept (R7)

- GERAN i UTRAN pristupne mreže u zajedništvu sa CS i PS domenama te IMS-om
- Veliki porast IP podatkovnog prometa
- Komutacija paketa u 3G mrežama zahtijeva daljnja proširenja
- Daljnja evolucija i optimizacija mreže
- Povezivanje pokretnih mreža s ostalima uz osiguranje pokretljivosti, sigurnosti kvalitetom usluga te upravljanja naplatom

All-IP mreža


PSTN
AIPN
IP mreže
WLAN
WLAN
Drugi pristupni sustavi
Postojeći i budući
Širokopojasni fiksni i bežični
Pokretljivost terminala
Pokretljivost sesije

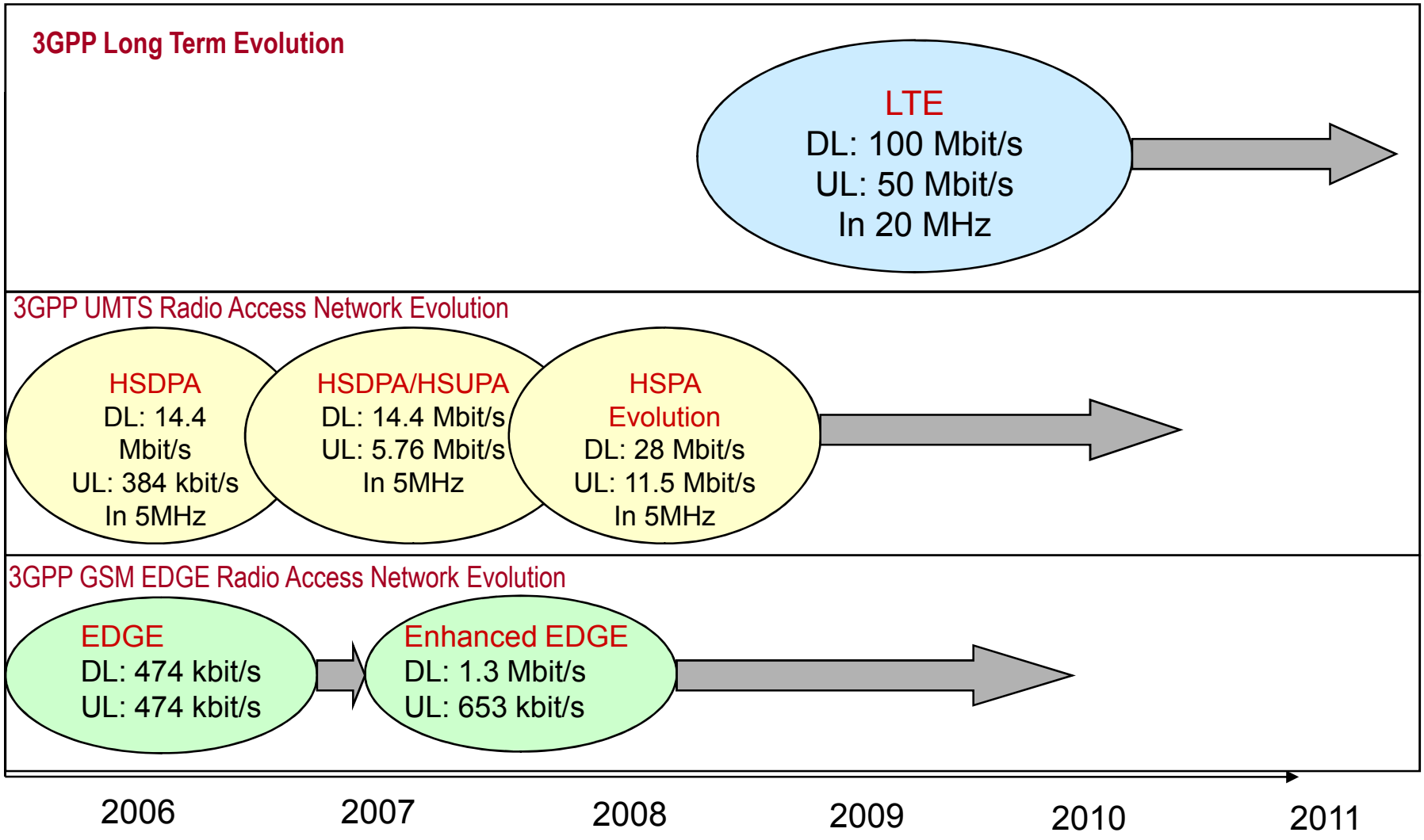
AIPN evolucija (R8)

- Uobičajena IP mreža koja osigurava upravljanje mrežom temeljeno na IP protkolu te transport podataka temeljen na IP mreži putem različitih pristupnih mreža
  - Proširenje upravljanja pokretljivosti
  - Napredne usluge
  - Dodatne funkcionalnosti sigurnosti n privatnosti
  - QoS, terminalska i korisnička identifikacija
  - fiksno/pokretne konvergirane usluge
  - MVNO podrška

Long Term Evolution (LTE)

- Nakon GSM-UMTS-HSPA sustava
- Viša razina kapaciteta i performansi mreže
- Brzina prijenosa podataka do 100 Mbit/s (downlink peak)
- Zahtjevi
  - Potpuna IP mreža
  - Više usluga, niže cijene
  - Fleksibilnije korištenje postojećeg frekvencijskog pojasa (frekvencijski spektar od 20 Mhz)
  - Pojednostavljenje arhitekture, otvorena sučelja
  - 2009. do 2012.
- Thnologija:
  - OFDM (Orthogonal Frequency Division Multiplexing)
  - MIMO (Multiple-Input Multiple-Output) – višestruke antene, više paralelnij strujanja podataka prema pojedinom korisniku
  - HSOPA (High Speed OFDM Packet Access)

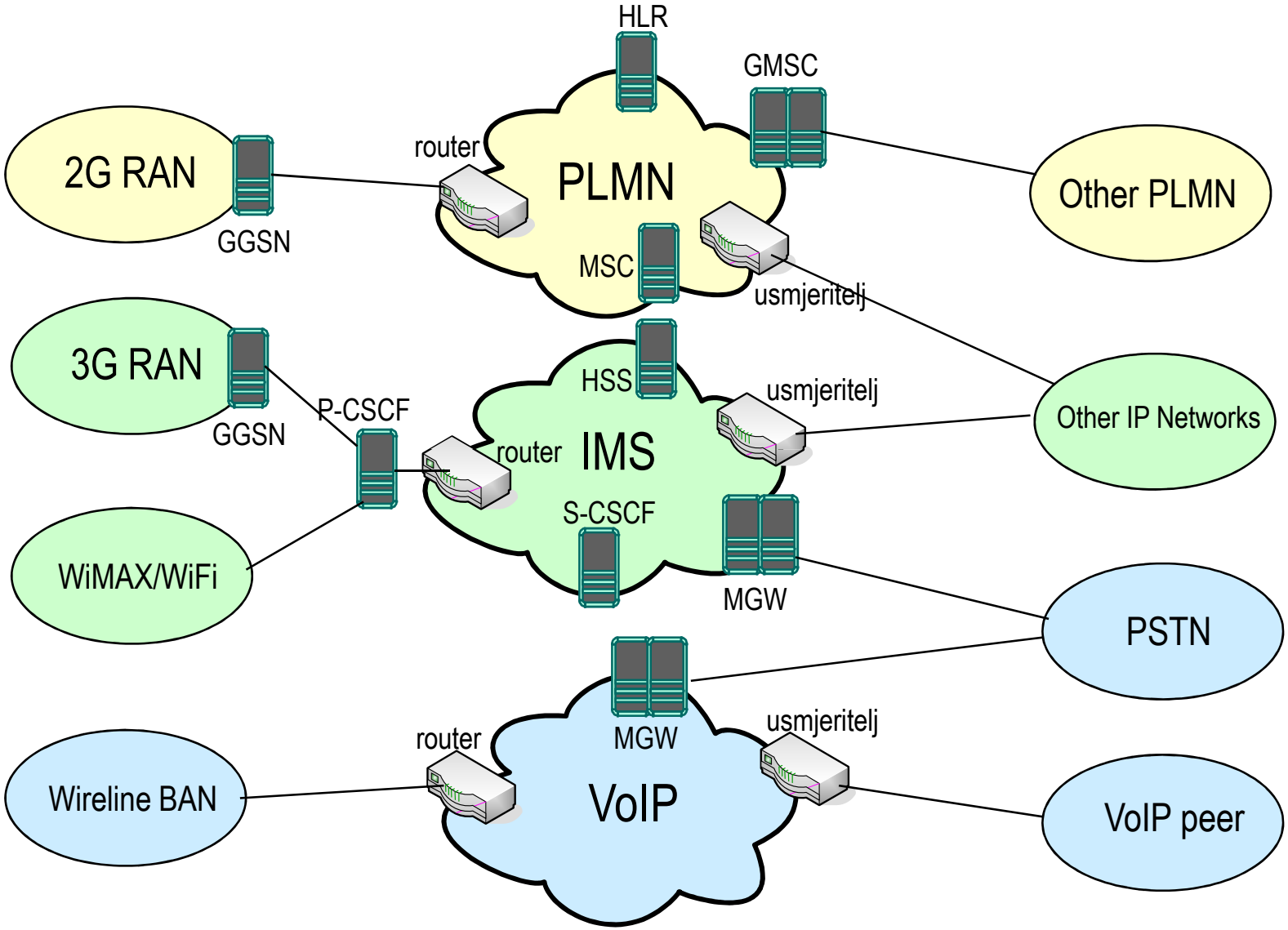
3G prema LTE


3GPP Long Term Evolution
LTE
DL: 100 Mbit/s
UL: 50 Mbit/s
In 20 MHz
3GPP UMTS Radio Access Network Evolution
HSDPA
DL: 14.4 Mbit/s
UL: 384 kbit/s
In 5MHz
HSDPA/HSUPA
DL: 14.4 Mbit/s
UL: 5.76 Mbit/s
In 5MHz
HSPA Evolution
DL: 28 Mbit/s
UL: 11.5 Mbit/s
In 5MHz
3GPP GSM EDGE Radio Access Network Evolution
EDGE
DL: 474 kbit/s
UL: 474 kbit/s
Enhanced EDGE
DL: 1.3 Mbit/s
UL: 653 kbit/s
2006
2007
2008
2009
2010
2011

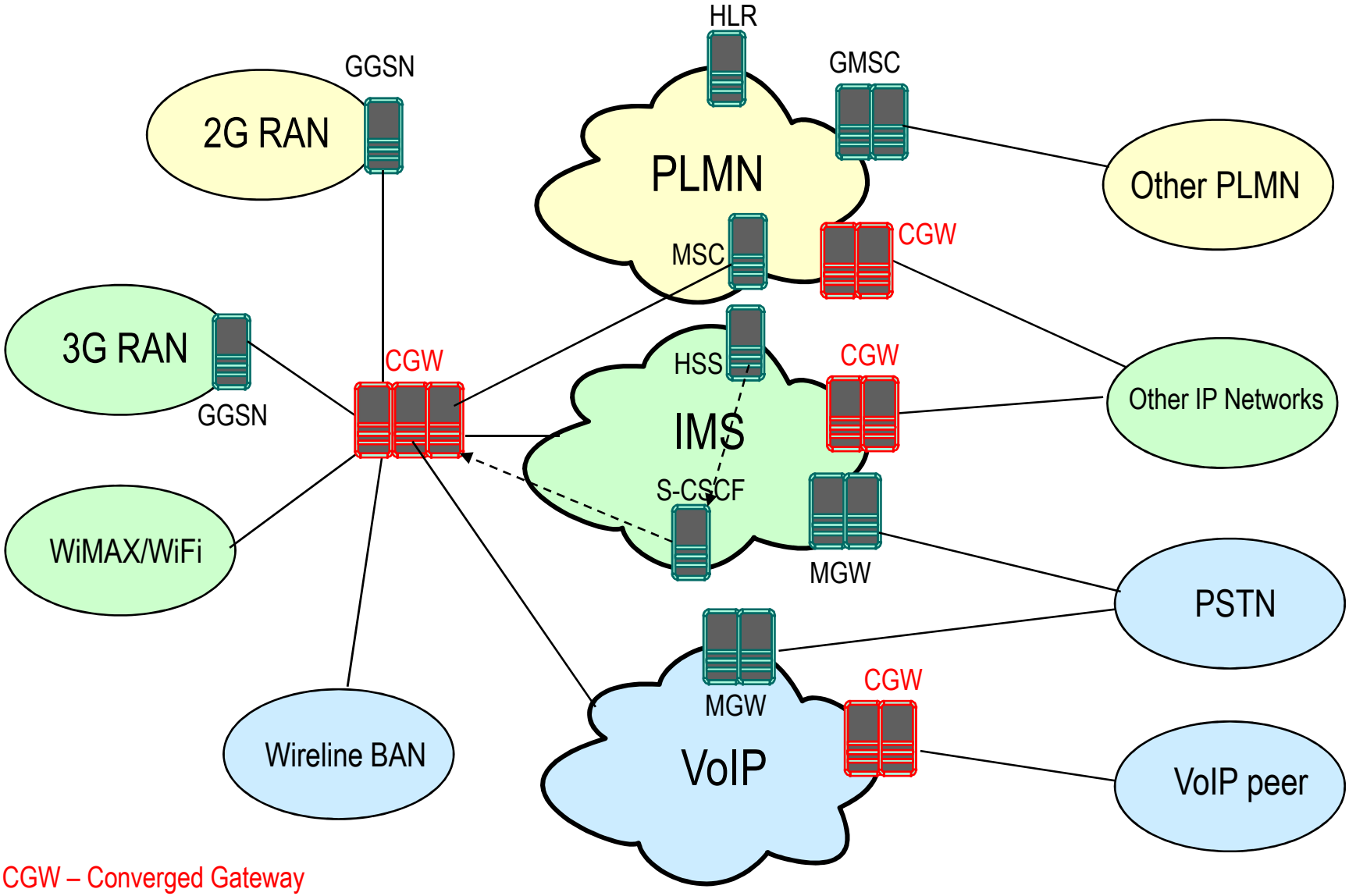
FMC mreža

- Pristupni dio mreže
  - Pokretni RAN
  - WiMAX/WiFi
  - Fixed-Line BAN
- Jezgreni dio mreže
  - Različiti autentifikacijski mehanizmi
  - Različite sigurnosne metode pristupa
  - Različiti zahtjevi QoS
  - Različiti sigurnosni modeli
  - Nema definiranih standarda
  - Cijena, složenost

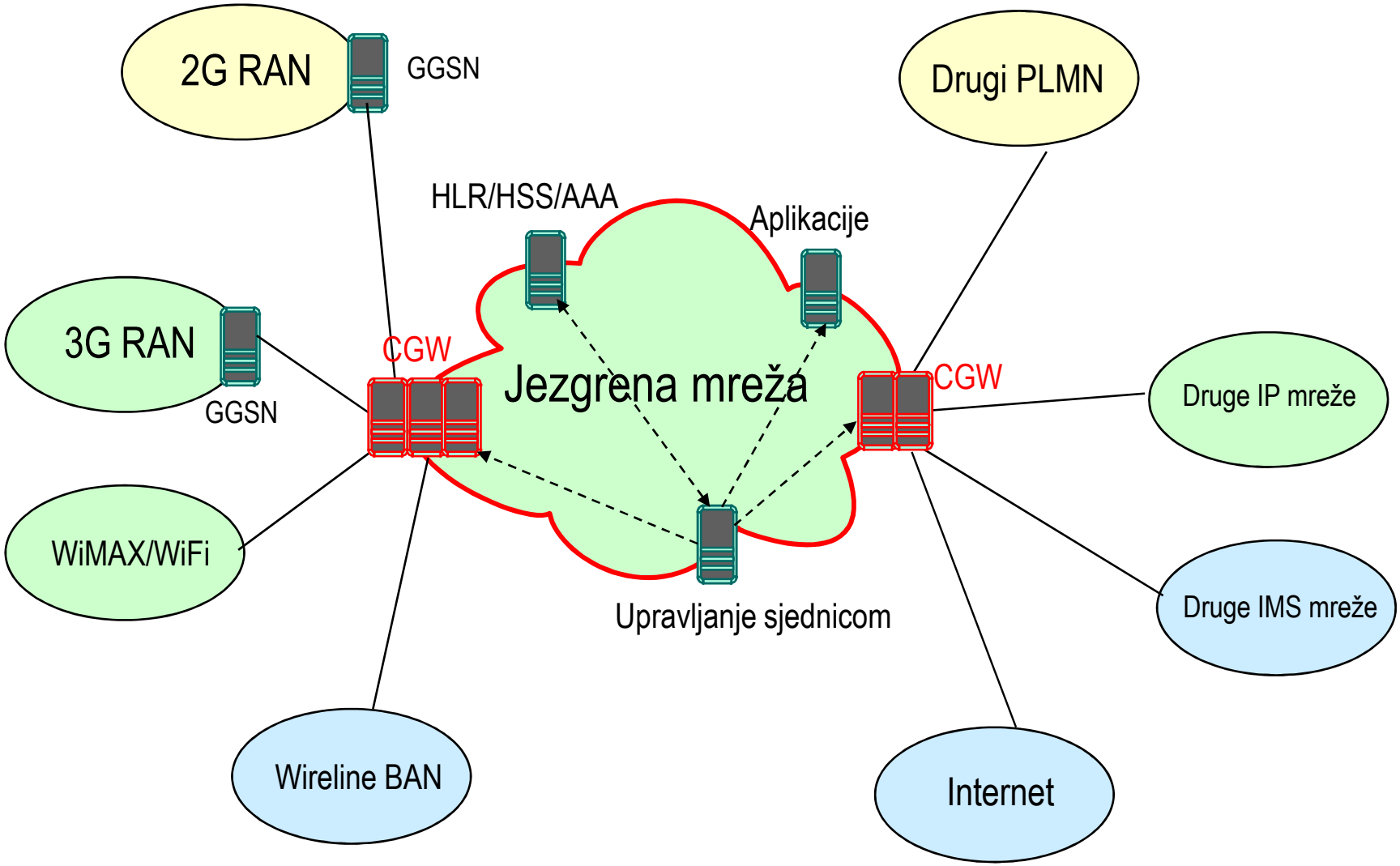
Evolucija prema FMC – prvi korak



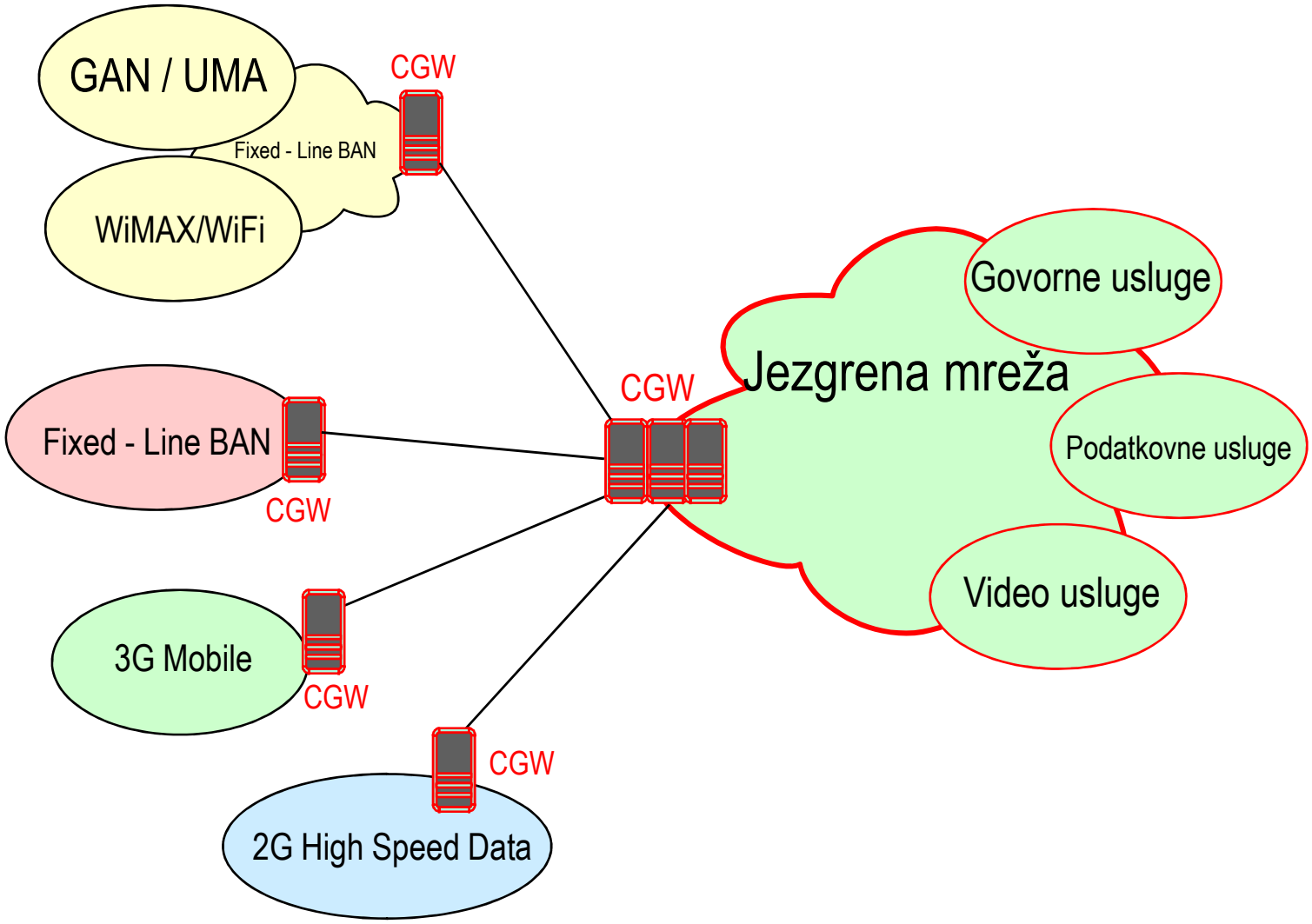
Evolucija prema FMC - više jezgrenih mreža



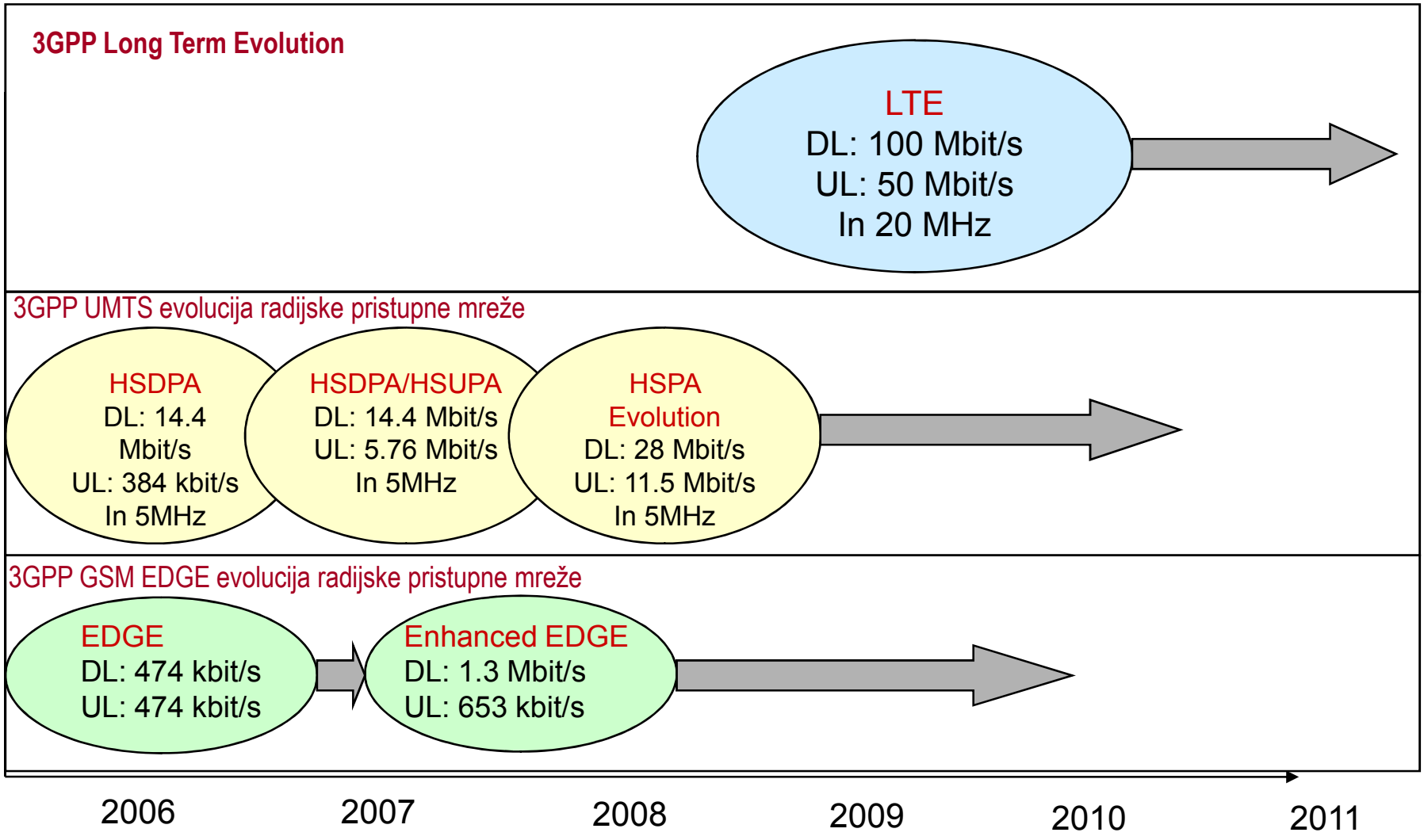
Evolucija prema FMC – konvergirana jezgrena mreža



Evolucija prema FMC – zadnji korak



Od 3G prema LTE



Preddiplomski studij

Prijenosi preko mreže IP

Softswitch

SIGTRAN

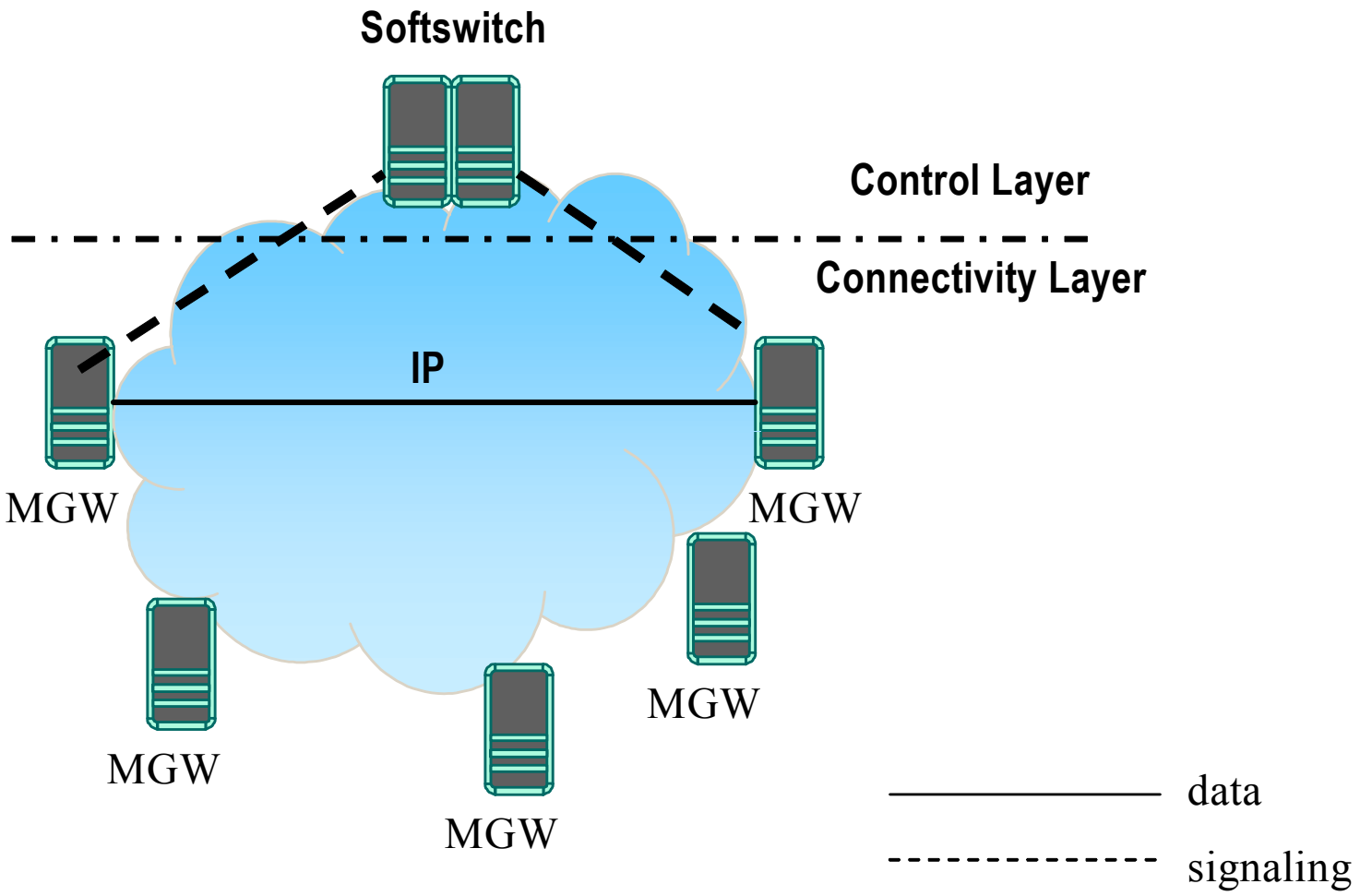
Ak.g. 2007./2008.

Svibanj 2008.

Softswitch

- Softswich: djelotvoran prijenos govora preko IP mreže
- “Prvi korak” prema All-IP architekturi
- Razdvajanje upravljanja pozivom od funkcija usmjeravanja podataka u IP mreži
  - Upravljački sloj
    - Softswitch čvorovi djeluju kao poslužitelji koji upravljaju pozivom/vezom
    - Signalizacija između mrežnih čvorova
  - Sloj povezivanja
    - Media Gateways (MGW) su upravljani od strane softswitcha
    - Odgovorni za ostvarivanje veze kroz IP mrežu i za strujanje medija kroz mrežu
- Usluga: prijenos govora mrežom IP

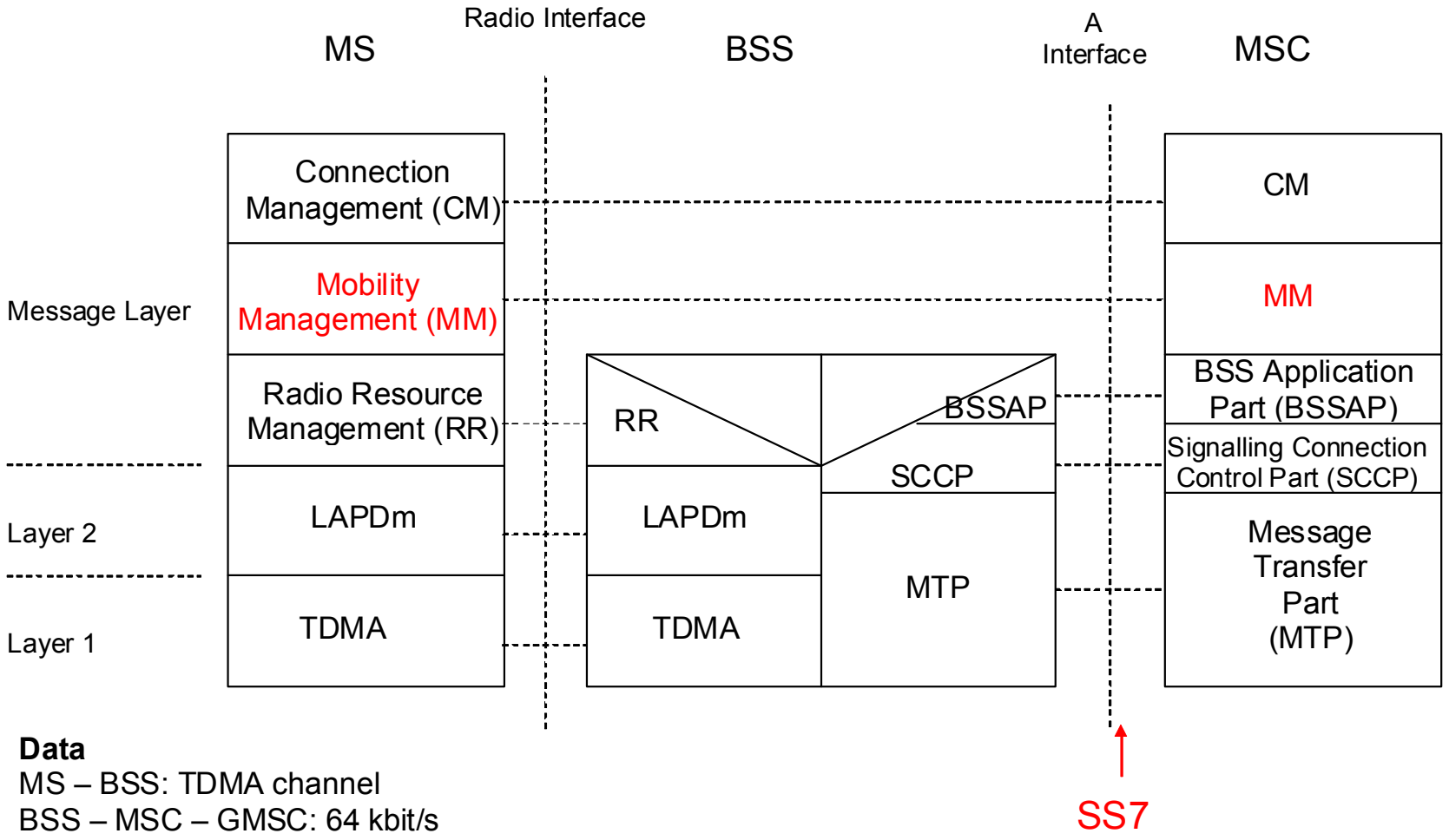
Softswitch arhitektura



Signaling Transport (SIGTRAN)

- Skup protokola koji omogućavaju prijenos signalizacije SS7 preko mreže IP
- IETF, RFC 2719 (arhitektura protokola)
- Sastoji se od tri komponente
  - Protokol za adaptaciju (adaptation protocol)
    - Podržava specifične primitive
    - M2UA, M2PA, M3PA, SUA, IUA
  - Common Signaling Transport Protocol (SCTP)
    - Podržava skup pouzdanih prijenosnih funkcija za prijenos signalizacije
  - Internetski protokol IP

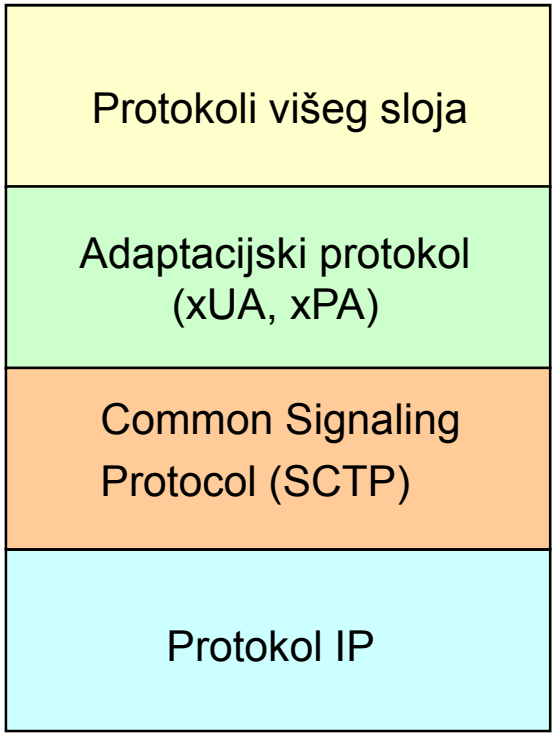
GSM Protokoli

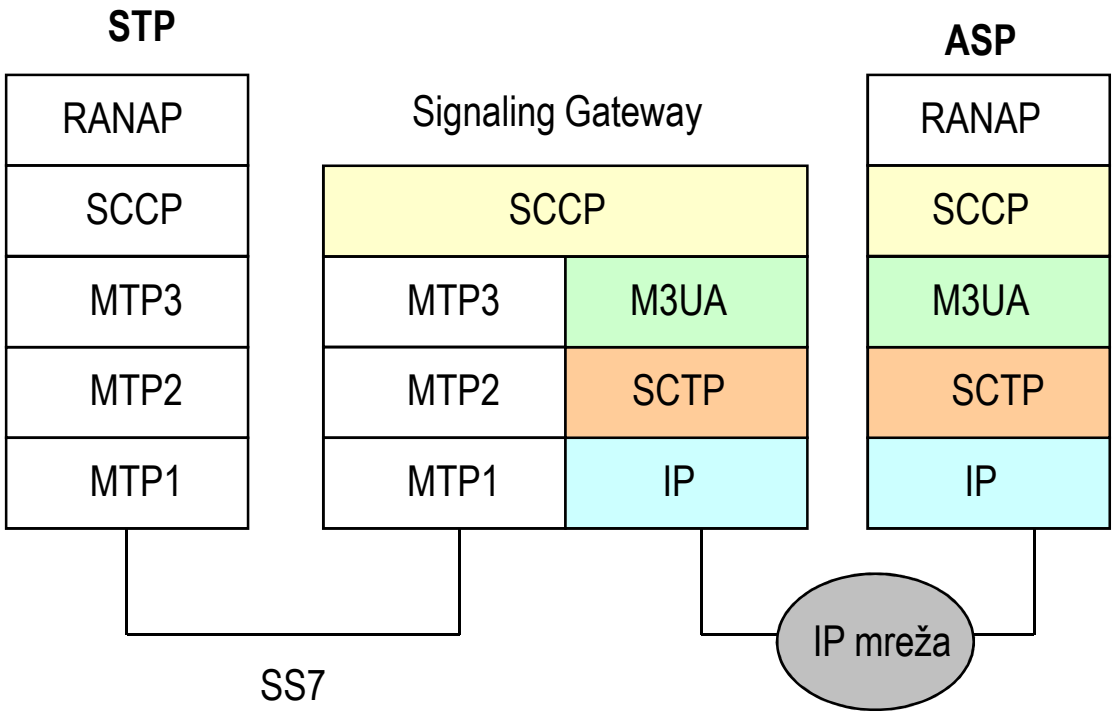


Data
MS – BSS: TDMA channel
BSS – MSC – GMSC: 64 kbit/s

SIGTRAN protokolni složaj

Protokolni složaj





STP – SS7 Signaling Transfer Point (npr. MSC)

ASP – Application Server Process – MGC, IP SCP ili IP HLR

Preddiplomski studij

Javna pokretna mreža

9.

Evolucija ćelijskih sustava

Ak.g. 2007./2008.

12.5.2008

Teme predavanja

Evolucija ćelijskih sustava

2+ generacija
- HSCSD (High Speed Circuit-Switched Data)
- GPRS (General Packet Radio Service)
- EDGE (Enhanced Data rates for GSM Evolution)

Evolucija ćelijskih sustava

1. generacija: analogni sustavi

2. generacija
   - GSM 900 (Global System for Mobile Communication), DCS 1800 (Digital Cellular System)
     - adaptivno kodiranje radi prilagodbe na karakteristike prijenosnog kanala
     - jednostavna dogradnja sustava, visoka spektralna učinkovitost

2+ generacija
   - HSCSD (High Speed Circuit-Switched Data)
   - GPRS (General Packet Radio Service)
   - EDGE (Enhanced Data rates for GSM Evolution)

3. generacija
   - UMTS (Universal Mobile Telecommunication System), IMT 2000:
     - integracija podatkovnih i govornih komunikacija,
     - brzine prijenosa od 140 kbit/s (vani) do 2 Mbit/s (unutra),
     - vrlo dobra podrška mobilnosti

2+ generacija

U GSM sustavu prijenos podataka moguć uz netto brzine prijenosa 9,6 kbit/s
- napredni postupci kodiranja omogućavaju brzine 14,4 kbit/s
- nedovoljno za Internet i multimedijske primjene

Što je problem?
- za mnoge primjene podatci se prenose u kratkim sekvencama - usnopljeni promet (bursty traffic): http, smtp, pop, telnet, ...
- zašto rezervirati fizičke resurse na radijskom sučelju ako će oni biti uglavnom neiskorišteni?
- zašto rezervirati istodobni prijenos uz full duplex kanale ako je promet uglavnom half duplex?

– povećanje kapaciteta rješava HSCSD High Speed Circuit-Switched Data

HSCSD (High-Speed Circuit Switched Data)

- uglavnom potreban samo novi software
- kako bi se postigao veći AIUR - *Air Interface User Rate* koristi se veći broj prometnih kanala, istovremenim korištenjem nekoliko vremenskih odsječaka
- teoretski bi se moglo koristiti svih 8 vremenskih odsječaka jednog TDMA okvira za jednog korisnika (ukupna ostvariva brzina prijenosa 115,2 kbit/s ako imamo neto brzinu 14,4 kbit/s po kanalu)
- u praksi se gornja granica postavlja na 4 kanala
  ukupna brzina prijenosa:
  57,6 kbit/s uz 4 kanala po 14,4 kbit/s
  38,4 kbit/s uz 4 kanala po 9,6 kbit/s

Prednost: jednostavan za primjenu, konstantna kvaliteta

Nedostatak: kanali blokirani za prijenos govora

GPRS (General Packet Radio Service)

- uvodi novu infrastrukturu u jezgrenu mrežu za paketski prijenos
- u radijskom dijelu nema promjena, ali se 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 za privremeno omogućavanje većeg kapaciteta
- MS mora biti prilagođen za GPRS uslugu

Prednost: korak bliže prema UMTS, fleksibilnost

Nedostatak: potrebna veća investicija (novi hardware)

ostvarive brzine [kbit/s] u ovisnosti o broju korištenih vremenskih odsječaka

kodiranje	1	2	3	4	5	6	7	8
CS-1	9,05	18,2	27,15	36,2	45,25	54,3	63,35	72,4
CS-2	13,4	26,8	40,2	53,6	67	80,4	93,8	107,2
CS-3	15,6	31,2	46,8	62,4	78	93,6	109,2	124,8
CS-4	21,4	42,8	64,2	85,6	107	128,4	149,8	171,2

2+ generacija (2,5G)

Četiri različita načina kodiranja razlikuju se u parametrima blokovskog i konvolucijskog kodiranja

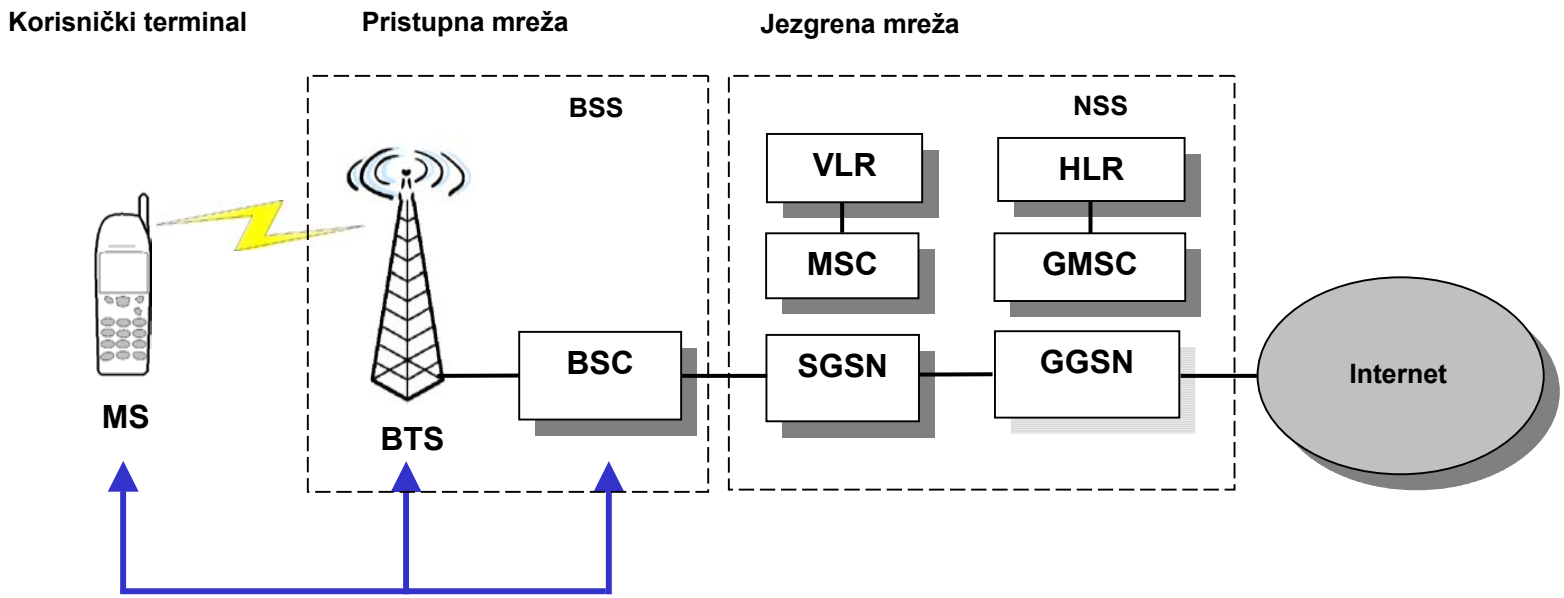
- **Blokovski koder** dodaje fire code (detekcija pogrešaka) od 40 ili 16 bita, kodira USF (Uncoded Uplink State Flag) koristeći 3, 6 ili 12 bita i dodaje 4 tail bita (ako ide na konvolucijski koder).
  - CS1: fire code 40, USF 3
  - CS2: fire code 16, USF 6
  - CS3: fire code 16, USF 6
  - CS4: fire code 16, USF 12, nema tail bitova!

- **Konvolucijski koder** sa 1/2 koristi se za CS1-CS3. Razlika je u tome da u CS2 i CS3 neki se bitovi isprekidaju prije odašiljanja. Isprekidani konvolucijski kod rezultira u omjeru koda od 2/3 ili 3/4.
  - CS1: 1/2
  - CS2: 2/3
  - CS3: 3/4
  - CS4: ----

2+ generacija (2,75G) - **EDGE**

- Enhanced Data Rates for Global/GSM Evolution (EDGE):
  - novi modulacijski postupak (8 PSK)
  - različite klase kodiranja
  - maksimalna brzina prijenosa 43 kbit/s po kanalu
- EDGE faza 1:
  - kanalno kodiranje i modulacijski postupci trebaju omogućiti brzine prijenosa do 384 kbit/s
  - GPRS terminal može dobiti do 8 vremenskih okvira, ali stroži zahtjevi za kvalitetom kanala.
- EDGE faza 2:
  - smjernice za postizanje visokih brzina prijenosa za usluge s komutacijom kanala.
- ostvarive brzine prijenosa skoro iste kao kod UMTS-a
- visoke brzine nisu dostupne svuda u ćeliji

2+ generacija - **EDGE**



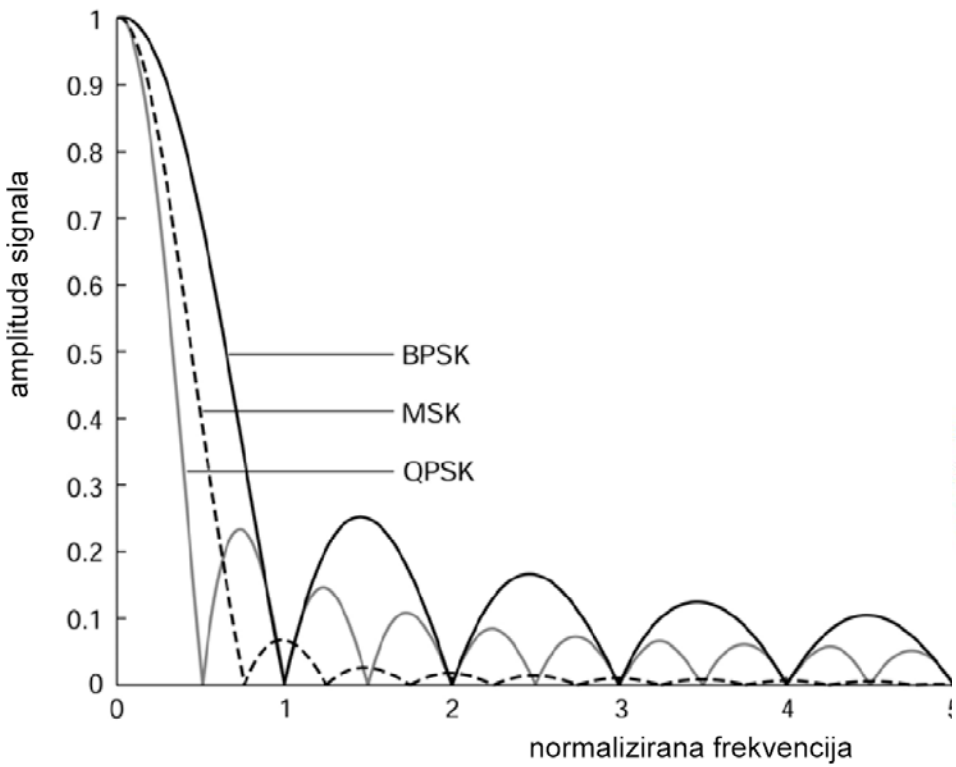
BSS – bazna postaja sadrži opremu za upravljanje radijskim kanalom

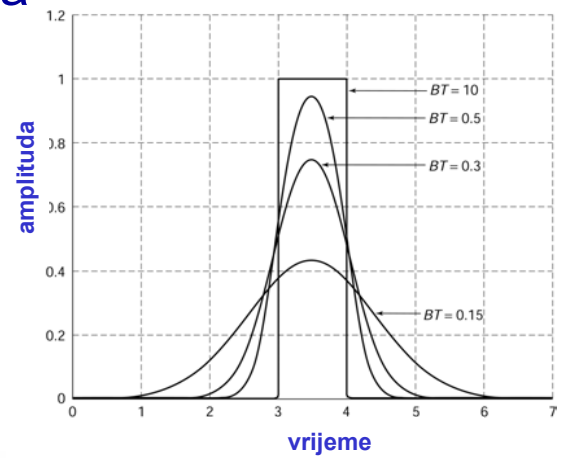
- u jezgrenom dijelu mreže koristi se GPRS infrastruktura

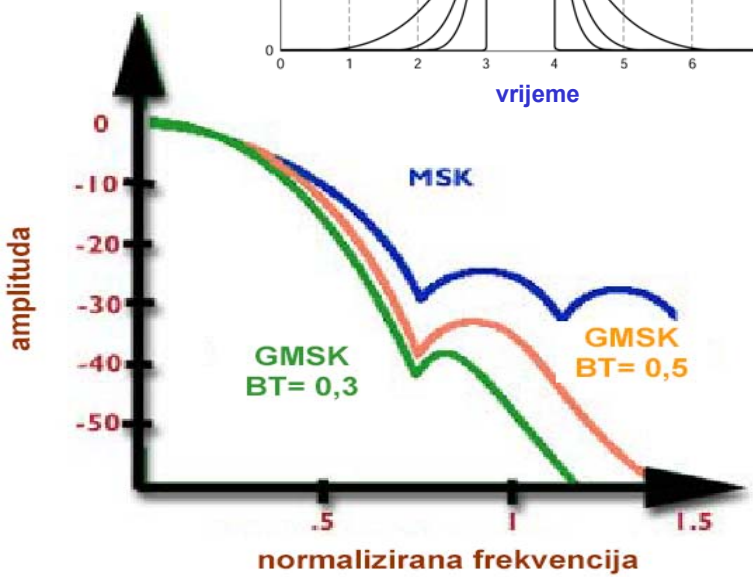
2+ generacija - **EDGE**

- cilj EDGE tehnologije je uz maksimalno zadržavanje postojeće GSM/GPRS infrastrukture postići veće brzine prijenosa efikasnijim iskorištavanjem raspoloživih radijskih frekvencija

GMSK modulacijski postupak:

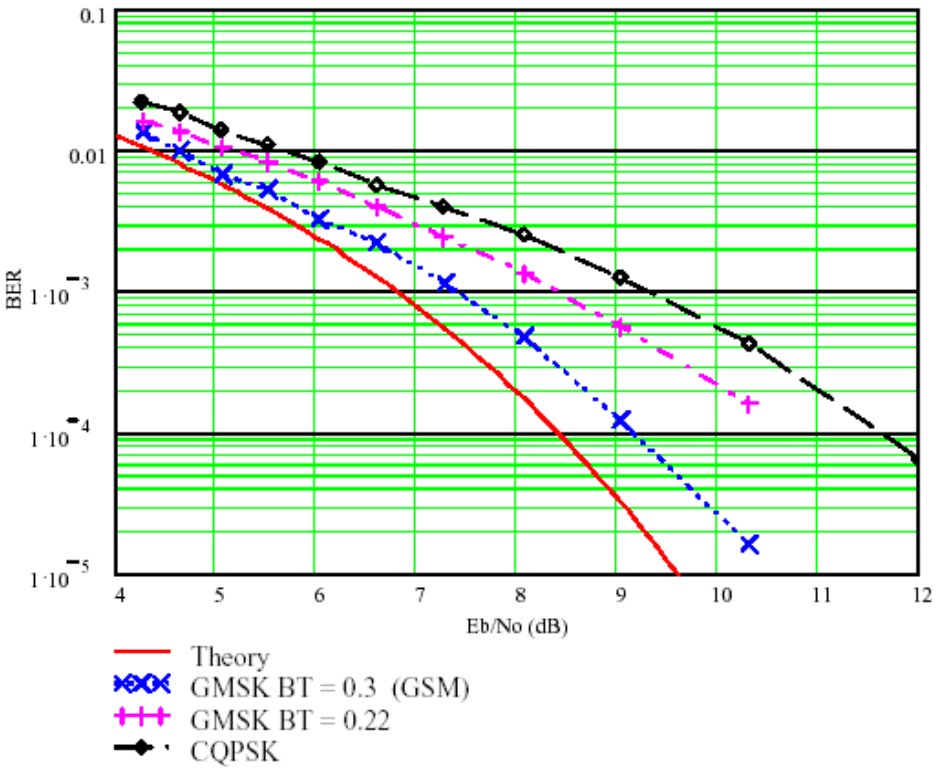


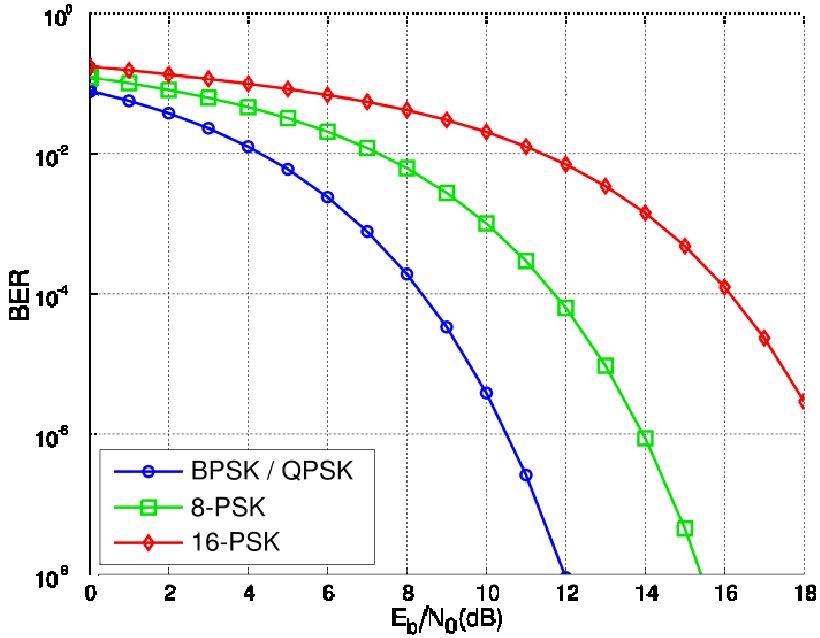




2+ generacija - **EDGE**

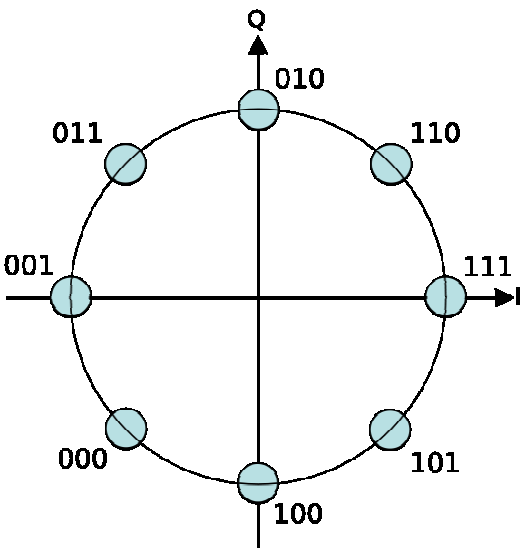
GMSK modulacijski postupak → 8PSK modulacijski postupak

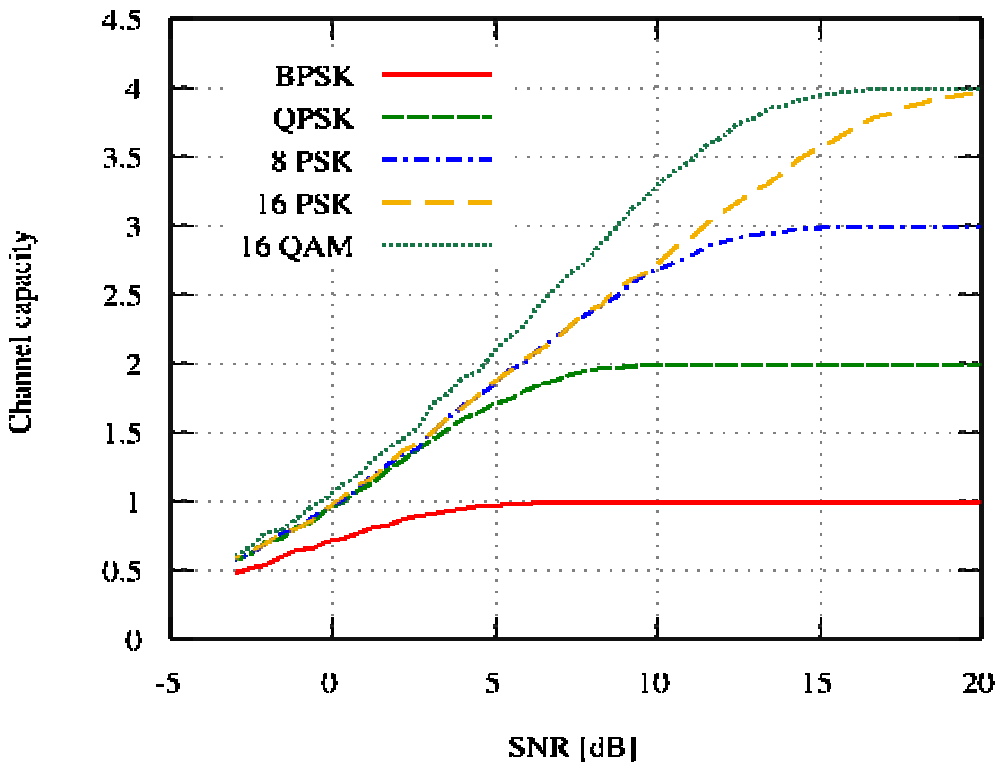




2+ generacija - **EDGE**

- na GSM radijskom sučelju umjesto klasičnog GMSK modulacijskog postupka koristi se **8PSK** s 3 bita/simbolu





2+ generacija - **EDGE**

- cilj EDGE tehnologije je uz maksimalno zadržavanje postojeće GSM/GPRS infrastrukture postići veće brzine prijenosa efikasnijim iskorištavanjem raspoloživih radijskih frekvencija
- na GSM radijskom sučelju Um umjesto klasičnog GMSK modulacijskog postupka koristi se 8PSK s 3 bita/simbolu
- novim modulacijskim postupkom i novim algoritmima kanalnog kodiranja omogućena je realizacija novih prometnih kanala
- ukupno je definirano 9 postupaka koji se razlikuju u modulaciji, kodiranju i načinu zaštite od pogrešaka, čija primjena ovisi o trenutačnim parametrima radijske veze i kvaliteti signala:
  - četiri se baziraju na robusnoj GMSK modulaciji i omogućavaju brzine prijenosa između 8,8 i 17,2 kbit/s po kanalu
  - pet preostalih se baziraju na 8PSK modulaciji i omogućavaju brzine prijenosa između 22,4 und 59,2 kbit/s po kanalu

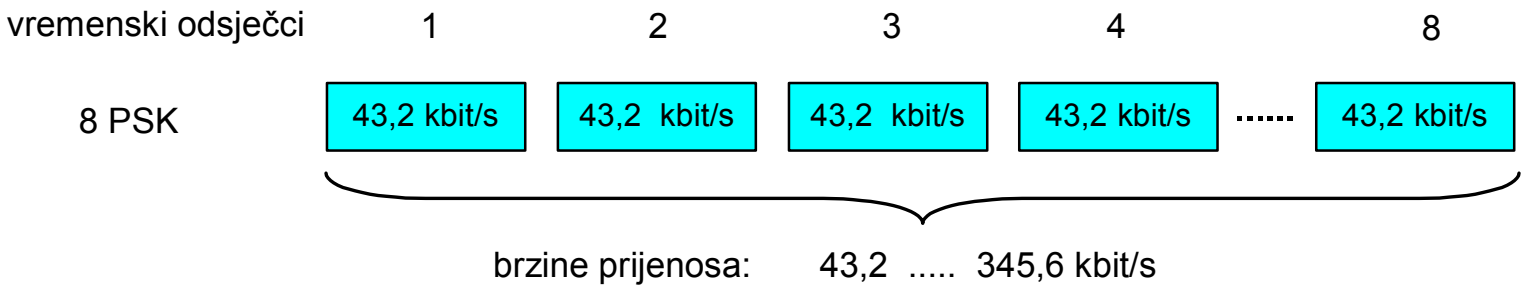
2+ generacija - **EDGE**

- novim modulacijskim postupkom i novim algoritmima kanalnog kodiranja omogućena je realizacija novih prometnih kanala - E-TCH / F (Enhanced Circuit Switched Data)
  - podaci s brzinama prijenosa 28,8 kbit/s (E-TCH / F 28,8)
  - podaci s brzinama prijenosa 32,0 kbit/s (E-TCH / F 32,0)
  - podaci s brzinama prijenosa 43,2 kbit/s (E-TCH / F 43,2)
- problem EDGE tehnologije je da je nužna bolja kvaliteta signala u odnosu na kvalitetu koju nudi prosječna GSM-mreža, kako bi se stvarno postigao učinak. To traži postavljanje većeg broja novih baznih postaja, a time i znatnu dodatnu investiciju.
- tako visoke brzine prijenosa moguće su samo u povoljnim uvjetima u neposrednoj blizini bazne postaje i za korisnike koji se ne kreću
- uz normalne (promjenjive) uvjete prijama optimalno iskorištavanje radijskih resursa podrazumijeva odabir najpovoljnijih postupaka za postizanje što veće trenutne brzine prijenosa

2+ generacija - **EDGE**

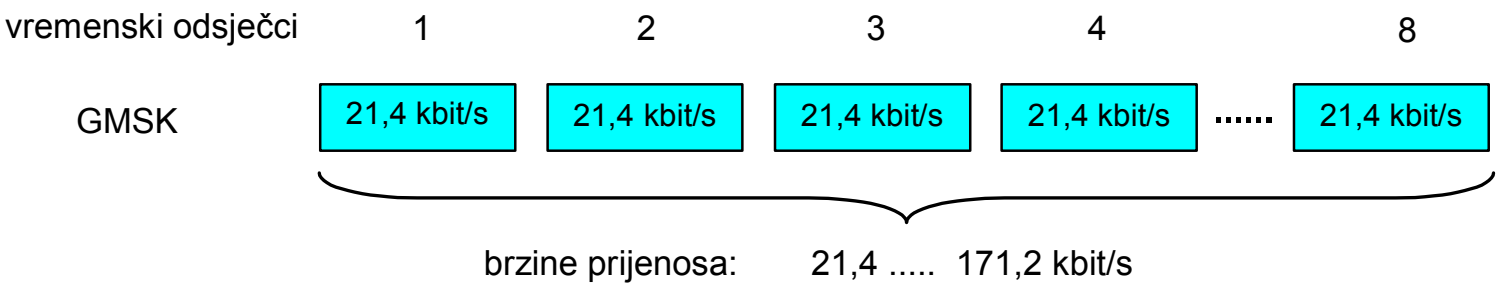
EDGE (Enhanced Data rates for GSM Evolution):

- omogućava brzine prijenosa 28,8 - 43,2 kbit/s po vremenskom odsječku uz korištenje novog modulacijskog postupka: 8PSK umjesto GMSK



GPRS (General Packet Radio Service)

- po vremenskom odsječku ostvarive su brzine prijenosa 9,05 - 21,4 kbit/s, ovisno o korištenom kanalnom kodiranju



2+ generacija - **EDGE**

- povećanje prijenosnog kapaciteta u GSM frekvencijskom pojasu uz zadržavanje FDMA/TDMA postupaka višestrukog pristupa (primjenom modulacijskog postupka 8PSK)
- nepotrebno je ishođenje novih licenci, kao i novo planiranje ćelija i frekvencija
- iskorištavanje postojećih frekvencijskih pojasa
- zadržavanje postojeće mrežne infrastrukture, nadogradnja u koracima
- nužno je opremanje baznih postaja s novom opremom prilagođenom za 8PSK
- kombinirani rad postojećih i EDGE prijamnika u mreži
- signal je vrlo osjetljiv na interferencije

2+ generacija - **EDGE**

- za očekivati je se da će GSM operatori postupno uvoditi EDGE
- međutim, mnogi operatori u Europi uvode 3G mreže i moglo bi se čekati na EDGE nadogradnju.
- EDGE će povećati brzine prijenosa, ali neće promijeniti broj govornih veza koji se mogu ostvariti unutar ćelije
- 3G mreže su nužne za ostvarivanje povećanja kapaciteta govornih komunikacija u sustavu.

2+ generacija - **EDGE**

Prednosti:

- povećane brzine prijenosa
- nije potrebna modifikacija u jezgrenom dijelu mreže

Nedostaci:

- novi modulacijski postupak (8PSK) nekompatibilan sa GMSK
- nužna modifikacija opreme u baznoj postaji i korisničkog mobilnog uređaja