ARHITEKTURA, PROTOKOLI I SERVISI INTERNETA

Dr Zvezdan Stojanović
ARHITEKTURA, PROTOKOLI I SERVISI INTERNETA

UREDNIK:
Dr Nedeljko Stanković

RECENZENTI:
Dr Halid Žigić
Dr Mile Petrović
Dr Velimir Dedić

IZDAVAČ:
EVROPSKI UNIVERZITET BRČKO DISTRIKTA
Tel. 049 590-605
http://www.evropskiuniverzitet-brcko.com/

Odlukom Senata Evropskog univerziteta u Brčkom, broj: 21-6/2015, od 7.2.2015. godine, knjiga «Arhitektura, protokoli i servisi interneta» autora dr Zvezdana Stojanovića, prihvaćena ja kao udžbenička literatura.

ŠTAMPA:
Markos, Banja Luka

TIRAŽ:
200.

ISBN 978-99976-605-9-6

Dr Zvezdan Stojanović

ARHITEKTURA, PROTOKOLI I SERVISI INTERNETA

EVROPSKI UNIVERZITET
BRČKO, 2015.

P R E D G O V O R

Internet predstavlja informacionu tehnologiju koja je najradikalnije promijenila svijet i najviše doprinijela internacionalizaciji i globalizaciji. Tokom pedesetak godina svog postojanja Internet je evoluirao, mijenjao uloge, ali bismo s pravom mogli reći da Internet danas predstavlja najveću informaciono-telekomunikaciono-poslovnu platformu. U knjizi će se prvenstveno razmatrati prva dva aspekta

Knjiga je namijenjena studentima Tehničkog fakulteta Evropskog univerziteta u Brčkom, ali može poslužiti i kao koristan udžbenik i za ostale fakultete na kojima se kao predmeti razmatraju „Internet“ i „Uvod u veb“.

Knjiga je podijeljena u devet poglavlja.

U prvom poglavlju je predstavljen istorijat Interneta sa posebnim akcentom na godine nastajanja pojedinih Internet servisa koji će se razmatrati u knjizi.

U Drugom poglavlju su dati osnovni elementi Infrastrukture Interneta, tehnologije u pristupnoj i magistralnoj mreži, ukazano je na problem nedostatka propusnog opsega u pristupnoj mreži i načini za njegovo otklanjanje.

Treće poglavlje predstavlja praktično kratak kurs digitalnih telekomunikacija, koji je neophodan radi cjelovitosti shvatanja načina funkcionisanja Interneta.

U prvom poglavlju smo definisali Internet kao globalnu računarsku mrežu sastavljenu od više miliona drugih mreža. U Četvrtom poglavlju će biti govora o tome šta je računarska mreža, bit će izvršena podjela računarskih mreža i opisan je malo šire Ethernet kao najzastupljenija računarska mreža kako u LAN tako i WAN kruženju.

U Petom poglavlju su opisani referentni modeli, OSI i TCP/IP sa posebnim akcentom na TCP/IP protokol stek jer na njemu se bazira rad Interneta. Opisani su najznačajniji protokoli na svim nivoima protokol steka.

Kao posebno poglavlje izdvojeno je adresiranja na Internetu. U Poglavlju 6 su opisane adrese na pojedinim slojevima TCP/IP protokol steka.

U Poglavlju 1 je dat kratak istorijski pregled razvoja Interneta sa posebnim osvrtom na najznačajnije Internet servise. U Poglavlju 7 će biti neki od njih detaljno objašnjeni, ali pored nekoliko osnovnih kakvi su WWW, elektronska pošta, bit će opisani i najnoviji setvisi kao što su VoIP, IPTV, VoD.

Pošto se segment mobilnih komunikacija, svakim danom sve popularniji, to će u Poglavlju 8 biti dat pregled nekih, u našem okruženju najzastupljenijih mobilnih tehnologija za pristup Internetu.

Kako je Internet danas postao platforma preko koje se odvijaju brojne transakcije i putem koga se svakodnevno razmjenjuju ogromne količine podataka, to se pitanje bezbjednosti Interneta nameće kao prioritet, te je zadatak Poglavlja 9 da da pregled sigurnosnih tehnika i najčešće korištenih protokola na pojedinim nivoima TCP/IP protokol steka.

Veliku zahvalnost dugujem recenzentima, profesorima dr Miletu Petroviću, dr Velimiru Dediću i dr Halidu Žigiću, koji su korisnim sugestijama doprinijeli poboljšanju kvaliteta knjige.

Posebnu zahvalnost dugujem predsjedniku upravnog odbora Evropskog univerziteta, profesoru Nedeljku Stankoviću bez čije podrške se ovaj projekat ne bi mogao realizovati..

S A D R Ž A J

Knjigu posvećujem sinu Aleksandru

POGLAVLJE 1

Istorijski razvoj Interneta

Internet predstavlja informacionu tehnologiju koja je najradikalnije promijenila svijet i najviše doprinijela internacionalizaciji i globalizaciji. Postoji više faktora koji su uticali na afirmaciju ove informacione tehnologije. Jedan od najvažnijih jeste taj što je Internet prvobitno razvijan kao vojni projekat, pa je ogromna količina kapitala uložena u njegov razvoj. Internet je danas postao nosioc digitalne revolucije. Broj korisnika Interneta je u stalnom porastu i prema podacima iz 2013-te godine, oko 38,8 % ukupne svjetske populacije koristi Internet, što je ogroman postotak, ako se uzme u obzir da je to postignuto u vremenskom intervalu kraćem od 50 godina. U ovom poglavlju će biti navedeni neki datumi i događaji koji su doprinijeli razvoju i popularizaciji Interneta i koji su odigrali presudnu ulogu u njegovom daljem razvoju.

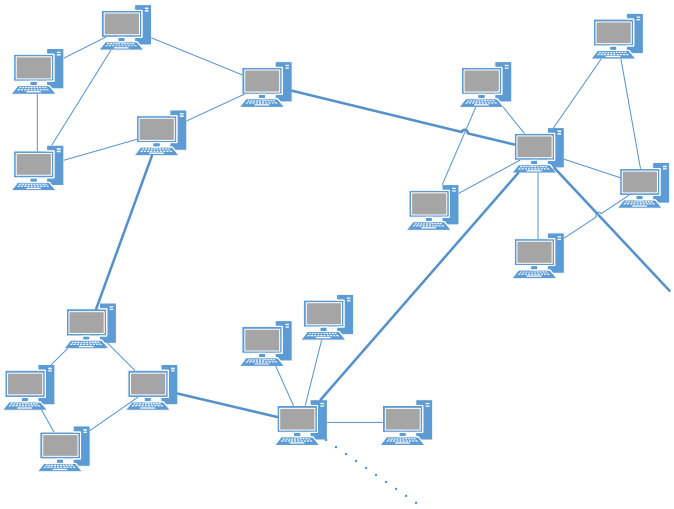
1.1. Istorijski razvoj interneta

Tokom pedesetak godina svog postojanja, Internet je evoluirao od mreže namijenjene za vojnu upotrebu do globalne mreže sa nekoliko milijardi korisnika.

Šta je u stvari Internet? U literaturi se mogu naći razne definicije. Ovdje su izdvojene samo neke, [90].

Def.: *Internet je globalna mreža sačinjena od hiljada drugih računarskih mreža pri čemu one koriste TCP/IP (Transmission Control Protocol/Internet Protocol) skup protokola (protokol stek) za međusobnu komunikaciju, pri čemu protokol predstavlja skup pravila koja definišu neke komunikacione funkcije.*

Def.: *Internet je globavna svjetska mreža napravljena od sličnih, povezanih mreža koje povezuju milione računara širom svijeta, uz primjenu odgovarajuće telekomunikacione infrastrukture.*



Slika 1.1: *Internet kao globalna svjetska mreža koja povezuje sve ostale*

Alternativno:

Def.: *Internet je globalni informacioni sistem koji je logički povezan preko globalnog jedinstvenog adresnog prostora zasnovanog na Internet protokolu i koji je sposoban da podrži komunikaciju korišćenjem TCP/IP-a.*

Def.: *Internet predstavlja informacionu tehnologiju (IT) koja je najradikalnije promijenila svijet i najviše doprinijela internacionalizaciji i globalizaciji.*

Nijedna druga informaciono-komunikaciona tehnologija nije dovela do tako značajnih promjena. Internet je transformisao stare industrije, finansijske usluge, maloprodaju i veleprodaju i klasične posrednike pri upotrebi nekih servisa ali je stvario nove: portale, pružaoce Internet usluga (ISP-Internet Service Provider) i usluga razvoja aplikacija, čime niču nova tržišta.

U literaturi se naširoko raspravlja i diskutuje o najvažnijim datumima pri razvoju Interneta, [47],[90]. U suštini mogli bismo izdvojiti tri faze u razvoju Interneta, kao što je prikazano na slici 1.2:

- fazu inovacije (1961-1974);
- fazu instutucionalizacije (1975-1994);
- fazu komercijalizacije (1995-do danas).

Slika 1.2: *Faze u razvoju Interneta*

Dat ćemo pregled najznačajnijih događaja u razvoju Interneta tebelarno (Tabela 1.1) sa posebnim akcentom na vremena nastajanja najpopularnijih servisa Interneta koji se razmatraju u ovoj knjizi.

Tabela 1.1: *Najznačajniji događaji u razvoju Interneta*

GODINA	DOGAĐAJ	ZNAČAJ DOGAĐAJA
FAZA INOVACIJE (1961-1974)		
1961	Leonard Kleinrock (sa MIT-a) je objavio rad o mrežama sa komutacijom paketa.	Rođen je koncept komutacije paketa.
1961	Lawrence Roberts (sa MIT-a) je povezao računare na Cambridge-u sa računarom u Kaliforniji upotrebom obične telefonske linije.	Ovo je prva demonstracija WAN-a upotrebom obične telefonske linije, povezivanje sa udaljenim računarom i pokretanje programa na udaljenom računaru (odmah se vidjelo da telefonski sistem ima previše šuma i da je previše spor za ovu namjenu).
1962	J.C.R. Licklider (sa MIT-a) je napisao zabilješke u kojima prvi put upotrebljava pojam "galaktička mreža" računara.	Rođen je koncept globalne računarske mreže.
1963	Licklider vodi razvoj ARPA (Advanced Research Project Agency) kao odjeljenja zaduženog za istraživanje i razvoj unutar Ministarstva odbrane SAD-a.	Ovo je početak vojnog interesovanja. ARPA je postala najveći finansijer prve faze u razvoju Interneta.
1966	Lawrence Roberts uvjerava ARPA-u da finansira razvoj ARPANET-a upotrebom komutacije paketa.	Prvi pokušaj izgradnje globalne mreže sa komutacijom paketa.
1968	ARPA je uputila zahtjev različitim kompanijama da naprave svičeve koji će podržati komutaciju paketa.	Koncept paketske komutacije se približio fizičkoj realizaciji.
1969	Instalirani su prvi paketski svičevi na univerzitetima UCLA i Stanford (Bolt Beranek and Newman-BBN).	Koncept paketske komutacije je realizovan hardverski.
1969	Prva poruka primjenom komutacije paketa je poslata sa UCLA univerziteta na Stanford.	Za ovu godinu se vezuje nastanak Interneta. Postavilo se pitanje namjene i upotrebe nove komunikacione tehnologije.
1972	NA ICCC konferenciji je izvršena je demonstracija prve ARPANET aplikacije, e-mail-a (Ray Tomlison)	Rođen je koncept **elektronske pošte**, kao jednog od najznačajnijih Internet servisa.
1973	Izumljena je Ethernet mreža (Bob Metcalfe)	Ustanovljen je klijent-server model. Putem etherneta i primjenom klijent server modela mogle su se povezati hiljade desktop računara na maloj međusobnoj udaljenosti (<1000m) u svrhu dijeljenja datoteka, aplikacija i slanja poruka.
1974	Vint Cer i Bob Kahn su predstavili koncept TCP/IP protokol steka.	Rođen je koncept **TCP/IP**-a. Napravljen je sa osnovnom namjenom povezivanja hiljada LAN-ova i udaljenih računara primjenom zajedničke adresne šeme.

FAZA INSTITUCIONALIZACIJE (1975-1994)		
1980	Američko ministrstvo odbrane je prihvatilo TCP/IP kao standardni komunikacioni protokol.	Jedna od najvećih računarskih organizacija na svijetu je usvojila TCP/IP i koncept paketske komutacije.
1980	Počinje upotreba personalnih računara.	Prve personalne računare su napravile firme Altair, Apple i IBM. Njihova primjena je omogućila milionima ljudi širom svijeta da pristupe Internetu i i vebu.
1983	ARPA je kreirala odvojenu vojnu mrežu (MILNET) i ARPANET je od tada ostao samo za civilnu upotrebu.	Rođena je ideja "civilnog" Interneta.
1983	Razvijeni su servisi Telenet i FTP (File Transfer Protocol).	Ovi servisi su uz već postojeću elektronsku poštu postali prvi Internet servisi. **Telnet** je omogućavao udaljenom računaru da se konektuje na lokalni i izvršava programe, dok **FTP** omogućava prenos datoteka.
1984	Apple je realizovao HyperCard program kao dio svog Macintosh operativnog sistema.	Uvodi se koncept hiperlink dokumenta koji je omogućio korisnicima da „skaču“ sa jedne stranice dokumenta na drugu (i sa jedne lokacije na drugu).
1986	NSF (National Science Foundation) je usvojio Internet kao svoju međuuniverzitetsku mrežu.	NSF je uložio 200 miliona dolara za razvoj univerzitetske mreže.
1989	Tim Berners Lee je predložio formiranje svjetske mreže hiperlink dokumenata zasnovane na HTML-u (HyperText Markup Language)	Rođen je koncept novog Internet servisa, **WWW** (World Wide Web). Veb se sastoji od stranica napisanih u HTML-u sa hiperlinkovima koji omogućavaju lak prelazak sa jedne na drugu stranicu.
1990	NSF na sebe preuzima odgovornost za kreiranje civilne Internet magistrale i kreiranje NSFNET-a. ARPANET se prestaje koristiti.	Napravljen je koncept "civilnog" Interneta koji je dostupan svima.
1993	Na Illinois univerzitetu napravljen prvi grafički veb čitač, Mosaic.	Mosaic je omogućio običnim korisnicima da veoma lako pristupe HTML dokumentu na vebu.
1994	Andreeson i Jim Klark su formirali Netscape.	Pravi se prvi komercijalni veb čitač.
1994	Prva reklamna poruka, baner, je postavljena na Hotvired.com sajtu.	Počinje era e-trgovine.
FAZA KOMERCIJALIZACIJE (od 1995 do danas)		
1995	NSF privatizuje magistralu i komercijalni provajderi preuzimaju nadzor nad magistralom.	Rođen je potpuno komercijalizovani, civilni Internet. Nadzor nad magistralom preuzimaju ATT, Sprint, GTE, UUNet i MCI.
1996	Formiran je Internet2 konzorcijum	34 vladine agencije, univerziteti i poslovne kompanije su planirale uvođenje Interneta 100-1000 puta bržeg od dotadašnjeg.
1998	Vlada SAD-a je stimulisala finansiranje ICANN-a (Internet Corporation for Assigning Numbers and Names)	Nadzor nad imenima domena i adresama je prepušten privatnim neprofitnim međunarodnim organizacijama.
2003	Internet2 dostiže protok od 8 Gbit/s pri testu na međunarodnoj trasi.	To je bila prekretnica pri razvoju ultra-brzih međunarodnih mreža nekoliko puta bržih od postojećih magistrala.

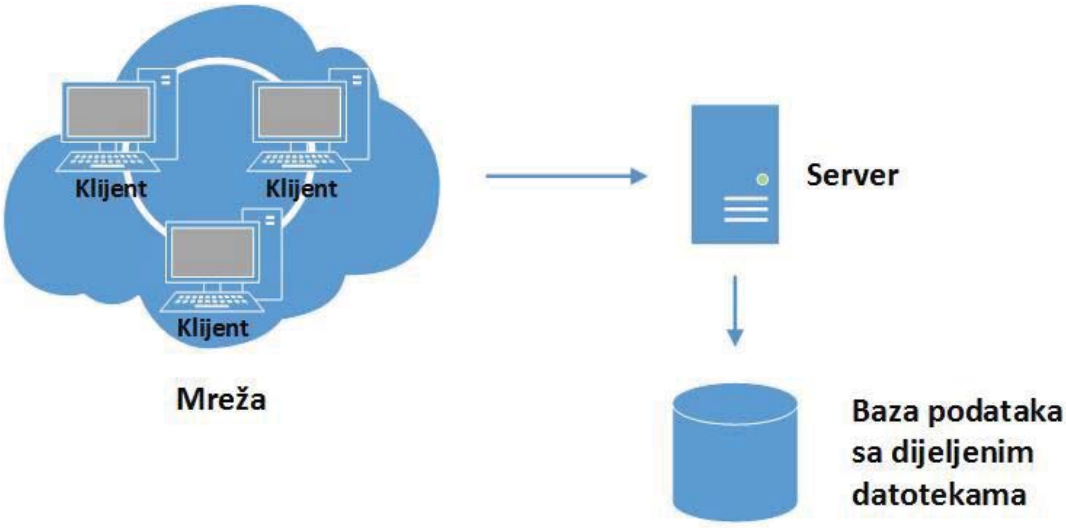
POGLAVLJE 2

Arhitektura Interneta

U ovom poglavlju će biti opisani osnovni elementi koji čine infrastrukturu Interneta, kao što su magistrala na kojoj radi neka od tehnologija koja omogućava velike brzine prenosa (SDH, WDM, DWDM), pristupne mreže putem kojih krajnji korisnici mogu pristupiti Internetu, ...

2.1. Klijent-server model Interneta

Internet je fizička mreža koja povezuje računare širom svijeta. Sastoji se od infrastrukture mrežnih servera i komunikacionih kanala između njih koji se koriste za prenos informacija između PC-a klijenata i veb servera (Slika 2.1).

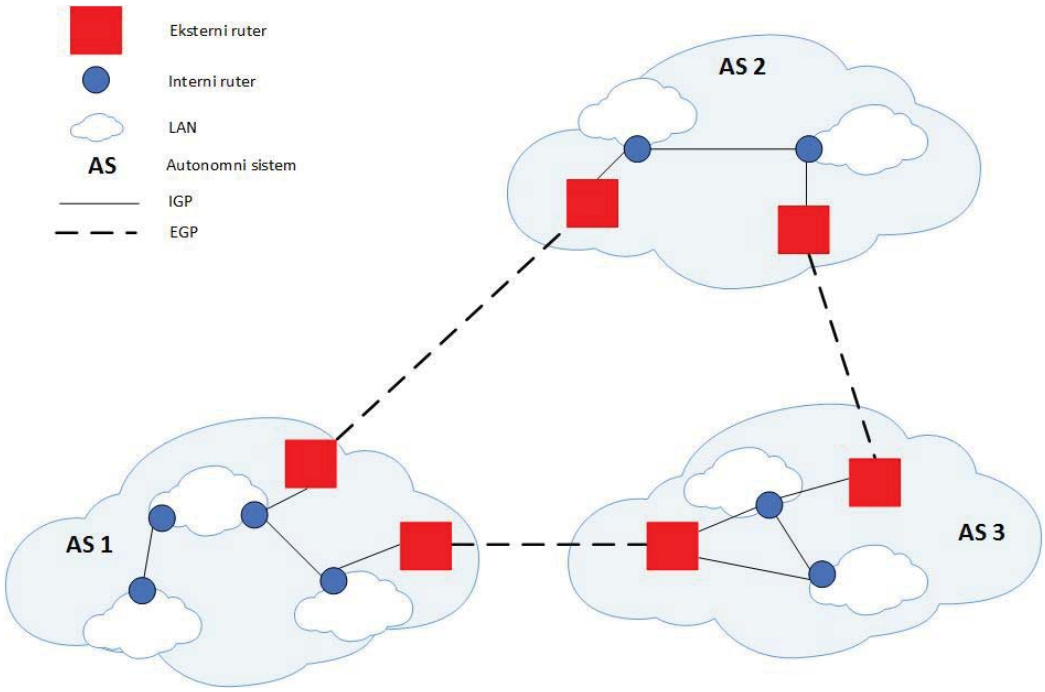


Slika 2.1: *Klijent-server model Interneta*

Klijent-server model predstavlja model u kojem su personalni računari (klijenti) povezani u mrežu sa jednim ili više servera.

Def.: *Klijent se definiše kao aplikacija koja traži uslugu, dok je server mrežni računar namijenjen obavljanju zajedničkih funkcija neophodnih za rad klijenta na mreži, kao što je memorisanje datoteka, softverske aplikacije, uslužni program kao što su veb konekcija i štampači.*

Internet je podijeljen na mnogo zasebnih cjelina koje nazivamo autonomnim sistemima (AS - Autonomous Systems) ili administrativnim domenima, kako je to prikazano na Sl. 2.2, [11].



Slika 2.2: *Podjela Interneta na autonomne sisteme*

Def.: *AS predstavlja skup IP mreža i rutera kojima se upravlja iz jednog administrativnog centra i između kojih se saobraćaj usmjerava pomoću zajedničkog protokola.*

Postoje dvije osnovne kategorije administrativnih domena na Internetu:

- pristupni domen: domen na koji se povezuju krajnji korisnici i koji je povezan najmanje sa jednim tranzitnim domenom da bi se obezbijedio pristup Internetu; pristupni domen može biti provajder Internet servisa (bez obzira da li je on lokalni, nacionalni ili međunarodni) i privatna mreža neke korporacije,
- tranzitni domen prenosi saobraćaj između drugih domena.

Povezivanje pristupnih domena (ISP-ova) se obavlja radi veće fleksibilnosti servisa, kao i iz ekonomskih razloga, a kako su pristupni domeni ravnopravni (peer) kažemo da se uspostavljaju *peering* relacije, tj. uspostavljaju kontakti između ravnopravnih učesnika.

Pristupni domen se može povezati sa više tranzitnih domena. Ta strategija se naziva *multihoming* i vrši se radi obezbjeđivanja redudancije, tj pravljenja rezervne veze za pristup Internetu u slučaju otkaza primarne veze, kao i radi ravnomjernije raspodjele

saobraćaja i poboljšanja performansi. Decentralizovana organizacija doprinosi većoj otpornosti Interneta na otkaze, budući da otkaz bilo kojeg dijela mreže ne utiče na ostatak mreže, [11]. [90].

Infrastrukturu Interneta čine:

- okosnica, kičma (backbones);
- ruteri;
- tačke pristupa (POP-Point of Presence);
- serveri;
- računari korisnika.

2.1.1. Okosnica (backbone)

Okosnica, magistrala (backbones) predstavlja komunikacioni link velikih brzina (optička vlakna) koji omogućavaju Internet komunikaciju unutar jedne države ili van nje.

Koriste se monomodna optička vlakna, optimizovana za rad u drugom i trećem optičkom prozoru (na talasnim dužinama 1310nm i 1550nm respektivno).

Najrasprostranjenija tehnologija prenosa u okosnici je SDH/SONET (Synchronous Digital Hierarchy/Synchronous Optical network). SDH je evropski, SONET američki standard.

Osnovna jedinica prenosa u SDH mreži je sinhroni transportni modul, STM-1, koji obezbjeđuje protok od 155,52 Mbit/s. Veći protoci se dobijaju multipleksiranjem STM-1 strukture, STM-N, gdje je N=4, 16, 64, 256.

SDH tehnologija je dobro prilagođena prenosu signala iz klasične telefonske mreže, kao i prenosu signala iz paketskih mreža kao što je ATM (Asynchronous Transfer Mode).

Dva glavna nedostatka SDH tehnologije:

- zahtijeva veoma skupu sinhronizaciju svih uređaja u transportnoj mreži,
- stalni porast IP saobraćaja ima potencijal prevazilaženja kapaciteta SDH sistema.

U poslednjij deceniji primat je preuzela WDM (Wavelength Division Multiplexing) tehnologija koja omogućava multipleksiranje signala koje se prenose po jednom optičkom vlaknu, korištenjem različitih talasnih dužina, [59].

WDM sistemi mogu da prenose različito kodovane signale, ali se uobičajeno koriste za prenos TDM ili Ethernet okvira.

U mrežama regionalnih operatera se susreću najčešće CWDM (Coarse Wavelength Multiplexing) i DWDM (Danse Wavelength Division Multiplexing) tehnike multipleksiranja po talasnim dužinama.

CWDM predstavlja tehniku konvencionalnog multipleksiranja po talasnim dužinama koja koristi skup od 18 talasnih dužina raspoređenih u opsegu od 1270nm do 1610nm na međusobnim rastojanjima 20nm i protoka po kanalu je 2,5 Gbit/s.

Kod DWDM-a tehnike gustog multipleksiranja, definisano je nekoliko skupova talasnih dužina:

- C opseg (1528-1561nm),
- L opseg (1561-1620 nm).

sa rastojanjem između talasnih dužina 1nm.

Imaju znatno veći broj kanala sa protokom po kanalu od 10 Gbit/s ili 40 Gbit/s. Ovdje treba napomenuti da se cijelo optičko vlakno može posmatrati kao jedan komunikacioni kanal, bez obzira na tehnologiju prenosa po tom optičkom vlaknu.

Postojeći SDH sistemi prenosa se zadržavaju radi obezbjeđivanja transportnih servisa za klasične telekomunikacione servise (telefonija, prenos podataka koji nisu prilagođeni IP protokolu), dok se za prenos IP saobraćaja potreban dodatni kapacitet koji pruža DWDM sistem.

2.1.2. Ruteri

Ruteri predstavljaju specijalizovane računare u kojima se odvijaju sledeći procesi:

- rutiranje (routing): popunjavanje i održavanje tabele rutiranja, odnosno nalaženje putanje (rute) od izvora ka odredištu i to je najvažnija funkcija IP protokola; rutiranje se odvija na osnovu tabela; popunjavanje tabele rutiranja se naziva politika rutiranja,
- prosleđivanje (forwarding): procesiranje svakog dolaznog paketa i traženje odlaznog linka po kome će ga proslijediti sledećem elementu mreže (pretražuje tabelu rutiranja, mada može postojati i tabela prosleđivanja);

Tabela rutiranja se sastoji od:

- odredišne IP adrese koja može biti odredišna adresa računara ili mreže,
- mrežne maske,
- adresa mrežnog prolaza (gateway-a), tj rutera sledećeg skoka; naime, ukoliko se adresa odredišta nalazi na istoj mreži računari komuniciraju direktno

međusobno, dok, ako se adresa odredišta nalazi na drugoj mreži, paketi podatka koji su namijenjeni njima se šalju preko predodređenog mrežnog prolaza,

- IP adresa mrežnog interfejsa, odnosno same kartice (na osnovu adrese mrežnog interfejsa, znamo na kojoj mreži se nalazi odredište),
- metrika pokazuje potreban broj skokova (hopova) do odredišta.

Ruteri unutar jednog autonomnog sistema (AS) komuniciraju preko IGP (Interior Gateway Protocol) protokola, dok ruteri koji povezuju AS komuniciraju preko EGP (Exterior Gateway Protocols) protokola, [11], [16], [42], [52], [76].

Algoritmi rutiranja predstavljaju dio softvera mrežnog sloja koji je odgovoran za upućivanje dolaznih paketa na izlazni interfejs (port).

Kao protokoli za rutiranje unutar domena koriste se:

- protokoli zasnovani na razmjeni stanja linkova, LS (Link State) protokoli, koji predstavljaju centralizovane algoritme rutiranja koji podrazumijevaju da svaki ruter održava informacije o kompletnoj topologiji mreže;
  - predstavnici:
    - OSPF (Open Shortest Path First);
    - IS-IS (Intermediate System-Intermediate System).
- protokoli zasnovani na razmjeni vektora rastojanja DV (Distance Vector) protokoli: čvor ne zna topologiju čitave mreže, već informaciju o svojim susjedima.
- treba napomenuti da se DV protokoli mogu koristiti i za:
  - rutiranje u domenu:
    - predstavnik: RIP (Routing Information Protocol).
  - za rutiranje između domena:
    - predstavnik: BGP (Border Gateway Protocol).

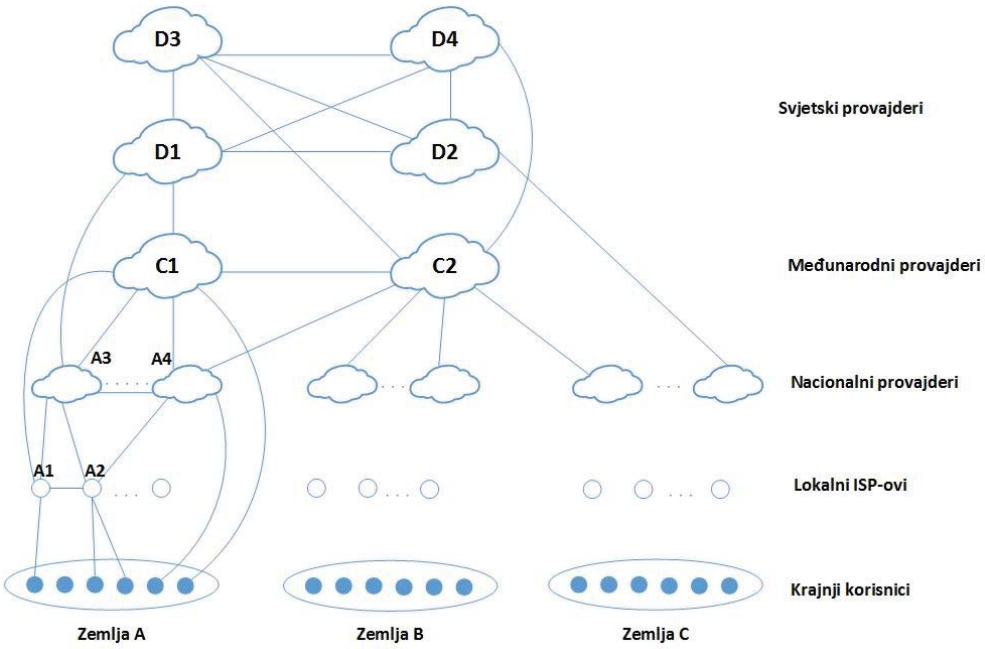
2.1.3. Tačke pristupa (PoP)

Pretplatnik koji pokušava da pristupi Internetu to može uraditi samo preko nekog od ISP-ova. Tehnički gledajući, pristup Internetu se može desiti samo u tački pristupa (Point of Presence-PoP), odnosno fizičkoj lokaciji gdje su smješteni modemi ili ruteri koji prihvataju IP saobraćaj koji generiše krajnji korisnik i prosleđuju ga na Internet ili saobraćaj sa Interneta prosleđuju krajnjem korisniku, [90].

Načini povezivanja na Internet su različiti:

- velike kompanije se obično povezuju sa tačkama pristupa Internetu (PoP-ovima) nekog ISP-a preko iznajmljenih linkova velikog kapacieta, najčešće putem SDH infrastrukture ili primjenom pasivnih optičkih mreža (PON-Passive Optical Network),
- male kompanije i krajnji korisnici se povezuju sa ISP-om putem neke xDSL tehnologije (Digital Subscriber Line), pri čemu x u oznaci označava da se može raditi o čitavoj familiji različitih tehnologija, (ADSL, ADSL2, ADSL2+, VDSL, VDSL2 i sl).

Generisani saobraćaj će se preko lokalnog ISP-a izrutirati do nacionalnog ISP-a, preko njega, moguće je do nekog internacionalnog i tako sve do odredišta, kako je to predstavljeno na Sl. 2.3.



Slika 2.3: *Klase ISP-ova*

Lokalni ISP-ovi u jednoj zemlji su predstavljeni oznakama A1, A2, ...Oni mogu imati vezu i između sebe, ali moraju imati vezu sa nacionalnim (A3) ili internacionalnim ISP-om (C1).

Internacionalni ISP-ovi (A3 i A4), mogu imati vezu i između sebe, ali moraju imati veze sa međunarodnim ISP-ovima, (recimo A3 sa C1 i A4 sa C2), ali mogu imati vezu i sa nekim svjetskim (više-regionalni) ISP-om (D1 i D2), dok svjetski ISP-ovi (D1, D2, D3 i D4) imaju najvjerovatnije direkne linkove između sebe.

Dvije osnovne funkcije ISP-a su:

- obezbjeđuju kompaniji/pojedincu pristup WWW-u i omogućavaju uslugu slanja elektronske pošte budući da su ovo dva najpopularnija servisa Interneta i svaki ISP mora da obezbijedi pristup ovim servisima,
- obezbjeđuju postavljanje veb sajta na svojim serverima ili link ka serverima kompanije čime taj veb sajt postaje dostupan potrošačima i drugim kompanijama, što se naziva *hosting* veb sajta.

Elementi koji utiču na kvalitet usluga koje pruža ISP su: brzina, dostupnost i cijena, [90]. Brzina pristupa uslugama ISP-a određena je:

- brzinom mrežne konekcije sa serverom,
- brzinom računara korisnika: brzina procesora, količinom operativne memorije, brzinom hard diska,
- brzinom obrade informacija na serveru: da li su svi indeksni podaci na serveru ili ne,
- broj istovremenih korisnika,
- broj računara (korisnika) na kojima je realizovan server.

Mogli bismo dakle zaključiti da su pri izboru odgovarajućeg ISP-a preovlađujući naredni faktori:

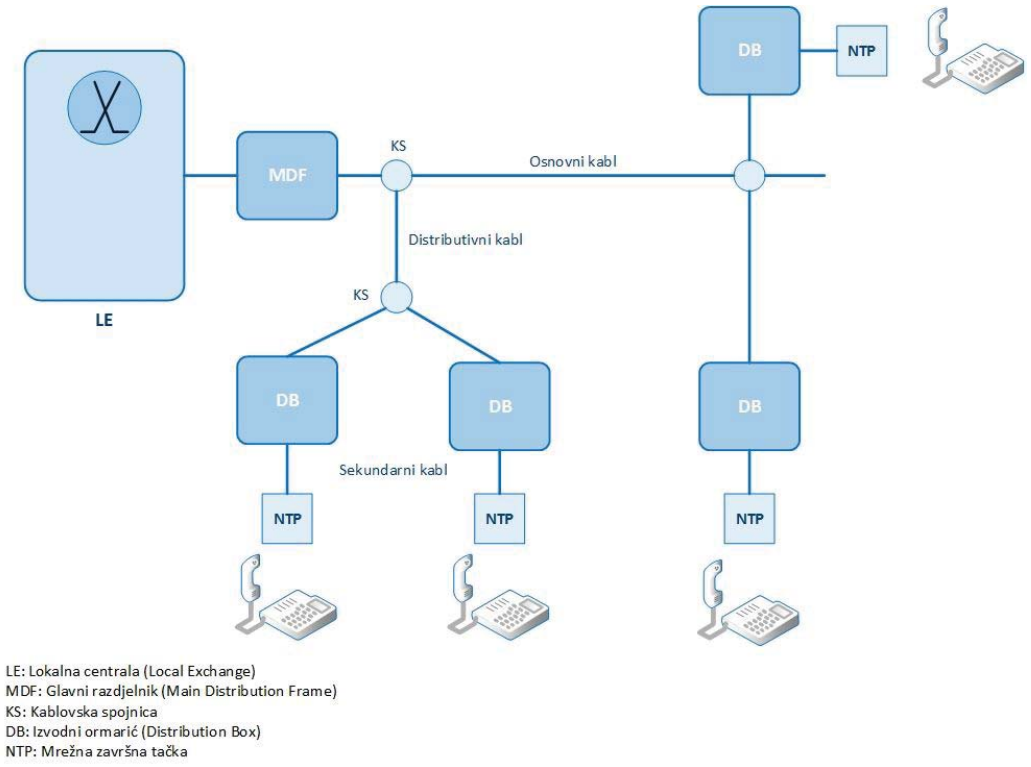
- raspoloživi propusni opseg (brzina linka ka Internetu),
- brzina kojom se preuzimaju stranice sa Interneta što je u vezi sa raspoloživim propusnim opsegom ISP-a i performansama njegovih servera,
- raspoloživost servera,
- skalabilnost; kako se ponaša veb server pri vršnom opterećenju,
- jednostavnost ažuriranja veb sajta,
- uspješnost u slanju e-pošte,
- sigurnost sajta,
- komercijalni faktori: cijena usluga i podrška koju obezbjeđuje ISP.

2.1.3.1. Pristupne mreže

Pristupna mreža se sastoji od višežilnih kablova, korisničkih parica, do razdjelnika, odakle se parica nastavlja do svakog pojedinačnog korisnika, kako je to prikazano na Sl 2.4.

Sa ekspanzijom Interneta javila se potreba za tehnologijom koja će omogućiti veće protoke u odnosu na ISDN (Integrated Digital Suscriber Line), uz što je moguće veću upotrebu postojeće mrežne infrastrukture (bakarnih parica). Rješenje je ponudila xDSL familija tehnologija koja omogućava pristup postojećoj PSTN mreži i uslugama koje ona pruža, kao i pristup Internetu sa velikim protocima, [10].

Ovdje ćemo ukratko nešto više reći samo o DSL tehnologijama koje se danas najviše koriste u pristupnoj mreži, [60], [61].



Slika 2.4 - *Organizacija pristupne mreže*

2.1.3.1.1. ADSL (Asimetric Digital Suscriber Line)

Upotrebom DMT modulacije (Discrete Multitone) kod ADSL-a se mogu postići brzine u dolaznom smijeru, ka korisniku, (download) od 8,192 Mbit/s a u odlaznom (upload) od 1024 Mbit/s. Pomoću diskretne Fourier-ove transformacije frekvencijski opseg od 1,1 MHz koji koristi ADSL (Slika 2.10) se dijeli na 256 potkanala (subchannels), pri čemu svaki potkanal koristi vlastiti podnosioc (subcarrier), a podaci se u svakom potkanalu prenose primjenom QAM (Quadrature Amplitude Modulation) modulacije. Linijska brzina po svakom potkanalu iznosi 4000 QAM simbola po sekundi. Broj bita po simbolu u svakom potkanalu se kreće od 0-15 (obično se uzima 8), [61], [90].

Kako je maksimalan broj potkanala u dolaznom smijeru 256 uz pomenutu linijsku brzinu od 4000 simbola po sekundi i za broj bita po simbolu od 8, dobit ćemo teorijsku brzinu u dolaznom smijeru od 8,192 Mbit/s, a za odlazni smijer u kojem se koriste 32 potkanala, teorijsku brzinu od 1,024 Mbit/s. Da bi se spriječila interferencija ADSL-a sa POTS-om (Plain Old Telephone System) obično se ne koristi pet potkanala, tako da su realne bitske brzine 8Mbit/s za dolazni, odnosno 864 kbit/s za odlazni smijer, [1].

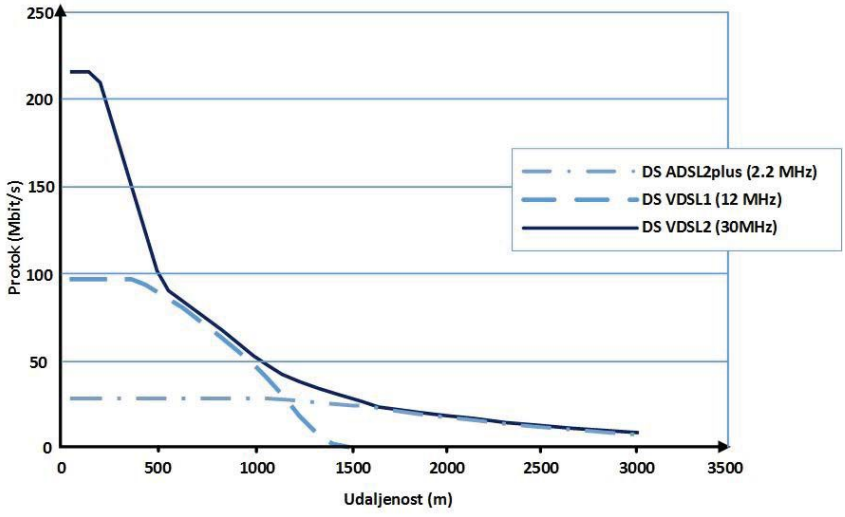
2.1.3.1.2. ADSL2

ADSL2 koristi istu širinu frekventnog opsega od 1,1 MHz, kao ADSL (Slika 2.6), ali su se poboljšanjem modulacione tehnike postigle značajno veće brzine u dolazu od 12 Mbit/s, dok je odlazna brzina 1 Mbit/s. ADSL2 omogućava smanjenje potrošnje električne energije jer modemi za vrijeme neaktivnosti prelaze u *standby* stanje. Vrijeme inicijalizacije modema je značajno skraćeno, uvedene su dodatne mogućnosti za nadzor sistema tokom rada, [1], [13],[61], [90]

2.1.3.1.3. ADSL2+

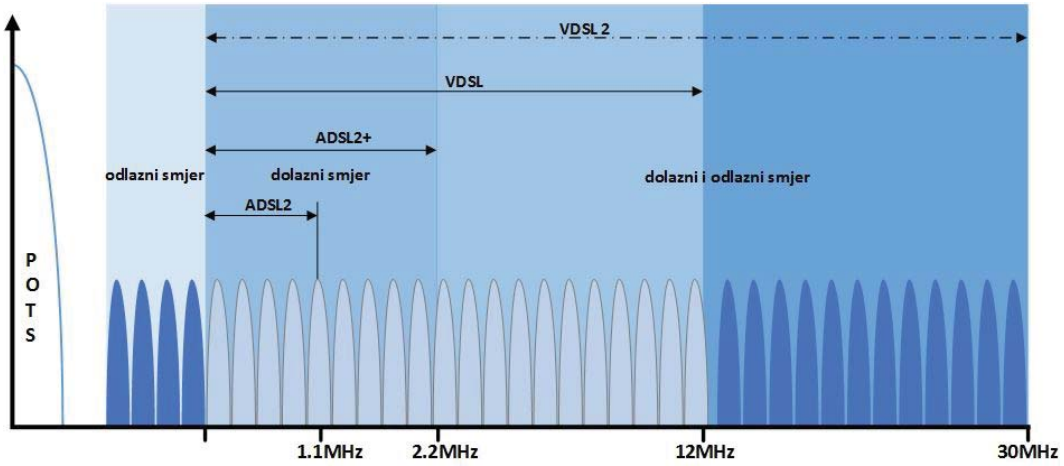
ADSL2+ koristi frekventni opseg od 2,2 MHz uz upotrebu 512 nosioca, što omogućava značajno povećanje protoka podatka (oko 25 Mbit/s za dolazni smijer) ali za male dužine lokalne petlje kako je to prikazano na Sl. 4.7, [1], [7], [13].

Na Sl. 2.5 možemo uočiti i to da je brzina prenosa podataka, odnosno protok, u obrnutoj srazmjeri sa dužinom pretplatničke petlje, tj veći protoci se mogu postići na manjim dužinama pretplatničke petlje.



Slika 2.5: *Zavisnost protoka od dužine pretplatničke petlje*

Frekvencijski opsezi koji se koriste kod pojedinih DSL tehnologija su sumarno predstavljeni na Sl. 2.6.



Slika 2.6: *Frekvencijski opsezi koji se koriste kod pojedinih DSL tehnologija*

2.1.3.1.4. VDSL i VDSL2 tehnologije, triple play koncept

Danas većina regionalnih operatera nastoji da omogući preko jedinstvene mrežne infrastrukture pružanje više servisa, odnosno razvoj *triple play* koncepta.

U telekomunikacijama *triple play* koncept predstavlja marketinšku oznaku za nuđenje usluga širokopojasnog pristupa Internetu, prenosa govora (VoIP, danas još uvijek u vidu IP Centrex usluge za poslovne korisnike) videa (IPTV i VoD) i podataka preko jednog širokopojasnog pristupa u zatvorenom mrežnom okruženju jednog operatera. Za uvođenje *triple play*-a primjena prethodno opisanih tehnologija neće biti dovoljna i postoji velika opasnost od stvaranja uskih grla i nemogućnosti realizacije servisa zbog neodgovarajućeg protoka u pristupnoj mreži, [1],[7],[13],[62],[90].

Za sticanje uvida u to koliki su protoci u pristupnoj mreži potrebni za realizaciju *triple play* servisa, uvrštena je Tabela 2.1, u kojoj su uzeti u razmatranje komercijalni paketi usluga koje u svojoj ponudi ima M:TEL kao regionalni operater, [88].

Za operatere koji su tek ušli na tržište i koji nemaju vlastitu mrežnu infrastrukturu rješenje bi bilo polaganje optike. Ali postojeći operateri koji su u postojeću infrastrukturu uložili ogromna sredstva i pored pojeftinjenja optičkih kablova (smatra se da cijena samih optičkih kablova predstavlja svega 6% ukupne investicije pri uvođenju optike), nastojat će da postojeću infrastrukturu zadrže što duže.

Tabela 2.1: *Potrebni protoci za triple play servise*

TRIPLE PLAY SERVISI	ODREĐIVANJE POTREBNOG KAPACITETA U PRISTUPNOJ MREŽI		
		ADSL paketi	Brzina download/upload (kbit/b)
Širokopojasni pristup Internetu	ADSL paketi u mreži M:TEL-a	HOBBY	512/128
		OPTIMA	1536/192
		OPTIMA +	3072/320
		PREMIUM	6144/384
		EXPERT	8192/512
IPTV kanali	Kanal standardne definicije (SD)	MPEG 2 sistem kodovanja	3,8 Mbit/s
		MPEG 4 sistem kodovanja	1,8 Mbit/s
	Kanal visoke definicije (HD)	MPEG 2 sistem kodovanja	1,8 Mbit/s
		MPEG-4 sistem kodovanja	6,8 Mbit/s
VoID kodni standardi i algoritmi kompresije govora	G.711/PCM (Pulse Code Modulation)		64
	G.726/ADPCM (Adaptive Diferential Pulse Code)		16; 24; 32
	G.728/LOCELP (Low/Delay Code Excited Linear)		16
	G.729/CS-ACELP (Conjugate Structure Algebraic)		8
	G.723.1/MP-MLQ (Multipulse Maximum Likelihood)		6,3

Kao rješenje nameće se kombinovanje optike sa uvođenjem novih xDSL tehnologija kao što su VDSL (Very High Speed DSL) i VDSL2 koje nude velike protoke ali za malu dužinu pretplatničke petlje (Sl.2.7), što je poznato kao FTTN koncept (Fiber to the Node). Ovdje će se postaviti novi problem a to je dovođenje napajanja u izdvojeni kabinet na udaljenosti do 1km od pretplatnika u kome će biti smješten DSLAM (Digital Signal

Access Multiplexer) i optička mrežna jedinica (ONU-Optical Network Unit), koja će izvršiti elektro-optičku konverziju nakon koje se signali razdvajaju prema zahtjevima korisnika i vode ka korisniku putem ADSL2+/VDSL/VDSL2 tehnologija, [13].

VDSL/VDSL2 koriste frekventne opsege od 12 odnosno 30MHz (Slika 2.6.) pa su brzine u dolaznom smijeru koje se mogu postići pomoću tih tehnologija velike, ali veoma brzo se smanjuju sa povećanjem dužine pretplatničke petlje (Slika 2.5.).

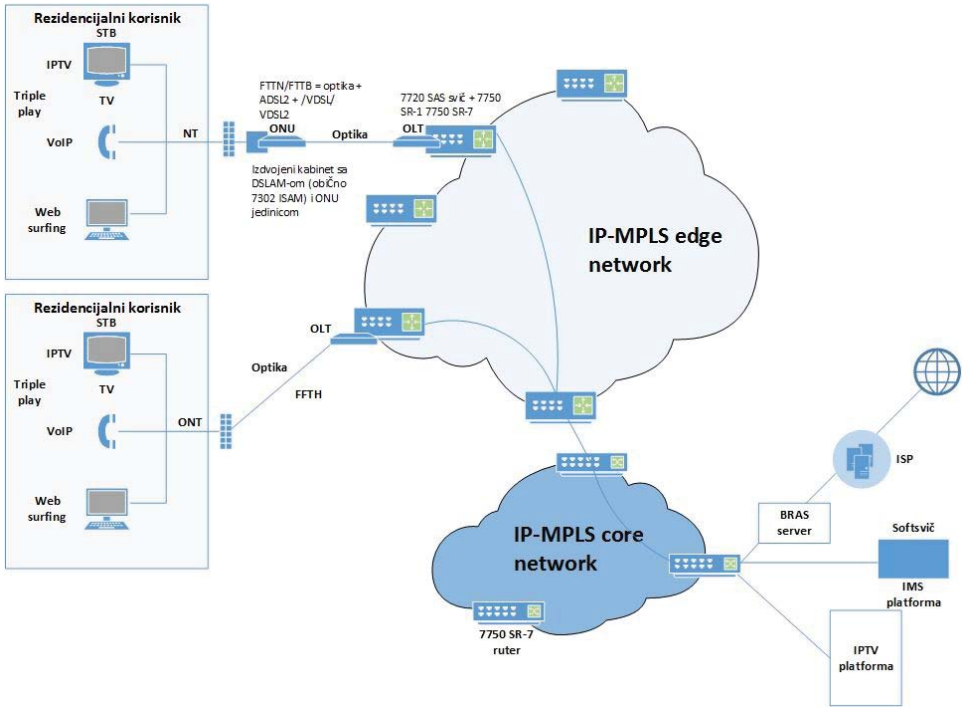
VDSL tehnologija podržava i simetričen i asimetričan prenos. Kad podržava simetričan prenos pomoću nje se mogu ostvariti protoci u dolaznom smijeru od oko 13Mbit/s na udaljenosti do 900m i 25Mbit/s na udaljenosti od oko 300m. Kad podržava asimetričan prenos pomoću nje se mogu ostvariti protoci u dolaznom smijeru od 52Mbit/s i odlaznom od 6 Mbit/s na udaljenosti do oko 300m, dok su ostvareni protoci na udaljenosti od oko 900m, 24Mbit/s u dolazu i 3Mbit/s u odlazu. VDSL2 podržava simetričan prenos i pomoću nje se mogu ostvariti protoci od 100Mbit/s na udaljenosti od oko 350m, [1].

Uvođenje VDSL2 tehnologije će dovesti do značajnih promjena u pristupnoj mreži. Naime, VDSL2 podržava prenos paketa (PMT-Packet Transfer Mode), što treba dovesti do eliminacije ATM-a u pristupnoj mreži i do uvođenja arhitekture koja će se u potpunosti zasnivati na Ethernetu (na magistralnoj mreži se već upotrebljavaju 10 Gbit/s linkovi čime je omogućeno povezivanje komutacionih čvorava koji se nalaze na velikim udaljenostima). To bi dovelo do boljeg iskorištenja kapaciteta pristupne mreže jer zaglavlje ćelije ATM-a iznosi 5 bajta naspram 48 bajta korisnog dijela.

T*riple play* servisi: širokopojasni pristup Internetu, IPTV i IP Centrex se prenose kao izolovani tokovi od xDSL modema do DSLAM-a (Sl.2.7) i dalje kroz magistralnu mrežu. Kao noseći protokol za komunikacija xDSL modema i DSLAM-a (kod ADSL, ADSL2 i ADSL2+ tehnologija) se koristi ATM (Asynchronous Transfer Mode), iako se u novije vrijeme radi na potpunom izbacivanju ATM sa pristupne mreže i prelaženju na Ethernet i u pristupnoj mreži, [2], [13],[14],[20].

ATM ćelijski tok po fizičkom linku je logički organizovan u virtuelne kanale (VC-Virtual Channel) i u virtelne staze (VP-Virtual Path). Za uspostavljanje veze korisniku je potreban jedan VC. Virtuelni kanali su grupisani u virtuelne staze, pri čemu je svakom VC-u u jednoj VP dodijeljen jedinstveni identifikacioni broj VCI (Virtual Channel Identifier), a svakoj VP u okviru jednog fizičkog linka jedinstven broj VPI (Virtual Path Identifier). Sve ćelije nose informaciju o VCI i VPI u svom zaglavlju. Ovi brojevi su isti za sve ćelije koje pripadaju istoj vezi. Na portu xDSL modema se svakom od navedena tri servisa *triple play*-a dodjeljuje jedinstveni VPI/VCI broj koji se na portu DSLAM/MSAN (Multi Service Access Node) mapira u odgovarajući VLAN (Virtual Local Area Network) za prenos od DSLAM/MSAN-a preko IP/MPLS (Multiprotocol Label Switching) magistrale i odgovarajućih rutera u odlaznom saobraćajnom toku (uplink), [87].

Ranije nabrojana tri servisa *triple play*-a se realizuju nezavisno preko odgovarajućih platformi (Sl.2.7) i to širokopojasni pristup Internetu preko ISP platforme i BRAS-a (Broadband Remote Access Server), IPTV preko IPTV platforme, a IP Centrex preko IMS (IP Multimedia Subsystem) platforme. Dakle iz razloga što se *triple play* servisi prenose kao nezavisni, paralelni tokovi kroz mrežu, to je u pristupnoj mreži između xDSL modema i DSLAM-a potrebno obezbijediti protok koji je jednak sumi protoka koji su potrebni za realizaciju svakog *triple play* servisa pojedinačno, [2].



Slika 2.7: *Kombinacija DSL tehnologija i optike u pristupnoj mreži*

Situacija se još više komplikuje u slučaju kad je potrebno krajnjem korisniku prenijeti više IPTV kanala, recimo da u jednom domaćinstvu ima više korisnika IPTV-a i više STB-ova i da oni žele da gledaju različite kanale u isto vrijeme. Tada bi nam bili neophodni protoci koji se mogu postići pomoću VDSL/VDSL2 tehnologija. Kao što smo već imali priliku da vidimo, uvođenjem tih tehnologija mogu se ponuditi veliki protoci u pristupnoj mreži ali na ograničenoj udaljenosti zbog činjenice o kojoj se mora voditi računa, a to je, da što je veća brzina prenosa podataka, to je i kraće rastojanje na koje se signal može efikasno prenijeti, jer se povećanjem dužine linije (udaljenosti pretplatnika od DSLAM-a) usljed nesavršenosti pretplatničkih linija, protok koji se može ponuditi korisniku smanjuje, o čemu je već bilo govora ranije, [43].

Kao logično rješenje nameću se pasivne optičke mreže (PON-Passive Optical Network). Prve pasivne optičke mreže su služile samo za prenos govora (TPON-Telephone Passive

Optical Networks), [78]. TPON su zatim prerasle u širokopojasne pasivne optičke mreže (BPON-Broadband Passive Optical Networks), koje su omogućile distribuciju širokopojasnih servisa. Danas se u Evropi i SAD koristi GPON (Gigabit PON), kao daleko najnaprednije rješenje, dok telekom operateri u Aziji koriste EPON (Ethernet PON). Poređenje karakteristika različitih PON rješenja je dato u Tabeli 2.2.

Tabela 2.2: *Poređenje PON sistema*

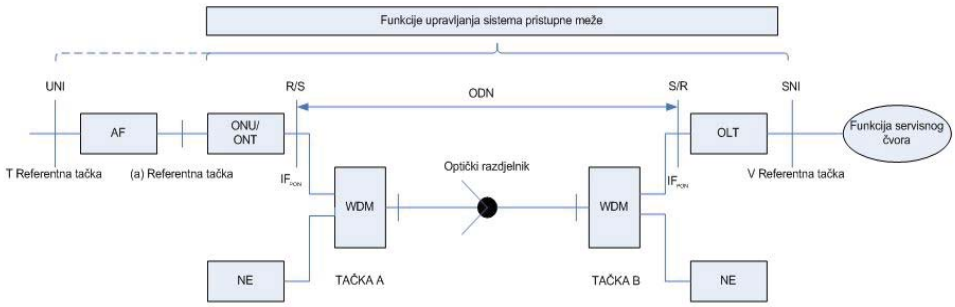
KARAKTERISTIKE	EPON	BPON	GPON
Standard	IEEE 802.3ah	ITU-T G.983	ITU-T G.984
Protokol	Eternet	ATM	Eternet, TDM
Protok (dolaz/odlaz Mbit/s)	1250 / 1250	622 / 155	2488 / 1244
Raspon (km)	10	20	20
Odnos dijeljenja	13	32	64

Budući da GPON podržava najveće brzine prenosa, što se može vidjeti i iz tabele 2.2, on omogućava uvođenje širokog opsega aplikacija i usluga i smatra se najboljim rješenjem za pristupnu mrežu sledeće generacije (NGA-Next Generation Access), [10], [51].

GPON pruža simetričnu brzinu prenosa podataka od 1.25 Gbit/s ili asimetričnu od 2.5 Gbit/s za *download* i 1.25 Gbit/s za *upload* za udaljenosti do 20 km. Na fizičkom interfejsu GPON može koristiti TDM i WDM tehnologiju, [32], [33].

GPON je point-to-multipoint tehnologija (Sl.2.8). GPON sistemi se sastoje od optičkog linijskog terminala (OLT-Optical Line Terminal), optičke mrežne jedinice (ONU-Optical Network Unit) ili od optičkog mrežnog terminala (ONT-Optical Network Terminal) koji su povezani optičkom distributivnom mrežom (ODN-Optical Distribution Network).

Primjena pasivnih optičkih mreža može dovesti do značajne uštede u količini potrebnih optičkih vlakana, jer se snaga signala koji se šalju ka krajnjim korisnicima dijeli u odnosu 1:N, pri čemu je N broj krajnjih korisnika koji su vezani na pasivni optički razdjelnik. Tipična GPON instalacija podrazumjeva optimalnu vrijednost dijeljenja 1:32, ali je moguć i odnos 1:64 kod postojećih izvedbi (Tabela 4.2.). Predviđa se da će se poboljšanjem optičkih modula postići odnos 1:128.



ONU	Optial Network Unit
ONT	Optical Network Terminal
ODN	Optical Distribution Network
OLT	Optical Line Termination
WDM	Wavelength Division Multiplex Module (Ukoliko se WDM ne koristi, ova funkcija nije neophodna)
NE	Mrežni element koji koristi različitu talsnu dužinu od OLT i ONU
AF	Funkcija adaptacije (Ponekad može biti uključen u ONU)
SNI	Service Node Interface
UNI	User Network Interface
S	Tačka na optičkom vlaknu poslije OLT-a (Downstream)/ONU (Upstream) tačke optičke veze (npr. optički konektor ili splajsovani optički nastavak)
R	Tačka na optičkom vlaknu prije OLT (Downstream)/OLT(Upstream) tačke optičke veze (npr. optički konektor ili splajsovani optički nastavak)
(a) Referentna tačka	Ukoliko je AF uključen u ONU, ova tačka nije neophodna
POINT A/B	Ukoliko se WDM nekoristi, ova tačka nije neophodna

Slika 2.8: *GPON*

Optička snaga signala pasivnog optičkog razdjelnika se raspodjeljuje jednako od OLT-a ka svim povezanim ONT-ovima na talasnoj dužini 1490 nm. U suprotnom smjeru, od ONT-ova ka OLT-u, optički signal se prenosi na talasnoj dužini 1310 nm.

Modeli koji kombinuju neku od PON tehnologija sa ADSL2/VDSL/VDLS2 u pristupu su:

- FTTN (Fiber to the Node): zahtijeva postavljanje DSLAM-a u na udaljenosti do 1km od pretplatnika i primjenu ADSL2+/VDSL/VDSL2 tehnologija u pristupnoj mreži.
- FTTB (Fiber to the Building): mali DSLAM koji se smješta u samu zgradu dok se se u pristupnoj mreži koristi VDSL/VDSL2.
- FTTH (Fiber to the Home): optika direktno do stana korisnika.

Zajednički naziv za ove arhitekture je FTTx, [71]. FTTH arhitektura je trenutno najpopularnija za područja bez postojeće infrastrukture (greenfield areas) kako za tradicionalne telekom operatere tako i za alternativne telekom operatere, uzimajući u obzir i to da troškovi izgradnje infrastrukture zasnovane na bakarnim paricama premašuju troškove izgradnje infrastrukture zasnovane na optičkim kablovima. U ovom slučaju OLT, koji se nalazi u centrali (CO-Central Office), povezan je optičkim vlaknom sa ONT-om, koji je instaliran u stanu pretplatnika (Sl.2.7). Umjesto FTTH se ponekad koristi naziv FTTP (Fiber to the Premises).

FTTC može biti atraktivno rješenje za područja gdje tradicionalni telekom operateri već imaju infrastrukturu zasnovanu na bakarnim paricama (brownfield areas).

FTTB je veoma popularno rješenje za urbana područja sa neboderima, gdje se optičko vlakno uvodi u zgradu tj. OLT je povezan optičkim valknima sa ONU, koja se instalira u samoj zgradi, odakle se koristi VDSL2 tehnologija do mrežnog završetka (NT-Network Termination), koji je instaliran u samom stanu pretplatnika.

FTTN zahtjeva postavljanje optičkog kabla od pretplatnika do udaljenog DSLAM-a, na udaljenosti od nekoliko kilometara. Servisi se onda isporučuju optičkim vlaknom putem ADSL2+. FTTN se po svojim karakteristikama može posmatrati i kao varijanata DSL-a, uzimajući u obzir da su brzine prenosa (12-20 Mbit/s) dosta manje u odnosu na brzine koje se ostvaruju primjenom FTTC, FTTB i FTTH (50-100 Mbit/s). Dugoročno gledano, FTTN arhitektura je limitirana po pitanju naprednih TV i video servisa.

Za povećanje protoka u pristupnoj mreži, ali i za povećanje dometa do pretplatnika kome treba omogućiti servis idealno bi bilo uvesti optiku do kuće, tj primijeniti FTTH model, ali je to za operatera još uvijek suviše skupo rješenje. Zato se operateri najčešće odlučuju na kombinovanje novih DSL tehnologija velikog protoka sa optikom, odnosno na primjenu FTTN-a i FTTB-a u kombinaciji sa ADSL2+/VDSL/VDSL2 čime je omogućena primjena postojeće bakarne infrastrukture.

POGLAVLJE 3

Osnove prenosa podataka

U ovom poglavlju su date osnove digitalnog prenosa podataka. Opisan je način komunikacije čovjeka pomoću tastature sa računarom, objašnjena je neophodnost prilagođenja signala prenosnom medijumu radi prenosa na velike udaljenosti. Objašnjen je osnovni model komunikacionog sistema.

3.1. Binarni brojni sistem

U svakodnevnoj upotrebi ljudi koriste decimalni brojni sistem. Međutim, računari za predstavu brojeva koriste binarni brojni sistem, kod koga se jedna cifra predstavlja sa dvije vrijednosti, nula ili jedinica. Razlog zašto računari koriste binarni brojni sistem jeste u tome da se većina komponenata računara bazira na elektronskim elementima koji razlikuju samo dva stanja; da li struje ima ili nema, [52].

Prevod iz jednog sistema u drugi je jednostavan.

Primjer:

1345 (decimalno) = 10101000001 (binarno)

Prevođenje iz decimalnog kodnog sistema u binarni se vrši na sledeći način:

$1x2^{10}=$ 1024
$0x2^{9}=$ + 0
$1x2^{8}=$ + 256
$0x2^{7}=$ + 0
$1x2^{6}=$ + 64
$0x2^{5}=$ + 0
$0x2^{4}=$ + 0
$0x2^{3}=$ +.....0
$0x2^{2}=$ + 0
$0x2^{1}=$ + 0
$1x2^{0}=$ + 1
= 1345

Prednost binarnog brojnog sistema je lakoća kojom se binarni brojevi mogu elektronski implementirati budući da svaka cifra ili bit ima samo dva električna stanja ili „0“ (off) ili 1 (on).

3.2. Upotreba binarnog koda za predstavu tekstualnih informacija i slika

Termin „podatak“ se koristi da opiše informaciju koja se memoriše i obrađuje u računaru. U komunikaciji sa računarom koriste se različiti tipovi podataka; tekst, slika, zvuk, video.

Većina izvornih poruka u komunikacionim sistemima (izuzimajući računar-računar komunikaciju) je ili tekstualna ili analogna. Čovjek pri komunikaciji sa računarom koristi neke standardne znakove poput slova, cifara decimalnog brojnog sistema, različitih specijalnih znakova i sl. Da bi računar mogao prihvatiti ove podatke potrebno je da ih pretvori u oblik koji on razumije, odnosno sukup „0“ i „1“, odnosno potrebno je izvršiti kodiranje, [52].

Def.: *Kodiranje predstavlja pretvaranje jednog skupa simbola u drugi.*

Da bi se predstavile sve cifre decimalnog brojnog sistema, sva slova, specijalni znaci, te da bi se u kod ugradile i odgovarajuće kontrole, danas se najčešće koriste kodovi sa 8 binarnih cifara, kojim se može predstaviti 2^8=256 znaka.

Najpoznatiji je 8-bitni IBM-ov prošireni ASCII (American Standard Code for Information Interchange), koje je prikazan u Tabeli 3.1.

Kao primjer kodovanja jednog alfanumeričkog karaktera uzet ćemo slovo „C“, koje se binarno koduje kao „0100 0011“, dakle prvo od MSB (Most Significant Bits) bita, dok se prilikom prenosa telekomunikacionom linijom prvo prenose biti najmanje važnosti (Least Significant Bits), dakle za slovo „C“ to je „1100 0010“.

Ovdje treba istaći da postoji razlika između kodiranja i konverzije decimalnog broja u binarni. Naime ako bismo preveli broj „0100 0011“ u decimalni, dobili bismo broj 67. To je zbog toga što se prilikom konverzije posmatra decimalan broj kao cjelina, a kod kodovanja se posmatra cifra po cifra.

Uzet ćemo kao primjer decimalni broj 10.

- Njegovim prevođenjem u binarni dobijamo 1010
- Kodiranjem u ASCII dobijamo 0011000100110000

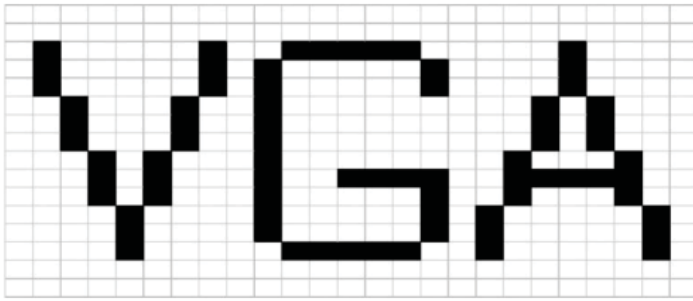
Prilikom unošenja podataka pomoću tastature računara, podaci se koduju na opisani način, da bi se potom odgovarajućim algoritmom preveli u odgovarajuću binarnu vrijednost. Nakon obrade u računaru rezultat se opet mora kodirati radi njegovog prikaza korisniku.

Tabela 3.1: *ASCI kod*

HEX CODE YX				X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
	BITS			4	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
				3	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
				2	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
Y	8	7	6	1 5	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
0	0	0	0	0	0	1 ☺	2 ☻	3 ♥	4 ♦	5 ♣	6 ♠	7 •	8 ◘	9 ○	10 ◙	11 ♂	12 ♀	13 ♪	14 ♫	15 ☼
1	0	0	0	1	16 ►	17 ◄	18 ↕	19 ‼	20 ¶	21 §	22 ▬	23 ↨	24 ↑	25 ↓	26 →	27 ←	28 ∟	29 ↔	30 ▲	31 ▼
2	0	0	1	0	32 spce	33 !	34 "	35 #	36 $	37 %	38 &	39 '	40 (	41)	42 *	43 +	44 ,	45 -	46 .	47 /
3	0	0	1	1	48 0	49 1	50 2	51 3	52 4	53 5	54 6	55 7	56 8	57 9	58 :	59 ;	60 <	61 =	62 >	63 ?
4	0	1	0	0	64 @	65 A	66 B	67 C	68 D	69 E	70 F	71 G	72 H	73 I	74 J	75 K	76 L	77 M	78 N	79 O
5	0	1	0	1	80 P	81 Q	82 R	83 S	84 T	85 U	86 V	87 W	88 X	89 Y	90 Z	91 [	92 \	93]	94 ^	95 _
6	0	1	1	0	96 `	97 a	98 b	99 c	100 d	101 e	102 f	103 g	104 h	105 i	106 j	107 k	108 l	109 m	110 n	111 o
7	0	1	1	1	112 p	113 q	114 r	115 s	116 t	117 u	118 v	119 w	120 x	121 y	122 z	123 {	124 ¦	125 }	126 ~	127 ⌂
8	1	0	0	0	128 Ç	129 ü	130 é	131 â	132 ä	133 à	134 å	135 ç	136 ê	137 ë	138 è	139 ï	140 î	141 ì	142 Ä	143 Å
9	1	0	0	1	144 É	145 æ	146 Æ	147 ô	148 ö	149 ò	150 û	151 ù	152 ÿ	153 Ö	154 Ü	155 ¢	156 £	157 ¥	158 Pts	159 ƒ
A	1	0	1	0	160 á	161 í	162 ó	163 ú	164 ñ	165 Ñ	166 ♀	167 ♂	168 ¿	169 ⌐	170 ¬	171 ½	172 ¼	173 ¡	174 «	175 »
B	1	0	1	1	176 ▒	177 ▒	178 ▓	179 ┤	180 ┤	181 ╡	182 ╢	183 ╖	184 ╕	185 ╣	186 ‖	187 ╗	188 ╝	189 ╜	190 ╛	191 ┐
C	1	1	0	0	192 └	193 ┴	194 ┬	195 ├	196 ─	197 ┼	198 ╞	199 ╟	200 ╚	201 ╔	202 ╩	203 ╦	204 ╠	205 ═	206 ╬	207 ╧
D	1	1	0	1	208 ╨	209 ╤	210 ╥	211 ╙	212 ╘	213 ╒	214 ╓	215 ╫	216 ╪	217 ┘	218 ┌	219 ▉	220 ▄	221 ▌	222 ▐	223 ▀
E	1	1	1	0	224 α	225 ß	226 Γ	227 π	228 Σ	229 σ	230 µ	231 τ	232 Φ	233 θ	234 Ω	235 δ	236 ∞	237 ø	238 ∈	239 ∩
F	1	1	1	1	240 ≡	241 ±	242 ≥	243 ≤	244 ⌠	245 ⌡	246 ÷	247 ≈	248 °	249 •	250 ·	251 √	252 ⁿ	253 ²	254 ■	255 blnk

U upotrebi su i drugi prošireni 8-bitni ASCII (American Standard Code for Information Interchange) kodovi kao što je text/html (ISO 8859-1).

Pored prenosa numeričkih i alfanumeričkih (ili tekstualnih) karaktera, binarni kod se koristi i za prenos, memorisanje, odnosno obradu slika u računaru. Najčešće se koristi tehnika pri kojoj se slika pretvara u veliki broj tačaka, bitmapu. Tačke (pikseli) predstavljaju osnovne elemente slike. Računar čuva podatke o svakoj pojedinačnoj tački i na osnovu toga prikazuje i obrađuje sliku, [52].



Slika 3.1: *Ilustracija predstavljanja grafika binarnim kodom*

Za prikaz crno-bijele slike koristi se jedan bit za svaku tačku (piksel), pri čemu se bit „1“ koristi za reprezentaciju crne a „0“ za bijelu boju (osvjetljava se, odnosno zatamnjuje tačka na ekranu). Razmatranje rešetke od 400 bita počinjemo od krajnje lijeve tačke i analiza se vrši red po red sa lijeva na desno, tako da u binarnom brojnom sistemu naša slika sada postaje:

00000 00000 00000 00000 00000

00000 00000 00000 00000 00000

01000 00100 11111 00000 10000

01000 00101 00000 10000 10000

01000 00101 00000 10000 10000

00100 01001 00000 00001 01000

00100 01001 00000 00001 01000

00100 01001 00000 00001 01000

00010 10001 00000 00010 00100

00010 10001 00111 10011 11100

00010 10001 00000 10010 00100

00001 00001 00000 10100 00010

00001 00001 00000 10100 00010

00001 00000 11111 00100 00010

00000 00000 00000 00000 00000

00000 00000 00000 00000 00000

Slova „VGA“ se preko ASCII koda mogu predstaviti sa 24 bita (01010110 01000111 01000001), dok smo u našem primjeru koristili čak 400 bita. Konverzija 24-bitnog formata u 400-bitni se odvija na sloju prezentacije OSI modela.

Za rezoluciju od 640x480 crno bijele slike potrebno je, dakle, 307 200 bitova. Budući da se za predstavu svake tačke koristi samo jedan bit, to imamo mogućnost upotrebe samo dvije boje, što nije realan slučaj u praksi. Obično se za predstavu svake tačke koristi znatno više bita. Za televiziju u boji se koristi najčešće 24 bita što nam daje mogućnost upotrebe približno 16 miliona boja.

3.3. Električna predstava binarnih brojeva

Prednost binarnog brojnog sistema jeste u lakoći kojom se binarni brojevi mogu predstaviti električno. Tako se binarna jedinica može predstaviti prisustvom struje (ili napona) na liniji, a binarna nula njihovim odsustvom, [52].

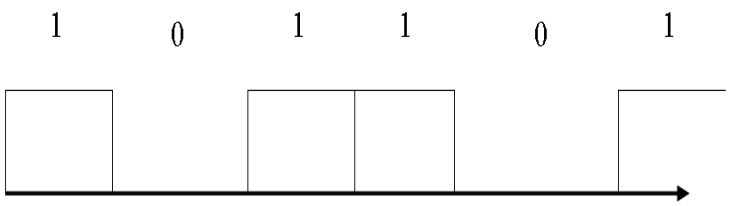
Sa bitom se često predstavlja i jedinica mjere količine informacije (binarni događaj čija su oba stanja jednako vjerovatna nosi informaciju od 1 bita).

***Def.: Bit** (binarni digit): Osnovna informaciona jedinica u digitalnim sistemima se predstavlja impulsom sa dva moguća amplitudna stanja, a koja simbolično označavamo sa „0“ i sa „1“.*

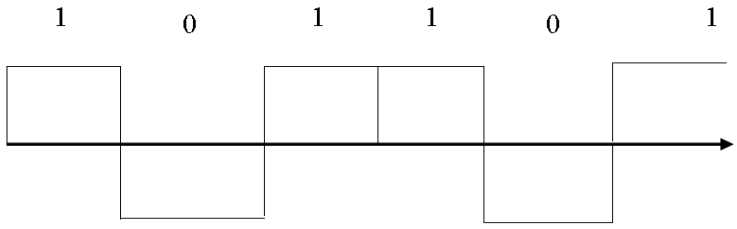
Najjednostavniji i u praksi najzastupljeniji je binarni oblik digitalnog signala koji se može predstaviti sa dvije različite vrijednosti napona, odnosno struje. Ovdje ćemo predstaviti unipolarni i polarni binarni signal bez povratka na nulu iako postoje i unipolarni i polarni signal sa povratkom na nulu i diferencijalno kodovani binarni signal.

***Def.:** Digitalni signal jeste diskretan signal koji se sastoji od povorke pravougaonih impulsa određene amplitude i trajanja.*

Na Sl. 3.2, Sl.3.3 i Sl.3.4 su dati najčešći naponski (strujni) oblici signala za predstavljanje bita informacija.



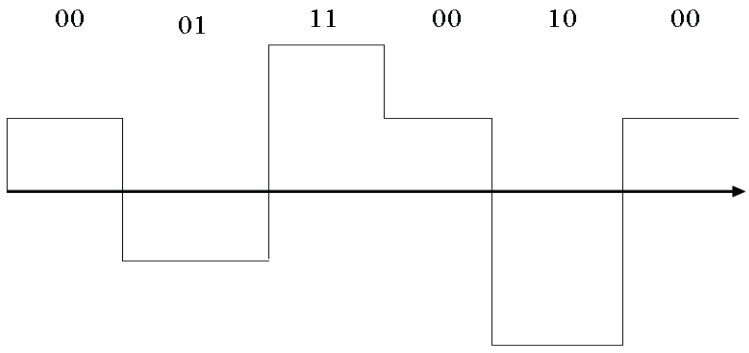
Slika 3.2: *Unipolarni signal bez povratka na nulu*



Slika 3.3: *Polarni signal sa povratkom na nulu*

U opštem slučaju digitalni signal se može predstaviti sa M različitih naponskih, odnosno strujnih nivoa.

Def.: *Simbole predstavljaju grupe od k bita koje se kombinuju tako da formiraju cifre ili simbole iz konačnog skupa od $M=2^k$ simbola; sistem koji koristi simbole iz skupa veličine M naziva se M-arni sistem.*

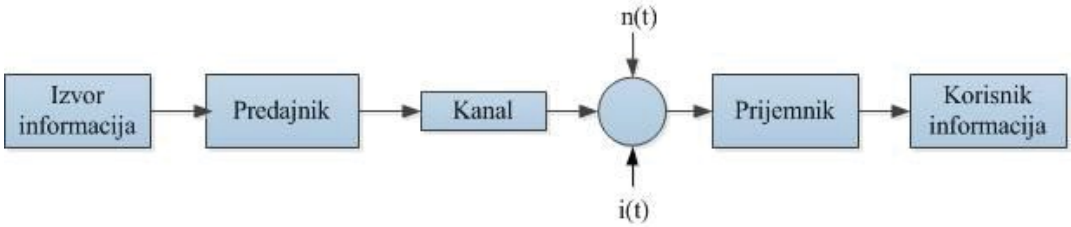


Slika 3.4: *Kvaternarni oblik signala*

Za prenos signala na male udaljenosti vrši se neposredno pretvaranje bita u napon, ali za prenos na veće udaljenosti potrebno je izvršiti prilagođenje signala uslovima prenosa, što će biti objašnjeno u nastavku.

3.4. Osnovni model komunikacionog sistema

Na Sl. 3.5 je prikazan osnovni model komunikacionog sistema. Njegov zadatak je da omogući razmjenu informacija između izvora informacija i korisnika informacija.



Slika 3.5: *Osnovni model komunikacionog sistema*

Definisat ćemo osnovne elemente sa Sl.3.5.

Def.: *Izvor informacija predstavlja bilo kakav objekat koji generiše poruke.*

Def.: *Poruke se iz izvora informacija transformišu u signale koji su električni ekvivalenti prenošene poruke.*

Def.: *Signali mogu biti analogni i digitalni. Analogni signal ima beskonačan broj vrijednosti između dvije ekstremne, maksimalne i minimalne, dok digitalni signal ima konačan (diskretan broj) vrijednosti.*

Primjer analognog signala je ljudski govor, a primjer analognog komunikacionog sistema jeste klasični telefonski sistem (PSTN-Public Switched Telephony System) čija je osnovna usluga upravo prenos govora (POTS-Plane Old Telephony System). U potpuno analognom komunikacionom sistemu, signal se od izvora do odredišta (korisnika informacije) prenosi duž čitavog puta u analognom obliku. Potpuno analognih sistema danas je jako malo, tako da ćemo se orijentisati na digitalne komunikacione sisteme.

Def.: *Predajnik transformiše signal poruke iz izvora informacije u oblik pogodan za prenos.*

Podaci sa kojima računar barata su isključivo digitalnog tipa, pa ako je potrebno da se izvrši prenos preko analognog medijuma (recimo telefonske linije) potrebno je izvršiti D/A konverziju (demodulacija), odnosno A/D konverziju (modulacija) što se radi putem modema.

Def.: *Kanal predstavlja fizički medijum koji spaja predajnik i prijemnik i kroz koji se obavlja prenos informacija (npr telefonski kanal, optički kanal, mobilni radio kanal, satelitski kanal)*

Signal se na prenosnom putu izobličava, dodaju mu se šum i interferencija.

Def.: *Šum predstavlja bilo koji neželjeni električni signal koji je uvijek prisutan u električnim sistemima, koji maskira i izobličava prenošeni signal i doprinosi ograničavanju sposobnosti prijemnika da donese korektnu odluku o primljenom simbolu.*

Najčešći izvor šuma jeste atmosferski uticaji, ali i vještački šum nastao uticajem čovjeka.

Da bi se okarakterisao kvalitet prenosa u analognim i digitalnim komunikacionim sistemima uvodi se kvantitativna mjera uticaja šuma.

- kod analognog prenosa to je odnos signal šum (SNR-Signal to Noise Ratio),
- kod digitalnom prenosa to je vjerovatnoća greške po bitu (BER-Bit Error Rate).

Def.: *Interferencija nastaje kao posljedica neželjenih signala (neželjenih električnih uticaja) drugih izvora čime dolazi do izobličenja prenošenog korisnog signala.*

Kao primjer interferencije navest ćemo preslušavanje do kojeg dolazi usljed neželjenog električnog uticaja koji se prenosi između parica koje se nalaze u istom pretplatničkom kablu u pristupnoj mreži, o čemu će biti više govora u nastavku.

3.4.1. Prilagođenje prenošenog signala uslovima prenosa

Signal u svom osnovnom obliku (kakav se pojavljuje na izlazu iz pretvarača poruka-signal nije pogodan za prenos na udaljeni kraj pomoću električnih provodnika. Da bi se to uradilo potrebno je izvršiti prethodnu obradu originalnog signala.

Suština metode je: jednom pomoćnom periodičnom signalu se modificiraju neki od njegovih osnovnih parametara, tako da on postane nosilac originalnog signala, a samim tim i prenošene poruke, [52].

Def.: *Postupak u kojim se modificiraju izvjesni parametri jednog periodičnog signala u funkciji karakterističnih veličina nekog drugog signala se naziva modulacijom.*

Cilj modulacije je da se signal obradi tako da postane podesan za prenos.

Def.: *Signal originalan nosilac poruke se naziva modulišućim signalom, pomoćni periodični signal nosiocem, dok se modulišućim signalom modificirani nosioc naziva modulisanim signalom.*

Na mjestu prijema modulisani signal se podvrgava inverznom procesu: iz modulisanog signala se izvlači originalan signal koji nosi poruku i taj postupak se naziva demodulacijom.

Sklop kojiim se obavlja modulacija naziva se modulatorom a onaj kojim se obavlja demodulacija demodulatorom. Modulator i demodulator jednim imenom nazivamo modemom.

I kod analognih i kod digitalnih modulacija, signal nosioca je sinusni signal oblika $A_c cos(2\pi f_c + \phi)$ u koji se utiskuje informacija da bi se prenijela do korisnika. Kod digitalnih modulacija, mudulišući signal je diskretnog tipa.
Ako je originalni signal analogni, potrebno ga je dakle prvo diskretizovati, što se sprovodi u saglasnosti sa Nyqusit-ovom teoremom o odairanju koja glasi:

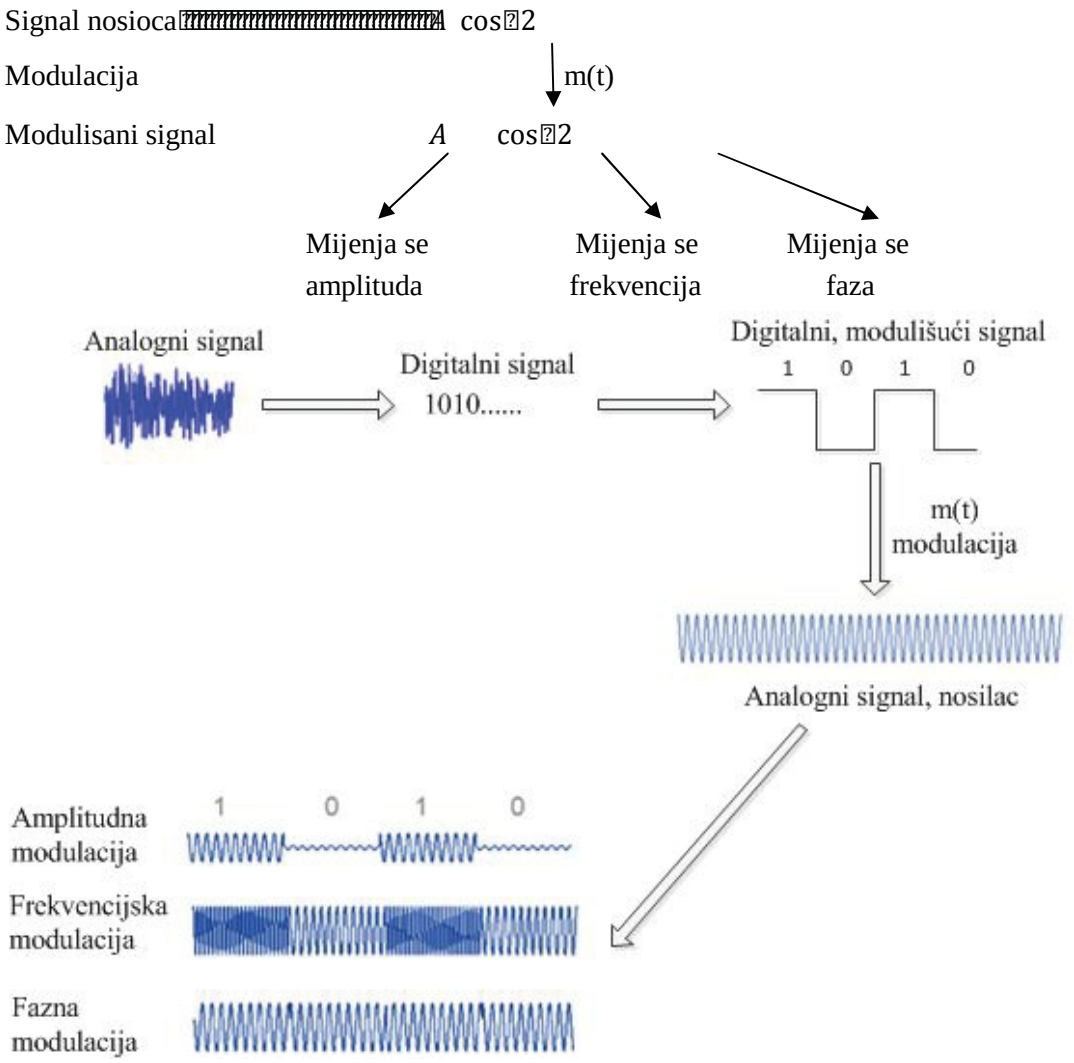
Def. Nyquist-ove teorema o odabiranju: *Ako se signal odabira u ekvidistantnim intervalima brzinom koja je najmanje dvaput veća od najveće frekvencije u spektru signala, tada odbirci sadrže svu informaciju o originalnom signalu.*

Primjer:

Ljudski glas se odmjerava 8000 puta u sekundi sa 8 bita po odmjerku (uzorku, semplu). Rezultujući signal je 64 kbit/s. Muzika se odmjerava sa 44100 odmjeraka u sekundi sa 16 bita po uzorku. To daje signal od 705, 6 Kbit/s za mono, odnosno 1,411 Mbit/s za stereo.

Odbirci su definisani njihovim položajem u vremenu, određenim korakom odabiranja i trenutnom vrijednošću inteziteta modulišućeg signala u trenucima odabiranja.

Digitalni modulacioni metodi se mogu posmatrati kao A/D konverzije, dok se demodulacija može posmatrati kao D/A konverzija.



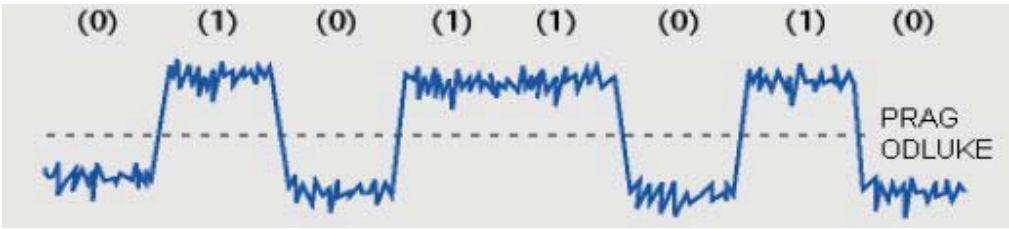
Slika 3.6: *Postupak digitalne modulacije*

3.4.2. Dekodovanje binarnih poruka

Bez obzira koji se prenosni medijum i vrsta modulacije koristi, na prijemu je potreban detektor ili demodulator. Idealni četvorougaoni impuls se tokom prenosa izobliči usljed različitih efekata, kao što su slabljenje, izobličenje i šum. Zadatak detektora je da odredi da li primljena vrijednost odgovara binarnoj jedinici ili nuli, što imlicira da mora postojati neki prag odlučivnja na prijemu, kao što je to prikazano na Sl.3.7.

Amplitude originalnog signala su opsegu od 0 do 1, a prag odlučivanja je postavljen na 0.5, što znači da svim oni signalima čije su amplitude ispod 0.5, detektor dodjeljuje

binarnu „0“, a svim onim signalima čije su amplitude iznad 0.5, detektor dojeljuje binarnu „1“.

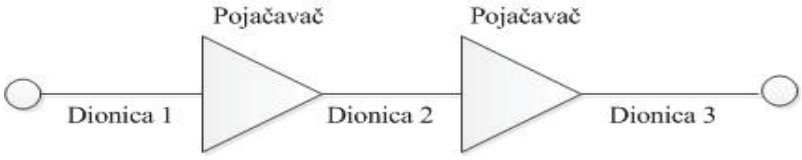


Slika 3.7: *Izobličen digitalni signal na prijemu*

Signal na Sl. 3.7 je pretrpio izvjesna oštećenja, ali su i dalje jasno vidljive visoke i niske vrijednosti signala. Ovakav signal se na regeneratorskim dionicama može očistiti od izobličenja radi daljeg prenosa na veću udaljenosti.

Ovdje se ogleda i prednost digitalnog sistema prenosa u odnosu na analogni sistem jer analogni sistem nema mogućnost regeneracije signala, dok digitalni ima.

Kod analognog sistema prenosa (Slika 3.8), radi prenosa na veće udaljenosti periodično se ubacuju pojačavači, koji zajedno sa korisnim signalom pojačavaju i šum, tako da se nakon nekoliko pojačavačkih dionica signal previše izobliči, što značajno ograničava udaljenost na koju se može prenijeti analogni signal a da odnos S/N bude još uvijek zadovoljavajući.



Slika 3.8: *Analogni sistem prenosa*

Kod digitalnog sistema prenosa (Slika 3.9), ubacuju se regeneratori koji imaju zadatak da na osnovu nekog od algoritama za detekciju greške (šeme zaštitnog kodovanja), grešku isprave i da na svom izlazu generišu potpuno novu bitsku sekvencu, identičnu originalnoj, koja je dakle oslobođena greški.

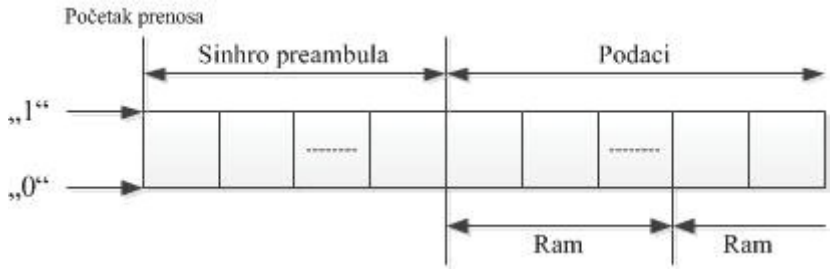
Slika 3.9: *Digitalni sistem prenosa*

3.5. Sinhronizacija

Tačnost prenosa podataka ne zavisi samo od tačnosti kodovanja prenošenog signala već i od sposobnosti prijemnog uređaja da izvrši tačno dekodovanje. Dakle, potrebna je sinhronizacije predajnika i prijemnika, kako bi se slanje i prijem svih bita informacija odvijalo u tačnim i predvidljivim intervalima, za što je potrebno izvršiti sinhronizaciju predajnika i prijemnika.

Postoje sinhroni i asinhroni način prenosa. Kod asinhronog prenosa emituju se neregularno raspoređeni karakteri, kod sinhronog karakteri se emituju u regularnim vremenskim intervalima.

Kod asinhronog prenosa generator takta na predaji i prijemu su nominalno isti, ali su nezavisni. Kod sinhronog prenosa, informacija o taktu se dobija iz primljenog signala. Danas se koristi većinom sinhroni način prenosa.



Slika 3.10: *Format poruke pri sinhronom prenosu*

Kod sinhronog prenosa preambula služi za uspostavu takta, a tokom daljeg prenosa, informacija o taktu se osvježava iz primljenog signala, [52].

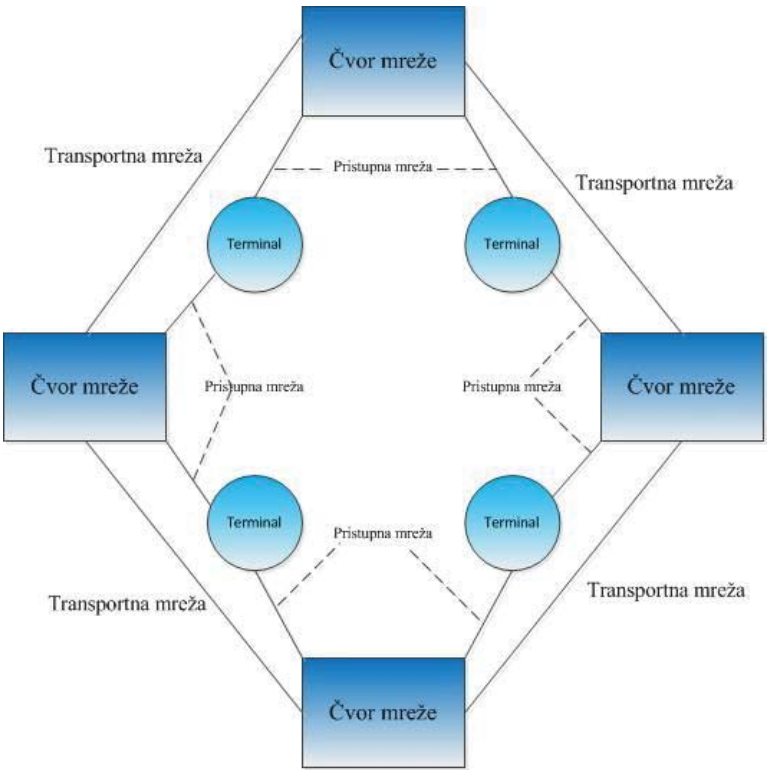
3.6. Mreža za prenos podataka

Prvo ćemo se upoznati sa osnovnim elementima mreže za prenos podataka (bilo koje) i sa osnovnim koracima pri usmjeravanju saobraćaja.

Sastavni elementi mreže za prenos podataka su dati na Sl.3.11.

Kako se vidi sa Sl.3.11, sastavni elementi mreže za prenos podataka su:

- čvorovi mreže: usmjeravaju saobraćaj kroz mrežu (telefoni, računari),
- prenosni sistemi: vrše povezivanje čvorova mreže,
- terminal: uređaj pomoću koga korisnik pristupa telekomunikacionoj mreži,
- pristupna mreža: obezbjeđuje povezivanje terminala sa čvorovima mreže.



Slika 3.11*: Sastavni elementi mreže za prenos podataka*

Osnovni koraci pri usmjeravanju saobraćaja u mreži su:

- rutiranje: (routing): prikupljanje informacija o topologiji i stanju mreže i na osnovu ovih informacija se formira i osvježava tabele rutiranja,
- prosleđivanje (forwarding): definisanje izlaznog porta uređaja za dolazne podatke, na osnovu destinacije prema kojoj su podatci upućeni i informacija dobijenih iz tabele rutiranja,
- komutacija (switching): prenos podataka sa ulaznog na izlazni port na osnovu podataka dobijenih prosleđivanjem.

3.6.1. Vrste komutacije

Razlikujemo sledeće načine komutacije: komutaciju kola, komutacija poruka i komutaciju paketa. Mreže prenose informacione jedinice i za mreže sa komutacijom kola ta informaciona jedinica je poziv (npr, telefonski poziv) dok je kod mreža sa komutacijom paketa to paket, [16].

Istorijski gledano, komutacija kola je najstariji način komutacije koji je razvijen za potrebe javne telefonske mreže i njenu osnovnu uslugu, prenos glasa, dok je komutacija paketa karakteristična za Internet koji je predmet našeg razmatranja tako da ćemo se mnogo više zadržati na ovoj formi komutaciji.

U ovom poglavlju ćemo objasniti osnove komutacije kola i paketa, sa posebnim aspektom na komutaciju paketa, budući da se na njoj zasniva rad Internet.

3.6.1.1. Komutacija poruka

Komutacija poruka koja radi po principu memoriši-pa-proslijedi (store-and-forward). Kod ove vrste komutacije prvi čvor prima cjelokupnu poruku, uspostavlja vezu sa sledećim i šalje mu cjelokupnu poruku, nakon čega se rezervisani link za taj prenos raskida. Drugi čvor uspostavlja vezu sa narednim, rezerviše link za prenos poruke i nakon što je poruku isporučio raskida link. Na ovaj način se čitava poruka prenosi do odredišta. Po ovom principu funkcioniše slanje elektronske pošte (e-mail-a) i SMS (Short Message Service) poruka kod mobilnih mreža. Ovdje ovaj vid komutacije nećemo posebno razmatrati, [16].

3.6.1.2. Komutacija kola

Između krajnjih tačaka veze (terminala A i B na Sl.3.12) se uspostavlja rezervisana putanja koja se naziva kolo, kanal (circuit), pa se ova komutacija po tome i naziva komutacija kola (kanala). Kolo je na raspolaganju korisnika za svo vrijeme prenosa govora, odnosno podataka (na ovom principu funkcionišu dial-up modemi).

Komutacija kola se odvija u koracima: uspostava kola, prenos korisničkog saobraćaja i raskidanje kola (koje može inicirati bilo koja strana u komunikaciji), [52].

Uspostava veze se odvija na sledeći način:

Prva faza: faza uspostavljanja kola

- čvor A želi da uspostavi komunikaciju sa čvorem B i šalje zahtjev čvoru 1 na koji je vezan
- čvor 1 prihvata zahtjev i donosi odluku prema kojem čvoru dalje da usmjeri saobraćaj (statičko ili dinamičko rutiranje) i neka je to čvor 2, zauzima link ka čvoru 2
- čvor 2 prihvata zahtjev i donosi odluku da usmjeri saobraćaj ka čvoru 3, zauzima link

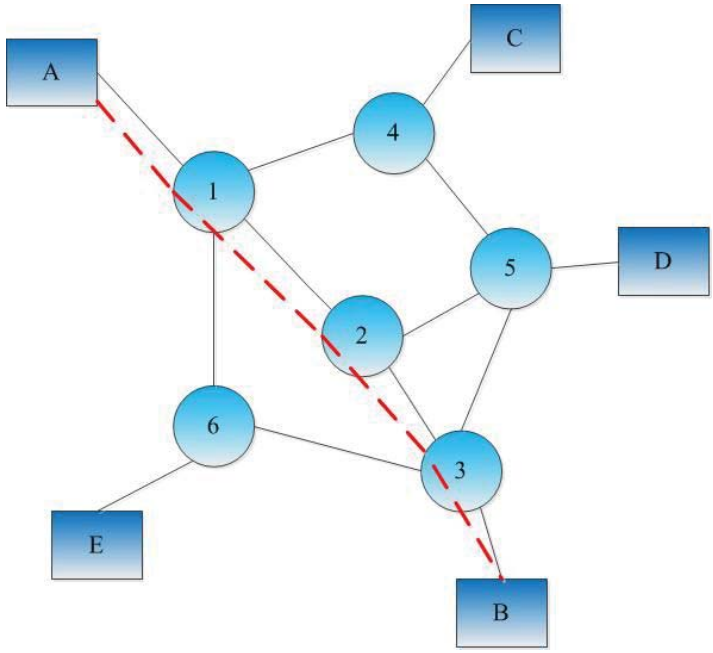
- čvor 3 prihvata zahtjev, zauzima link, pronalazi čvor B, provjerava da li je on slobodan za uspostavu komunikacije i prosleđuje mu zahtjev za uspostavu komunikacije od čvora A, a ako jeste rezerviše link, čime je završeno rezervisanje linka od čvora A do čvora B.

Druga faza: prenos korisničkog saobraćaja

- vrši se prenos ramova, u okviru kojeg se nalazi i vremenski slot (kanal) dodijeljen za komunikaciju između čvora A i čvora B.

Treća faza:raskidanje kola

- zahtjev za raskidanjem kola može da uputi bilo koja strana u komunikaciji (čvor A ili B), on se prosleđuje kroz sve čvorove i vrši se oslobađanje linkova (delociranje resursa), recimo ako je zahtjev za raskidanje veze podnio korisnik A, zahtjev se prosleđuje kroz čvorove 1, 2 i 3 i redom oslobađaju zauzeti linkovi.



Slika 3.12: *Komutacija kola*

Dobra osobina komutacije kola jeste malo i konstantno kašnjenje sa kraja na kraj veze dok su mane loša iskorištenost prenosnih linkova i nepostojanje zaštite od grešaka u toku prenosa, periodi tišine.

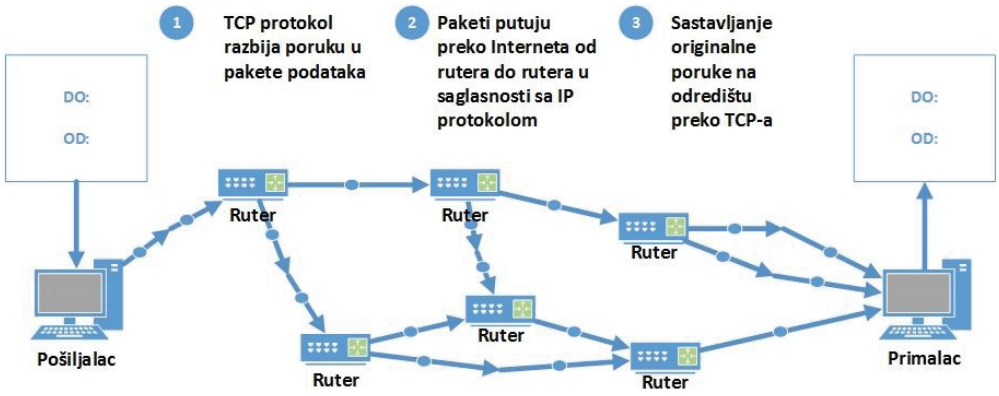
3.6.1.3. Komutacija paketa

Komutacija paketa je razvijena za potrebe računarskih mreža. Dvije osnovne tehnike komutacije paketa su: virtuelno kolo i datagram, [16], [52].

Virtuelno kolo većinom kreiraju administratori mreže. Dosta je slično komutaciji kola, jer se paketi šalju preko definisane putanje od izvora do odredišta čime se može postići malo kašnjenje pri prenosu kroz mrežu i zadovoljavajući nivo servisa i za takve servise kao što je prenos govora, kod koga veliko, ali i promjenjivo kašnjenje može značiti veliku degradaciju prenošenog govora i njegovu nerazumljivost.

Komutacija paketa je danas u osnovi svih modernih mreža za prenos podataka, kakva je Internet, X.25 mreža, frame relay...

Tehnikom komutacije paketa, poruka na predaji se izdijeli u pakete fiksne dužine, kojima se doda kontrolna informacija, pa se potom ti paketi prenose kroz brojne posredničke uređaje (rutere) do odredišta (moguće je i po različitim putevima), po najefikasnijoj putanji koja je na raspolaganju u tom trenutku.



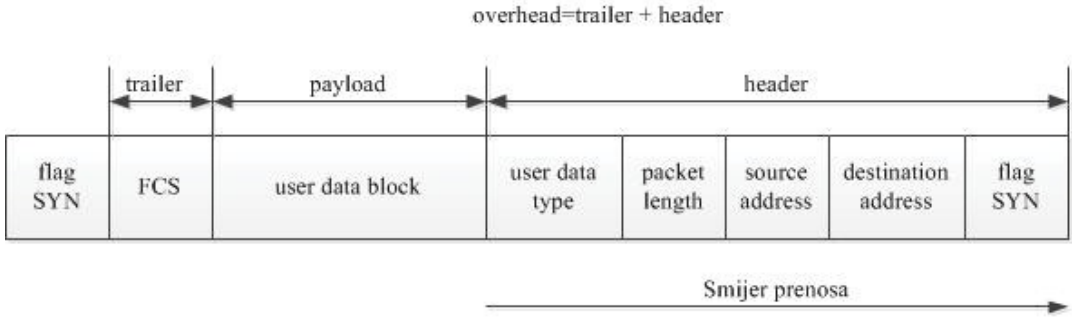
Slika 3.13: *Komutacija paketa*

Paketi se rutiraju do odredišta u saglasnosti sa potrebnim kvalitetom komunikacije između dvije krajnje tačke, trenutnim uslovima u mreži, po najkraćem putu i sl. Paketska komutacija daje bolju pouzdanost pri komunikaciji sa kraja na kraj mreže, jer greške nastale u toku same konekcije mogu biti prevaziđene, recimo rutiranjem saobraćaja po drugom putu.

Def.: Paket *predstavlja metod grupisanja bita i sastoji se od zaglavlja (header) koje uključuje više bita koji nose informaciju o adresi, tipu paketa i kontroli greški i korisnog dijela, sadržaja (payload) koji nosi korisničke podatke.*

Upotrebom statističkog multipleksiranja može se postići i bolja iskoristivost mrežnih resursa.

Tipični format paketa podataka je prikazan na Sl.3.14.



Slika 3.14: *Format paketa podataka*

Značenje pojedinih polja paketa:

- flag SYN (sinhronizaciona sekvenca): služi za sinhronizaciju i za razdvajanje jednog paketa od drugog,
- FCS (Frame Check Sequence): služi za kontrolu greške,
- user data block (blok korisničkih podataka): korisnički podaci, sadržaj (payload),
- user data type (tip korisničkih podataka): daje informaciju prijemniku, koji tip i format podataka se nalazi u *payload*-u,
- sequence number (broj sekvence): omogućava, da u slučaju da se neke duža poruka na predaji rastavila na više paketa, njihovo korektno spajanje na prijemu,
- packet length (dužina paketa): daje informaciju o dužini paketa
- source address (adresa izvora): adresa pošiljaoca paketa
- destination address (adresa odredišta): adresa primaoca paketa.

3.6.2. Multipleksiranje

Radi efikasnijeg iskorištenja prenosnih kapaciteta između čvorova mreže vrši se multipleksiranje kanala.

Def.: *Multipleksiranje predstavlja postupak prenosa više nezavisnih poruka kroz neki medijum bez interferencije.*

Ovdje ćemo objasniti ukratko objasniti neke od danas najčešće korištenih tipova multipleksiranja

3.6.2.1. Multipleksiranje sa frekvencijskom raspodjelom

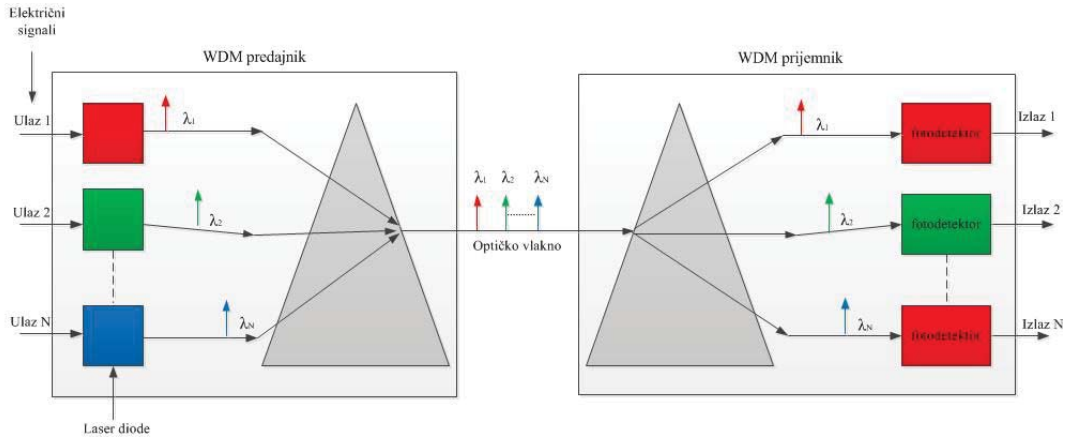
Multipleksiranje sa frekvencijskom raspodjelom (FDM-Frequency Division Multiplexing) kanala se postiže pomoću više signala nosioca. Frekvencije se filtrima razdvajaju da bi se izbjeglo miješanje i interferencija. FDM je vezan većinom za analogne prenosne sisteme ali isti princip se koristi i kod multiplekiranja po talasnim dužinama (WDM-Wavelength Division Multiplex) s tim što se ovdje umjesto slaganja kanala (jedna frekvencija dodijeljena paru ulaz-izlaz) po frekvencijama vrši slaganje kanala po talasnim dužinama (jedna talasna dužina dodijeljena paru ulaz-izlaz). WDM se danas koristi na magistralnim mrežama i predstavlja kičmu infrastrukture svakog provajdera Internet servisa koji pretenduje da pruža servis na nacionalnom nivou.

3.6.2.1.1. Multipleksiranje po talasnim dužinama

Multipleksiranje po talasnim dužinama (WDM) se koristi u optičkim komunikacijama. Primjenom WDM-a znatno je poboljšan prenosni kapacitet optičkog sistema, jer je omogućen istovremeni prenos više talasnih dužina (više kanala) po jednom optičkom vlaknu tako da se otvaraju mogućnosti prenosa brzinama većim od terabita po sekundi. Svaka talasna dužina prenosi svoj informacioni tok, [52].

Postoje dva WDM sistema:

- CWDM (Coarse WDM) vrši multipleksiranje najčešće 8 kanala po vlaknu sa razmakom od 5-50nm,
- DWDM (Dense WDM) vrši multipleksiranje većeg broja kanala, 32, 96 do čak 192 kanala po vlaknu i sa brzinama od 10 Gbit/s po kanalu (talasnoj dužini).



Slika 3.15. *Princip WDM multipleksiranja*

Električni signali modulišu u laserskim diodama optičke signale nosioce, odnosno svjetlosne signale određene talasne dužine i tako nastaje modulisani optički signal. Takav signal koji se nalazi oko jedne talasne dužine se naziva optički kanal.

Nastali optički signali različitih talasnih dužina se usmjeravaju na WDM multiplekser koji koristi optičku prizmu da svjetlosne signale koji dolaze pod određenim uglom kombinuje u jedan koji se potom prostire kroz vlakno do prijemnika gdje WDM demultiplekser opet koristi prizmu da razdvoji talasne dužine.

Signali različitih talasnih dužina se prosleđuju ka fotodetektorima na čijim izlazima se pojavljuje električni signali koji bi, ako nije nastala neka greška u prenosu, trebali biti jednak originalnim signalima na predaji.

Kao optički detektori se koriste PIN (Positive Intrinsic Negative) i APD (Avalanche Photo Diode) diode. Njihova uloga je da pri određenoj optičkoj snazi proizvedu odgovarajuću struju (konverziona sposobnost dioda). APD dioda na prijemu poboljšava ojetljivost prijemnika za 10-15dB u odnosu na PIN diodu.

Vlakno sa Sl. 3.15 mora biti monomodnog tipa.

3.6.2.2. Multipleksiranje sa vremenskom raspodjelom

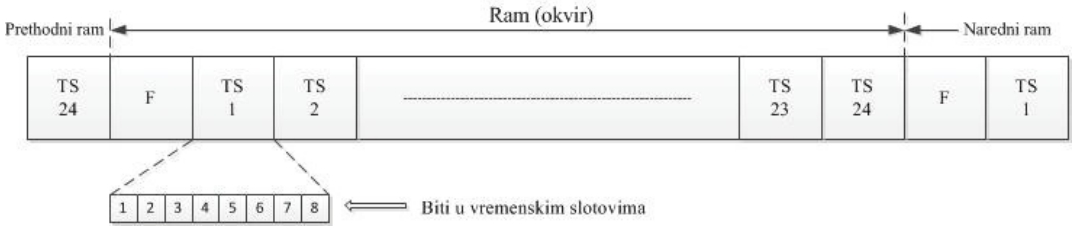
Pri formiranju digitalnih signala postoji asihrono (pleziohrono) multipleksiranje i sinhrono multipleksiranje

3.6.2.2.1. Pleziohrono multipleksiranje sa vremenskom raspodjelom

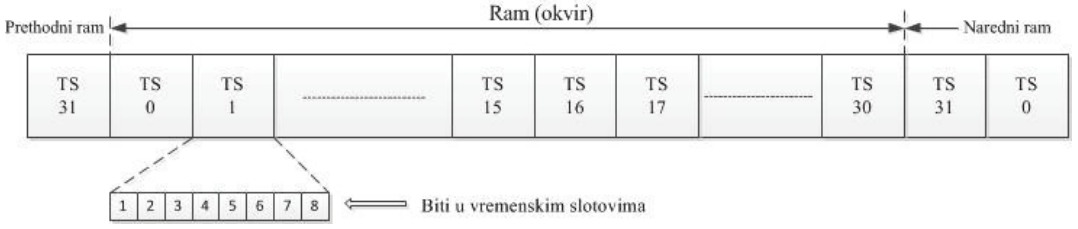
Multipleksiranje sa vremenskom raspodjelom kanala (TDM-Time Division Multiplexing) koristi jedan signal nosioc za istovremeno slanje različitih nizova podataka,

sa osnovnom idejom da se cio sistem u datom trenutku stavi na raspolaganje samo jednom kanalu. Ovaj sistem se koristi kod digitalnih prenosnih sistema.

U upotrebi su američki (Sl.3.16.a) i evropski standard (Sl.16.b) multipleksiranja.



(a)



(b)

Slika 3.16: *Američki (a) i evropski (b) standard multipleksiranja*

U evropskom standardu se koristi 30 kanala (vremenskih slotova) za prenos govornog saobraćaja, 0-ti za sinhronizaciju i 16-ti za signalizaciju, odnosno ukupno 32 kanala što daje tzv E1 signal od 2.048 Mbit/s.

Kod američkog standarda se koristi 24 kanala za formiranje okvira.

Kod ranije korištene pleziohrone digitalne hijerarhije (PDH-Plesiochronous Digital Hierarchy) definisani su dodatni nivoi multipleksiranja i multiplesiranje se obavljalo isključivo između susjednih nivoa, kako je to prikazano na Sl.3.17.

Sa Sl.3.17 se vidi i veliki nedostatak PDH hijerarhije a to je nemogućnost identifikacije pojedinačnih kanala ili signala manjih protoka iz viših hijerarhijskih digitalnih signala. Nedostatak je postojanje i različitih PDH hijerarhija (evropska i američka), pa samim tim nastaju i problemi pri komunikaciji opreme različitih proizvođača.

Slika 3.17: *PDH hijerarhija multipleksiranja.*

TDM je efikasan za prenos informacionih tokova stalne brzine, kakvi su govor i video, ali je neefikasan za prenos informacionih tokova čija brzina varira i tada se raspoloživi kapacitet TDM sistema neefikasno koristi.

3.6.2.2.2 Sinhrono multipleksiranje

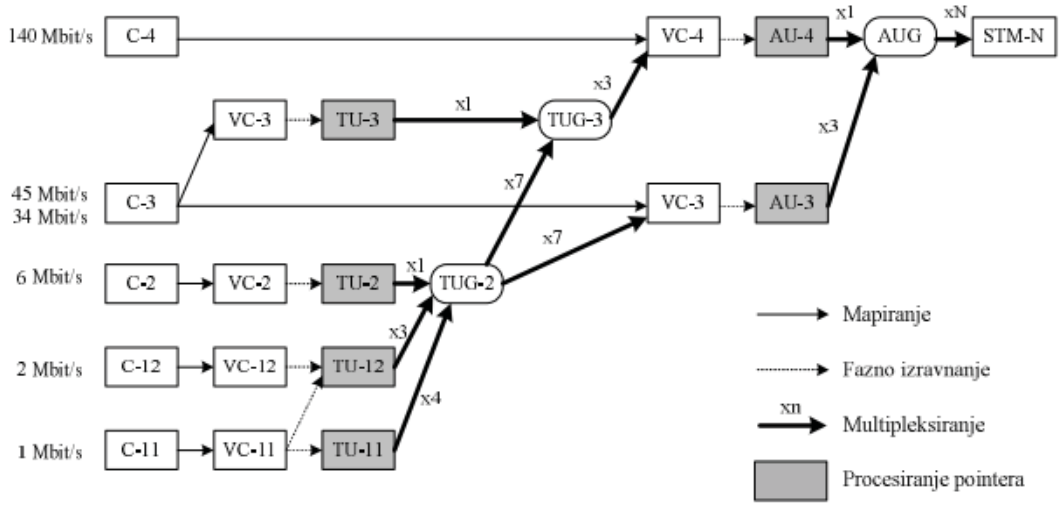
Da bi uklonili neki od ranije spomenutih nedostataka PDH tehnologije uvedena je sinhrona digitalna hijerarhija (SDH-Synchronous Digital Hiearchy) koja je obezbijedila kompatibilnost i sa PDH hijerarhijom i američkom hijerarhijom sinhronog multipleksiranja (SONET-Synchronous Optical Network), [52].

Osnovni protok u SDH hijerarhiji je 155 520 kbit/s (STM1-Synchronous Transport Module 1).

Veći protoci se dobijaju kao cjelobrojni umnožak osnovnog protoka STM-1, tako da je STM4=4STM1; STM16=16STM1; STM64=64STM1.

Ne ulazeći previše u detalje, reći ćemo da se radi ostvarivanja kompatibilnosti sa PDH hijerarhijom korisni signal iz PDH hijerarhije smiješta (mapira) u odgovarajući kontejner (C-Container), nakon dodavanja servisnog dijela, POH (Path Over Head) dobija se odgovarajući VC (Virtual Container) u procesu faznog izravnjavanja nakon čega slijedi multipleksiranje, kako je to prikazano na Sl.3.18.

Suština SDH multipleksiranja zasniva se dakle na tri procedure: mapiranje pritočnog signala u kontejner, fazno izravnavanje dodavanjem pointera i multipleksiranje.



Slika 3.18: *SDH hijerarhija multipleksiranja*

3.6.2.3. Statističko multipleksiranje

Paketska komutacija počiva na statističkom multipleksiranju. Da bismo shvatili suštinu statističkog multipleksiranja napravit ćemo analogiju sa telefonskim razgovorom.

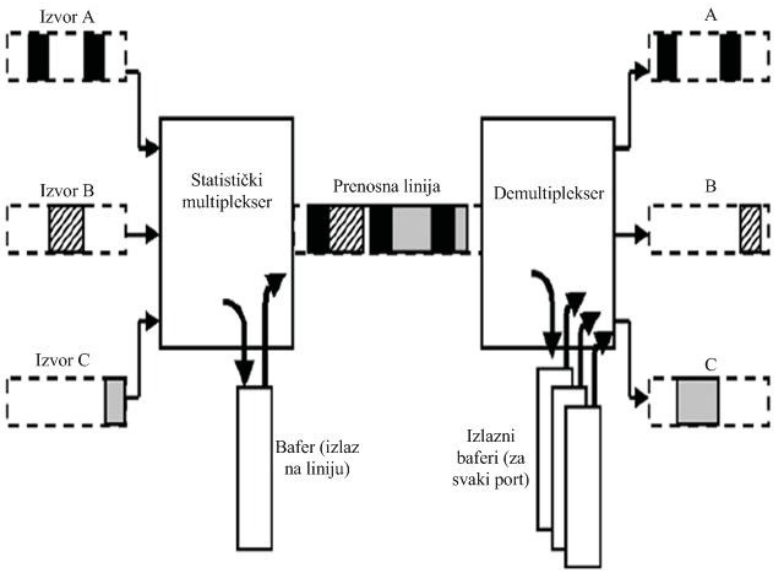
Recimo da želimo primijeniti tehniku statističkog multipleksiranja na dva telefonska razgovora. U pauzama u jednom razgovoru (periodima tišine) umećemo riječi drugog razgovora. Na ovom principu se prenose i paketi podataka, [27], [52].

Statističko multipleksiranje se zasniva na dvije činjenice:

- uređaji spojeni na ulaz multipleksera ne šalju konstantno svoje podatke,
- rijetko se desi da svi uređaji spojeni na ulaz multipleksera istovremeno šalju svoje podatke.

Statističkim multipleksiranjem se može povećati iskoristivost mrežnih resursa izbjegavanjem prenošenja redudantnih informacija (recimo perioda tišine). Resursi se korisniku dodjeljuju na zahtjev, zavisno o količini podataka koji se generišu.

Princip statističkog multipleksiranja je prikazan na Sl.3.19. Tri nezavisna izvora vrše prenos podataka preko iste prenosne linije, dijeleći resurse uz pomoć statističkog multiplekiranja. Statistički multiplekser šalje šta god da primi na svom ulazu direktno na izlaz. U slučaju da recimo prvi izvor želi da otpočne slanje podataka, a da neki od ostala dva izvora već vrši slanje podataka, prvi izvor će vršiti baferovanje podataka . Kad se linija oslobodi, bafer se prazni šaljući dotad baferovane podatke na liniju. Zašto se onda ovo naziva statističkim multipleksiranjem? Postoji mala statistička vjerovatnoća da sva tri izvora žele da istovremeno šalju podatke, ako se to ipak nekad desi tu je bafer koji treba da spriječi kolizije.



Slika 3.19: *Princip statističkog multipleksiranja*

U slučaju da se bafer prepuni, može doći do odbacivanja izvjesne količine podataka iz njega što opet ne mora da ima katastrofalne posljedice, jer postoje protokoli koji vrše prioritetizaciju podataka, tako da će se prvo odbaciti manje značajni podaci. Postoje takođe i protokoli koji će zahtijevati retransmisiju izgubljenih podataka od izvora iz kojeg oni potiču. Da bi se spriječilo zagušenje linijska brzina prenosa podataka mora biti veća od sume brzina svih pojedinačnih izvora.

Zagušenje u mrežama sa komutacijom kola (uzmimo kao primjer telefonsku mrežu) se manifestuje odbacivanjem novih poziva. Novi korisnik će dobiti u slušalici ton zauzeća što bi mu trebalo da ukaže da je mreža zauzeta i da proba kasnije. U slučaju zagušenja kod paketskih mreža sa statističkim multipleksiranjem, zagušenje se manifestuje povećanjem propagacionog kašnjenja zbog baferovanja podataka. Ovo kašnjenje se odražava na sve korisnike i kao posljedicu ima sporije izvršavanje servisa, ali se nove konekcije ne odbacuju.

3.6.3. Simetrična i asimetrična komunikacija

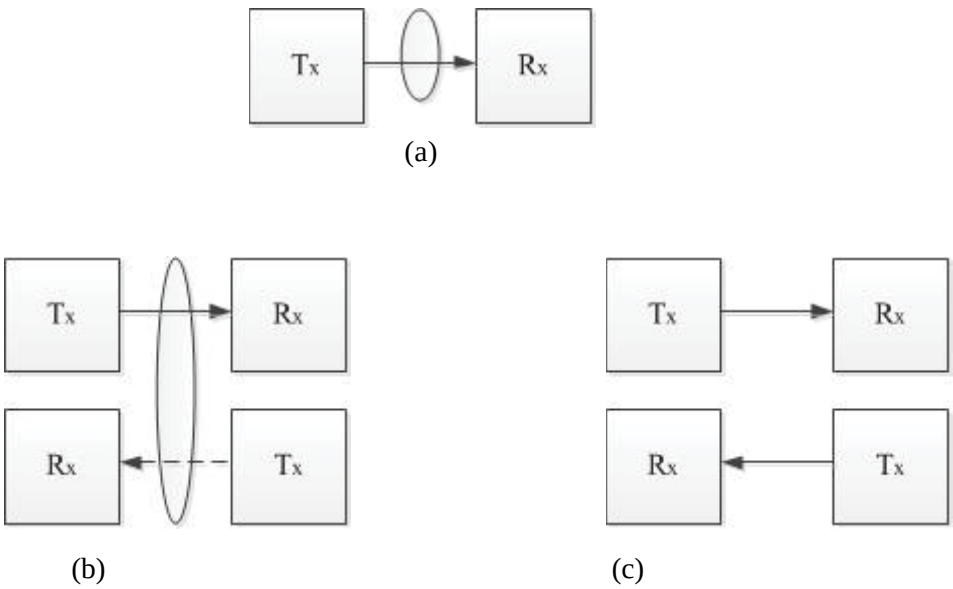
Prvo ćemo se upoznati sa komunikacijama tipa simpleks, poludupleks i puni-dupleks, [52].

Simpleks sistem se sastoji od jednog predajnika, jednog prenosnog medijuma i jednog prijemnika, kako je to prikazano na Sl.3.20.a. Simpleks komunikacija je jednosmijerna.

Poludupleksna komunikacija omogućava dvosmijernu komunikaciju između dvije strane od kojih samo jedna u datom trenutku može pričati ili slati podatke. Poludupleksni sistem

ima dva predajnika i dva prijemnik i jedan prenosni medijum, Sl.3.20.b. Kao primjer ove vrste komunikacije navest ćemo voki-toki komunikaciju.

Većina modernih komunikacija je tipa puni dupleks (Sl.3.20.c). Ova vrsta komunikacije omogućava dvosmijernu komunikaciju bez ograničenja, što znači da obje strane mogu pričati ili slati podatke u isto vrijeme pri čemu se koriste dva komunikaciona medijuma za svaki smijer (ili recimo četvorožični rad i jedna parica za prijem a druga za predaju) ili jedan, ali na taj način da su odvojeni prijem i predaja.



Slika 3.20: (a) *Simpleks, (b) poludupleks, (c) dupleks komunikacija*

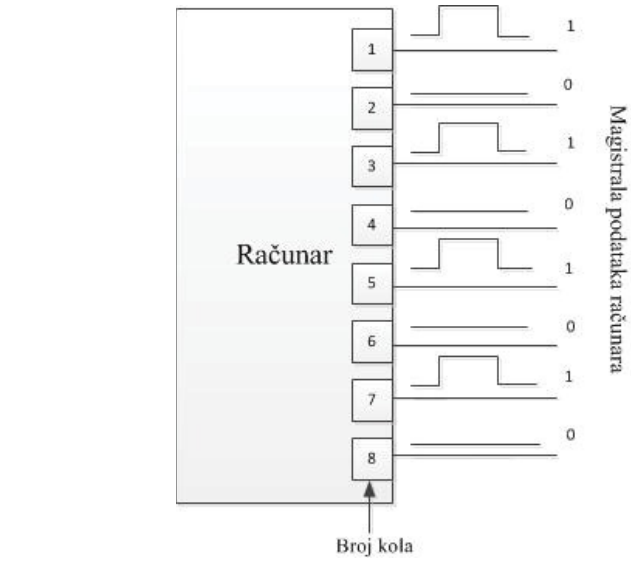
Iako sam komunikacioni link dozvoljava potpuno dupleksni prenos, ne mora značiti da se u oba smijera prenosi isti iznos podataka.

Kad je iznos podataka koji se prenosi u oba smijera približno jednak, radi se o simetričnoj komunikaciji, no ako je različit u tom slučaju se radi o asimetričnoj komunikaciji. Većina Internet korisnika više podataka preuzme s mreže nego što ih pošalje, pa je to uslovilo razvoj asimetričnih tehnologija u pristupnoj mreži (kakva je ADSL o čemu ćemo više reći u nastavku).

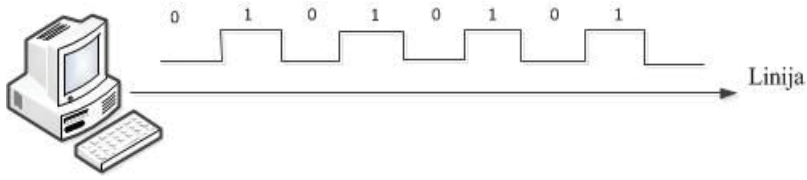
3.6.4. Serijski i paralelni prenos podataka

Svi komunikacioni linkovi i interfejsi su dizajnirani ili za serijski ili za paralelni prenos podataka.

Kako se vidi sa Sl. 3.21, paralelni prenos zahtijeva osam kola od kojih svako prenosi jedan bit informacija u odnosu na serijski koje zahtijeva samo jedno kolo. Paralelni prenos je brži ali i skuplji i koristi se samo za prenos podataka preko sistemske magistrale i na kraće udaljenosti (recimo komunikacija računar-štampač). Serijski prenos koristi samo jedno kolo, jeftiniji je, bolje standardizovan u odnosu na paralelni i koristi se za prenos podataka na veće udaljenosti, [52].



(a)



(b)

Slika 3.21: (a) P*aralelni, (b) serijski prenos podataka*

Neophodno je izvršiti paralelno-serijsku konverziju na predaji, odnosno, serijsko-paralelnu na prijemu.

POGLAVLJE 4

Računarske mreže

Za Internet smo u uvodnom poglavlju rekli da predstavlja globalnu računarsku mrežu sastavljenu od miliona drugih računarskih mreža. U ovom poglavlju će biti objašnjeno šta u suštini predstavlja računarska mreža, čemu je namijenjena, dat će se osnovne podjele računarskih mreža. Bit će predstavljeni i neki od osnovnih elemenata za povezivanje računarskih mreža, dakle, dat će se osnove umrežavanja.

4.1. Definicija i osnovni pojmovi iz računarskih mreža

Porast popularnosti Interneta doveo je do porasta broja korisnika računara i računarskih mreža. Internet smo ranije definisali kao globalnu računarsku mrežu. Ali šta predstavlja sama računarska mreža i kakva je njena osnovna namjena?

***Def**.: Računarska mreža predstavlja sistem povezanih komunikacionih uređaja (računara, perifernih uređaja, npr štampača) čime je omogućeno zajedničko korištenje resursa mreže, a samim tim i značajno smanjenje troškova.*

***Def**.: Računarska mreža je telekomunikacioni sistem za prenos podataka koju čini grupa međusobno povezanih komunikacionih uređaja koji treba da obezbijede prenos podataka od izvora (predajnika) do odredišta (prijemnika) posredstvom komunikacionog medijuma, uz zadovoljenje odgovarajućih komunikacionih protokola.*

***Def**.: Mrežni medijum (komunikacioni medijum) povezuje računar sa drugim računarom ili nekim uređajem koji se priključuje na računar. Mrežni medijumi su npr.upredena parica, koaksijalni kabl, optički kabl, bezžični,satelitski link …*

***Def**.: Mrežni resursi su hardverske i softverske komponente koje mogu koristiti (dijeliti) razni korisnici mreže.*

***Def**.: Uređaji su hardverske komponete koje se koriste u mreži. Za mrežu su posebno značajni komunikacioni uređaji (modemi, mrežne kartice,…).*

Def.: Mrežni protokol jeste skup pravila (procedura) za obavljanje komunikacije preko mreže.

Namjena računarskih mreža je višestruka:

- one omogućavaju zajedničko dijeljenje hardvera i softvera od strane više korisnika,
- zajedničko korištenje podataka,
- razmjenu podataka i komunikaciju među korisnicima,
- zajednički rad više korisnika na jednom problemu.

Da bi računar mogao da razmjenjuje podatke sa drugim računarom (ili nekakvim uređajem) moraju postojati:

- komunikacioni (mrežni) medijum,
- komunikacioni uređaj,
- komunikacioni softver.

Od komunikacionog medijuma zavisi brzina prenosa podataka (brzina prenosa mjeri se brojem prenijetih bitova u sekundi bps, odnosno većim jedinicama Kbps i Mbps).

Komunikacioni uređaj se povezuje na komunikacioni medijum. On podatke sačuvane u memoriji računara pretvara u oblik pogodan za prenos kroz mrežu.

Komunikacioni softver čine programi koji obezbeđuju komunikaciju. Razlikujemo drajvere i aplikativne programe.

4.1.1. Komunikacioni medijum

Većina današnjih mreža mreža koristi kao komunikacioni medijum [42], tri osnovne vrste kablova:

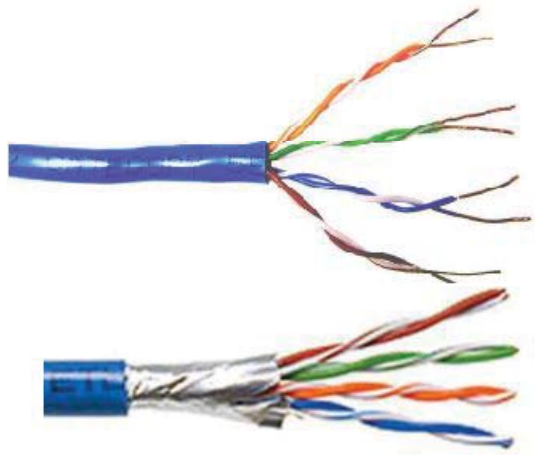
- kablove sa upredenim paricama
- koaksijalne kablove
- optičke kablove

4.1.1.1. Kablovi sa upredenim paricama

Kablovi sa upredenim paricama sastoje se od izolovanih bakarnih žica koje su obavijene, upredene, jedna oko druge. Upredanjem se postiže smanjenje preslušavanja (crosstalk) koje potiče od susjednih parica u istom kablu, kao i od vanjskih izvora, [42].

Dva osnovna tipa ovih kablova su:

- kablovi sa neoklopljenim paricama (UTP-Unshielded Twisted Pair).
- kablovi sa oklopljenim paricama (STP-Shielded Twisted Pair)



Slika 4.1: *(a) UTP i (b) STP kabl*

U oba slučaja, kabl se sastoji od osam žica, koje su upredene u četiri parice. Razlika je u oblasti primjene. UTP kablovi se koriste za unutrašnju (indoor) instalaciju, dok se STP kablovi koriste za vanjsku (outdoor) instalaciju, budući da STP kabl ima mnogo otporniji spoljašnji omotač, a i same parice su mnogo bolje zaštićene dodatnom metalnom folijom čime se smanjuje preslušavanje i povećava raspoloživi propusni opseg parica. Međutim, STP kablovi su značajno skuplji, a ispitivanjem nije utvrđeno da je taj trošak opravdan jer postignuta poboljšanja nisu toliko velika da bi se opravdala ta investicija, tako da se danas, ipak mnogo više koriste UTP kablovi.

I kod UTP i kod STP kabla koriste se samo dvije parice, jedna za predaju, a jedna za prijem podataka.

Zavisno od kvaliteta i načina izrade razlikuju se sledeće kategorije UTP kablova (Tabela 4.1).

Tabela 4.1: *Kategorije UTP kabliranja*

Kategorija UTP kabla	Protok
CAT1	Do 100 kbit/
CAT2	Do 4 Mbit/s
CAT3	Do 20 Mbit/s
CAT4	Do 54 Mbit/s
CAT5 **CAT5e**	Do 100 Mbit/s Do 1000 Mbit/s
CAT6 **CAT6a**	Do 1000 Mbit/s Do 10 Gbit/s
CAT7 **CAT7a**	Do 10 Gbit/s Do 100 Gbit/s

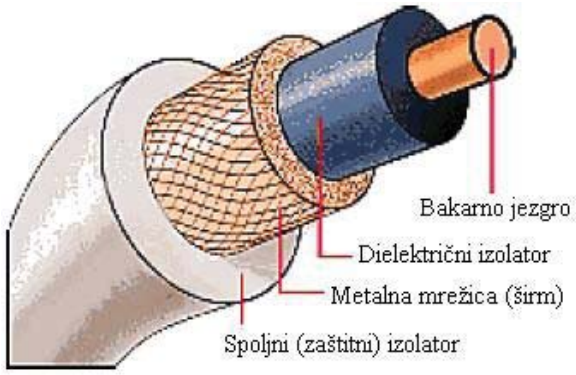
4.1.1.2. Koaksijalni kablovi

Koaksijalni kabl se sastoji od bakarnog jezgra kroz koje se prenosi signal. Jezgro je okruženo punom ili pletenom metalnom uzemljenom presvlakom i sve je obmotano plastičnim omotačem. U odnosu na upredenu paricu može da prenosi mnogo više podataka i manje je osetljiv na električne smetnje, ali je i znatno skuplji i teži za rad.

Tabela 4.2: *Kategorije koaksijalnih kablova*

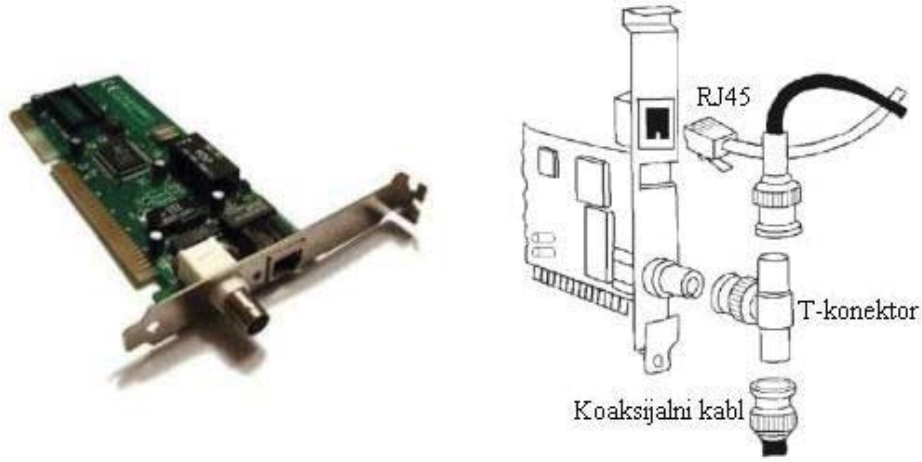
Kategorija koaksijalnog kabla	Prečnik kabla	Impedansa	Podržani protokli
RG58, 10Base2	0,2 inča	50Ω	Tanki (thin) Ethernet
RG8, 10 Base5	0,4 inča	50Ω	Debeli (thick) Ethernet

U računarskim mrežama se koriste najčešće dva tipa koaksijalnih kablova kako je to prikazano u Tabeli 4.2.



Slika 4.2: *Koaksijalni kabl (za debeli „thick“ Ethernet)*

Oznake 10Base2 i 10Base5 ukazuju na to da su ovi kablovi namijenjeni za prenos podataka brzinama od 10 Mbit/s na udaljenosti od 200, odnosno 500 metara. Ovi kablovi se koriste i dalje za kablovsku televiziju, ali zbog malih brzina prenosa podataka, sve se rjeđe koriste za mrežni prenos podataka.

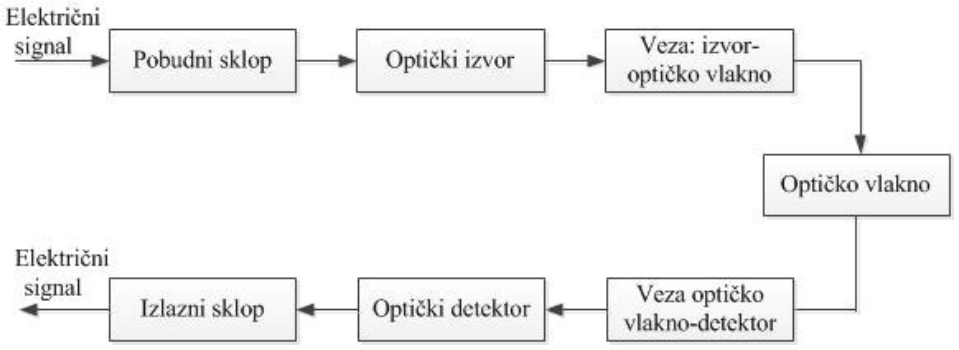


Slika 4.3: *Povezivanje mrežne kartice*

Za povezivanje sa mrežnom interfejsnom karticom (NIC-Network Interface Card) koristi se BNC tip konektora, ako se koristi koaksijalni kabl (10Base2), ili RJ45 ukoliko se koristi UTP kabl (Sl.4.3)

4.1.1.3. Optički kablovi

Na Sl.4.4 su prikazane komponente jedne optičke komunikacione mreže.



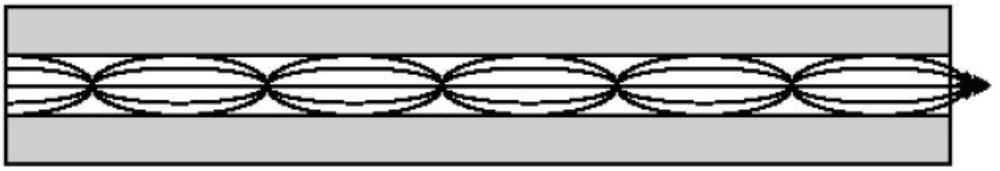
Slika 4.4: *Komponente optičke komunikacione mreže*

Optički predajnik (LED ili laser dioda) pretvara električni signal u svjetlosni signal. Prenosni medij je optičko vlakno (multimodno ili monomodno) i ono prenosi svjetlosni signal u koga su utisnuti podaci. Na prijemu PIN ili APD dioda svjetlosni signal ponovo prevode u električni.

LED dioda se kao izvor svjetlosti koristi kod multimodnih vlakana za prenos velikom brzinom na kratka rastojanja.

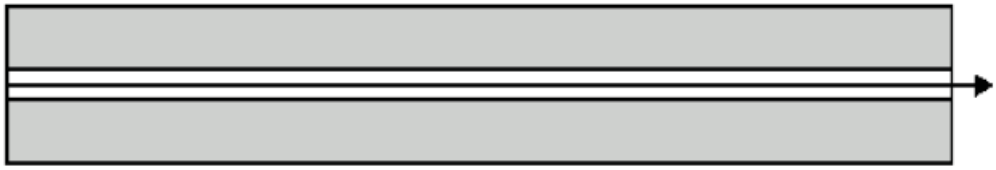
Slika 4.5: M*ultimodna vlakna sa skokovitim indeksom prelamanja*

Na Sl.4.5 je prikazano multimodno vlakno sa skokovitim indeksom prelamanja (step-index) za sisteme sa malim rastojanjima i malim zahtjevima za propusnim opsegom.



Slika 4.6: M*ultimodna vlakno sa gradijentnim indeksom prelamanja*

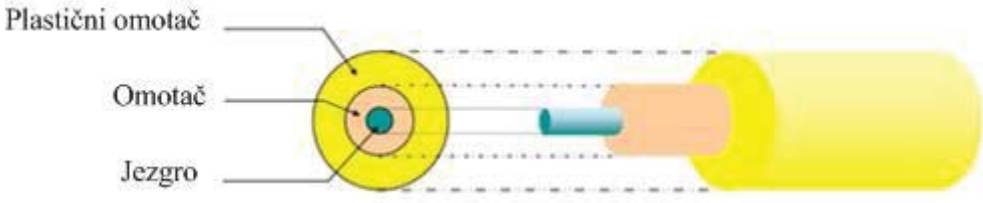
Na Sl.4.6 je dato multimodno vlakno sa gradijentnim indeksom prelamanja (graded index) za srednje udaljenosti i sa srednjim zahtjevima za propusnim opsegom



Slika 4.7: *Monomodno optičko vlakno*

Laser dioda (Sl.4.7) se koristi kod monomodnih vlakana, za prenos na duža rastojanja i tamo gdje su zahtjevi za propusnim opsegom veliki.

Optička vlakna se opisuju preko nekoliko fizičkih karakteristika koje su predstavljene na Sl. 4.8.



Slika 4.8: *Izgled optičkog vlakna*

Jezgro je izgrađeno od stakla na bazi silicijum dioksida, kvarcnog stakla, SiO2, (za prenos na veće udaljenosti) ili plastike (za manje udaljenosti, ali jeftinije). Kvarcno staklo se dopira materijalima poput, oksida germanijuma (GeO2), fosfora (P2O5) i bora (B2O3). SiO2 se koristi kao omotač, a SiO2 sa dodacima GeO2 ili P2O5 kao jezgro optičkog vlakna.

Većina optičkih vlakana pored primarne zaštite, koja se nanosi još u proizvodnji vlakna, ima i tzv. sekundarnu zaštitu od visoko otpornog plastičnog materijala visokog modula elastičnosti, koja im daje dodatnu čvrstoću i mehanički ih izoluje.

4.1.2. Komunikacioni uređaj

4.1.2.1. Mrežna kartica

Mrežna kartica predstavlja vezu između mrežnog ožičenja i računara. Instalira se na jedan od slobodnih portova na matičnoj ploči. Izgled mrežne kartice je dat na Sl.4.3.

Osnovne funkcije mrežne kartice:

- prenos podataka iz operativne memorije računara do mrežne kartice u slučaju slanja i obrnuto u slučaju prijema poruka,
- baferovanje čime se premoštava razlika u brzini mreže i brzine kojom računari obrađuju podatke,
- podjela poruke na okvire (frame): okvir kod Ethernet mreže je veličine od oko 1500 bajta,
- prisup mediju: mrežna kartica u slučaju Etherneta provjerava da li postoji saobraćaj na liniji, a u slučaju Token Ringa čeka dolazak pripadajućeg tokena,
- pretvaranja iz paralelnog zapisa u serijski (ili obrnuto kod prijema poruke),
- šifrovanje/dešifrovanje podataka koje mrežna kartica primi sa magistrale,
- slanje/prijem signala.

4.1.2.2. Modem

U slučaju da se veza između računarskih sistema ostvaruje putem telefonskih linija moraju se koristiti modemi koji obavljaju pretvaranje analognih signala u digitalne i obratno i prilagođavanje signala prenosnom medijumu kako je to objašnjeno ranije.

4.1.2.3. Razvodni uređaj (hub)

Razvodni uređaj se obično koristi kao centralna tačka u topologiji zvijezde. Funkcioniše na prvom nivou OSI (Open Systems Interconnection) modela (o tome će biti više riječi u narednim poglavljima). Ima najčešće od 6 do 24 portova i kako se najčešće koristi u Ethernet mrežama to su RJ45 konektori na koje se vezuju mrežni čvorovi (računari, serveri), [42].

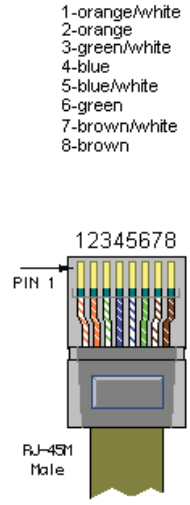
Sve što dođe na bilo koju od fizičkih veza razvodnog uređaja se odmah odašilje na ostale. Služi za povezivanje više segmenata mreže topologije zvijezda u jedan segment.

Za međusobno povezivanje računara i razvodnog uređaja, koristi se ravni kabl (straight), dok se za međusobno povezivanje razvodnih uređaja, koristi unakrsni kabl (crossover).

Na Sl.4.9 je prikazan razvodni uređaj sa 8 portova i izgled RJ45 konektora kod Ethernet kabliranja sa rasporedom boja UTP kabla prilikom pravljenja konektora.

Crossover Cable	
RJ-45 PIN	RJ-45 PIN
1 Rx+	3 Tx+
2 Rc-	6 Tx-
3 Tx+	1 Rc+
6 Tx-	2 Rc-

Straight Through Cable	
RJ-45 PIN	RJ-45 PIN
1 Tx+	1 Rc+
2 Tx-	2 Rc-
3 Rc+	3 Tx+
6 Rc-	6 Tx-



Slika 4.9: *Hub i RJ45 konektor za ravni i unakrsni kabl*

4.1.2.4. Mrežni most (bridge)

Most radi na drugom OSI nivou (nivou voda podataka). Služi za povezivanje LAN-ova. Usmjeravanje saobraćaja se obavlja na osnovu fizičkih (MAC) adresa. Mostovi se koriste u mreži da se smanje kolizije unutar emisionih domena. To se postiže razbijanjem jedne velike mreže na više dijelova koji se kasnije povezuju, ispočetka razvodnim uređajima i mostovima, danas komutatorima (switch) i usmjerivačima (router), a sve sa ciljem smanjenja zagušenja i mogućnosti sudara (kolozija), što će biti jasnije kad se u nastavku objasni princip pristupa medijumu (CSMA/CD), [76].

Def: Emisioni domen (broadcast domen) čine svi uređaji u mrežnom segmentu koji osluškuju sve opšte poruke (broadcast) poslate u taj segment. Opšta (broadcast) poruka jeste poruka koja se šalje svim računarima u mreži (segmentu mreže)

O opštim porukama ćemo više govoriti kad budemo govorili o adresiranju.

4.1.2.5. Komutator (switch)

Često se između mosta i komutatora ne pravi nikakva razlika, pa se često može čuti da je komutator samo most sa više portova i više inteligencije. Dakle, namjena oba uređaja je da se poboljšaju performanse lokalne mreže. Budući da su komutatori uređaji drugog nivoa (L2 nivo) to oni rade sa okvirima i njihov zadatak je njihovo usmjeravanje sa jednog porta na drugi komutirane mreže, [76].

4.1.2.6. Usmjerivač (router)

Usmjerivač, ruter, radi na trećem nivou, mrežnom nivou (L3 nivo) OSI modela. Prema Cisku, četiri osnovne funkcije rutera u mreži su:

- komutacija paketa,
- filtriranje paketa,
- komunikacija između mreža,
- odabiranje putanje.

Kako vidimo, umjesto okvira kao jedinice podataka koji je koristio komutator, usmjerivač koristi ko jedinici podataka paket, [52], [76].

4.1.3. Komunikacioni softver

***Def**: Programi i programski paketi koji određuju ponašanje računara se jednom riječju nazivaju softver.*

Softver se može podijeliti na:

- sistemski softver
  - programi prevodioci (asembleri i kompajleri): vrše prevođenje simboličkog jezika u mašinski,
  - veznici (drajveri): vrše povezivanje operativnih sistema sa hardverskim komponentama i omogućavaju korištenje raznih perifernih uređaja,
- operativne sisteme: pogonski program računara od koga zavise svi ostali,
- aplikativni softver: programi koji se primjenjuju na rješavanje nekog problema i rješavanje poslova kao što:
  - obrada teksta (Microsoft Word)
  - rad sa tabelama (Microsoft Excel)
  - prezentacije (Microsoft PowerPoint)

4.2. Klasifikacija računarskih mreža

Postoje razne podjele zavisno od kriterijuma koji se koristi [42],[52].

Kao kriterijum može se izabrati:

- površina koju pokriva mreža,
- odnos među čvorovima mreže,
- način povezivanja računara u mreži (topologija mreže),
- način komunikacije računara u mreži (logička organizacija).

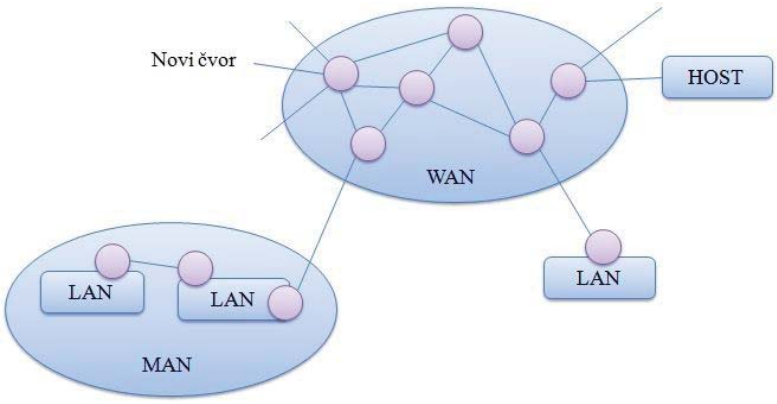
4.2.1. Klasifikacija na osnovu površine koju mreža zauzima

Zavisno od površine koju mreža pokriva , [56], može se izvršiti podjela računarskih mreža na:

- **LAN** (Local Area Network) mreže omogućavaju ostvarivanje veze između komunikacionih uređaja na manjim rastojanjima, do nekoliko kilometara, uz veliku brzinu prenosa podataka (od 10Mbit/s do 10 Gbit/s), uz male gubitke i greške pri prenosu, jednostavno rutiranje podataka i nisku cijenu komuniciranja; vlasnik LAN-a je obično jedna organizacija,
- **MAN** (Metropoliten Area Network) mreža predstavlja verziju LAN-a na gradskom nivou,
- **WAN** (Wide Area Network) mreža povezuje računare koji su geografski razdvojeni; broj računara u mreži može biti i do nekoliko miliona.

Razlike između WAN-a, MAN-a i LAN-a su u tehnologiji i oblastima primjene. Kao parametri poređenja najčešće se koriste:

- geografska veličina,
- broj čvorova,
- brzina prenosa podataka,
- kašnjenje,
- vjerovatnoća greške,
- tehnologija,
- topologija.



Slika 4.10: *Odnos između LAN, MAN i WAN mreža*

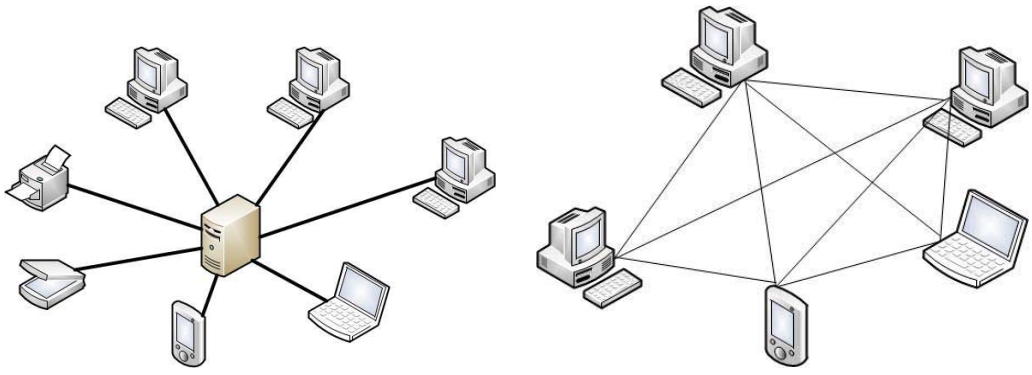
4.2.2. Klasifikacija računarskih mreža na osnovu odnosa između čvorova mreže

Na osnovu odnosa između čvorova mreže razlikujemo dva modela mreža i to:

- klijent/server (client/server)
- ravnopravne mreže (peer-to-peer networks)

U **mrežama tipa klijent/server** postoje računari koji koriste resurse mreže (klijenti) i računari koji raspolažu resursima i stavljaju ih na raspolaganje klijentima (print server, file server,…)

Kod **ravnopravnih mreža** svi čvorovi su međusobno ravnopravni, tj. svaki računar može da služi kao klijent ili server.



(a) (b)

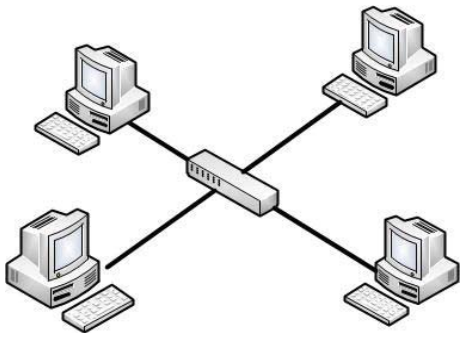
Slika 4.11: (a) *Klijent/server, (b) ravnopravne mreže*

Def: Topologija mreže predstavlja geometrijskog uređenje veza i čvorova u mreži.

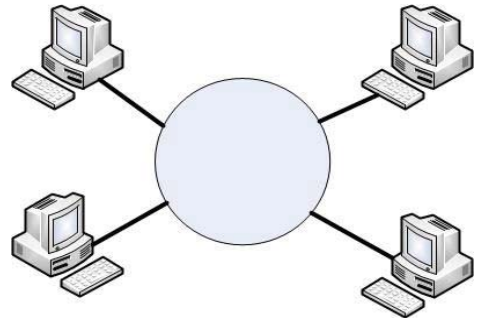
4.2.3. Klasifikacija računarskih mreža na osnovu toplogije

Na osnovu topologije [56], mreže dijelimo na:

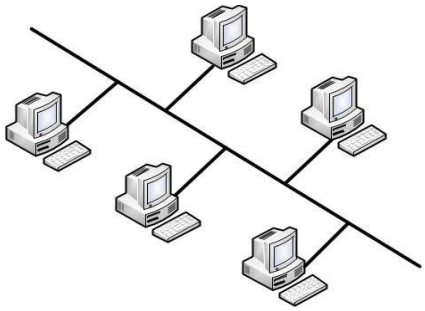
- zvjezdaste
- prstenaste
- magistralne
- hibridne



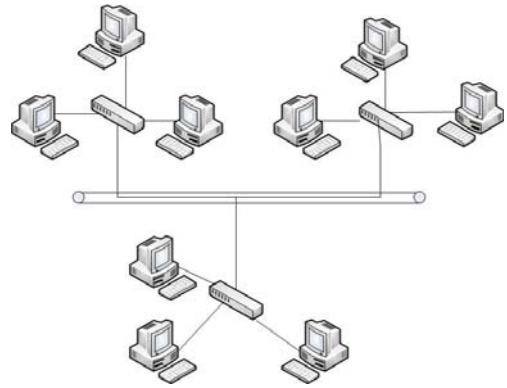
(a)



(b)



(c)



(d)

Slika 4.12: *Podjela mreža prema topologiji (a) zvjezdaste, (b) prstenaste (c) magistralne (d) hibridne*

Ovdje ćemo izvršiti i definisanje čvora i veze.

Def.: Čvor je krajnja tačka neke veze.

Def.: Veza je komunikacioni put između dva čvora.

U **topologiji zvijezde** (Sl.4.12.a) koristi se centralni uređaj za povezivanje, razvodnik (hub) ili koncentrator (switch). Svaki računar je povezan na centralni uređaj zasebnim kablom. Ethernet LAN mreže imaju topologiju zvijezde.

U **topologiji prstena** (Sl.4.12.b) svaki računar je povezan sa svojim susjednim.

Kod **topologije magistrale** (Sl.4.12.c), računari su povezani u jednu liniju, svako sa svojim susjedom. Signali se prenose magistralom u oba smijera.

Hibridna topologija, zvijezda-magistrala (Sl.4.10.d) predstavlja način za proširenje lokalne mreže koja ima toplogiju zvijezde. Centralni uređaji više mreža topologije zvijezda su povezani na zajedničku magistralu.

4.2.3. Klasifikacija računarskih mreža prema načinu komunikacije računara u mreži

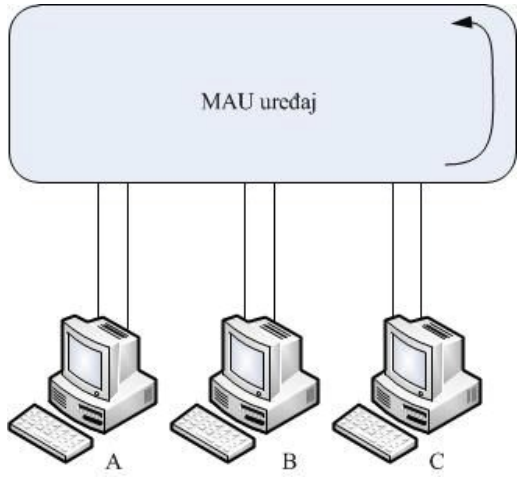
Prema načinu komunikacije računara u mreži razlikujemo dva osnovna tipa; token ring i Ethernet.

4.2.3.1. Token-ring mreža

Token ring mreža je lokalna mreža s topologijom prstena. Ove mreže su nekad bile jako popularne, ali su prevlast nad tržištem preuzela Ethernet mreže. Osnovni nedostatak Token ring mreža jeste niski standardizovani protok do 100 Mbit/s, dok su Ethernet mreže uspjele da standardizuju mnogo veće protoke. Nadalje, cijena implementacije Token-ring mreža je bila mnogo veća nego Ethernet mreža, maksimalni broj stanica u Token ring mreži je ograničen na 250, što su sve razlozi koji su doveli do prevladavanja Ethernet mreža, [42].

Pristupna kontrola medijumu se obavlja preko malog okvira, kontrolnog žetona, tokena koji cirkuliše prstenom sve dok nijedan čvor nema podataka za slanje. Token posjeduje indikator zauzetosti u zaglavlju, polje za podatke, predajnu i prijemnu adresu i kontrolno polje za provjeru da li je došlo do grešaka pri prenosu.

MAU (Multistation Access Unit) uređaj ima ulogu sličnu ulozi hub-a kod Etherneta, kako je to prikazano na Sl.4.13. Njegov zadatak je da generiše token.



Slika 4.13: *Token ring mreža*

Postoje dva pristupa.

- po prvom, mijenja se jadan bit tokena (od ukupno tri bajta kolika je dužina tokena) koji treba da ukaže na to da je medij zauzet jer je jedan čvor spreman da izvrši prenos; token se postavlja na početak okvira i šalje se ka odredištu; kada token dođe do stanice kojoj su podaci namijenjeni, učitava se čitav okvir, a u zaglavlje tokena se upisuje da su podaci preuzeti; kad token stigne do čvora koji je poslao podatke, sadržaj tokena se briše i mijenja bit u zaglavlju koji sada indicira da je token slobodan,
- po drugom, stanica koja treba da izvrši predaju uklanja token sa prstena, pa kad završi prenos generiše novi token.

Dakle, Token ring mreže su eliminisale mogućnost kolizije jer samo onaj čvor koji dođe u posjed tokena može da emituje podatke, [42].

4.2.3.2. Ethernet

Danas je Ethernet najzastupljenija i najraširenija mrežna tehnologija za implementaciju lokalnih računarskih mreža, [76].

Neki od najznačajnijih datuma za razvoj današnjeg Etehrneta su:

- 1983: Organizacija IEEE (Institute of Electrical and Electronic Engineers) je donijela standard 802.3 za lokalne računarske mreže,
- 1992 kompanija Grand Junction Networks je razvila standard Fast Ethernet; ovaj sistem je omogućavao protoke od 100 Mbit/s,
- 1998: IEEE je standardizovao 1 Gbit/s Ethernet,
- 2002: IEEE je standardizovao 10 Gbit/s Ethernet za LAN i WAN (802.3ae).

Ethernet standard sadrži sledeće komponente:

- specifikacija fizičkog sloja: definiše vrstu ožičenja i način signaliziranja,
- format okvira: koriste se dva formata okvira:
  - DIX (Digital Equipment Corporation, Intel and Xerox) format okvira, enkapsulacija po tipu okvira,
  - IEEE 802.3 format okvira, enkapsulacija po dužini okvira,
- mehanizam kontrole pristupa medijumu: višestruki pristup sa osluškivanjem nosioca i detekcijom sukoba, CSMA/CD (Carrier Sense Multiple Access with Collision Detection).

U praktičnoj realizaciji širokopojasnih pristupnih mreža više se koristi enkapsulacija po tipu okvira, iako su obje gore navedene enkapsulacije podržane još od 1997 god.

4.2.3.2.1. Specifikacije fizičkog sloja Etherneta

Osnovne specifikacije vezane za fizički sloj Etherneta su date u Tabeli 4.3.

Kako se može vidjeti iz Tabele 4.3 prvobitna topologija Etherneta je bila topologija magistrale.

Da bi se uklonili osnovni nedostaci topologije magistrale:

- nedostatak pouzdanosti: usljed kvara na magistralnom kablu više uređaja je van rada
- otežano proširenje mreže (usljed nedostatka priključaka na magistralni kabl.

prešlo se na toplogiju zvijezde kod koje se kao centralni uređaj mogu koristiti habovi, svičevi i ruteri o kojima će biti više riječi u nastavku izlaganja.

Tabela 4.3: *Specifikacije fizičkoj sloja Etherneta*

Oznaka	Protok	Topologija	Vrste kabla	Maksimalna dužina segmenta
10Base5	10 Mbit/s	Magistrala	Koaksijalni kabl RG-8	500m
10Base2	10 Mbit/s	Magistrala	Koaksijalni kabl RG-8	185m
10BaseT	10 Mbit/s	Zvijezda	UTP kabl CAT 3	100m
FOIRL	10 Mbit/s	Zvijezda	Višemodno optičko vlakno	1000m
10BaseFL	10 Mbit/s	Zvijezda	Višemodno optičko vlakno	2000m
10BaseFB	10 Mbit/s	Zvijezda	Višemodno optičko vlakno	2000m
10BaseFP	10 Mbit/s	Zvijezda	Višemodno optičko vlakno	500m
100BaseTX	100 Mbit/s	Zvijezda	UTP CAT 5	100m
100BaseT4	100 Mbit/s	Zvijezda	UTP CAT 3	100m
100BaseFX	100 Mbit/s	Zvijezda	Višemodno optičko vlakno	412m poludupleks ili 2000m puni dupleks
1000BaseLX	1000 Mbit/s	Zvijezda	Monomodno optičko vlakno	5000m
1000BaseSX	1000 Mbit/s	Zvijezda	Višemodno optičko vlakno	5000m
1000BaseLH	1000 Mbit/s	Zvijezda	Monomodno optičko vlakno	10km
1000Base ZX	1000 Mbit/s	Zvijezda	Monomodno optičko vlakno	10km
1000BaseT	1000 Mbit/s	Zvijezda	UTP CAT 5(e)	100m

4.2.3.2.2. Ethernet okviri

Na Sl.4.14 datu su osnovni formati Ethernet okvira i to DIX (Ethernet 2) i IEEE 802.3, [76].

(a)

(b)

Slika 4.14: *(a) DIX format okvira, (b) Ethernet IEEE 802.3 format okvira*

Značenje polja:

- Preamble: koristi se prilikom sinhronizacije prijemnika za dolazno okvir; kod DIX formata je dužine 8 bajta kod IEEE 802.3 je dužine 7 bajta koji imaju vrijednost 10101010,
- SOF (Start of Frame): označava početak okvira kod IEEE 802.3 formata i ima vrijednost 11010101, a kod DIX formata okvira to je vrijednost poslednjeg bajta preambule,
- Destination address: 48-bitna MAC adresa odredišta,
- Source adress: 48-bitna MAC adresa izvora,
- Type/Length:
  - Type: podatak o tipu mrežnog protokola čiji se podaci pakuju u korisničko polje DIX okvira,
  - Length: dužina informacionog polja,
- Data: podaci, broj okteta ne smije biti manji od 46,
- PAD: ako je broj okteta polja Data manji od 46 dodaje se dopuna (PAD),
- FCS (Frame Check Sequence): kontrolna sekvenca koja se koristi za detekciju greške pri prenosu.

4.2.3.2.3. Mehanizam kontrole pristupa medijumu

CSMA/CD mehanizam je svojstven topologiji magistrale i poludupleksnom radu Etherneta kod koga se koristi samo jedan par žica. On funkcioniše na sledeći način: kada jedan čvor želi da izvrši prenos okvira preko mreže, on prvo „osluškuje“ mrežu da bi ustanovio da li već postoji prenos. Ako nijedan drugi čvor u tom trenutku ne emituje okvire, počinje prenos. To ne garantuje da neki drugi računar neće u isto vrijeme probati da pristupi mreži što bi tada dovelo do kolizije. U tom slučaju prvi čvor emituje produženi signal zastoja (jam), što će dovesti do toga da svi drugi čvorovi u mreži obustave slanje podataka. Nakon nekog slučajnog intervala vremena obavlja se retransmisija, [76].

Dozvoljeno je najviše 16 retransmisija, nakon čega se okvir odbacuje. Da bi se smanjio broj kolizija Ethernet mreža se dijeli na segmente o čemu će biti još biti govora.

Prelaskom na topologiju zvijezde kod koje se svakom korisniku dodjeljuje njegov segment mreže, te velikom povećanjem protoka kod novijih verzija Etherneta, ukida se

problematika dijeljenog pristupa. Ovdje se koristi dupleksni režim rada te nema zajedničkog prenosnog medijuma, pa samim tim ni mogućnosti kolizije.

Ipak treba napomenuti da se i kod 1Gbit/s Etherneta i isključivo u LAN-u koristi još uvijek poludupleksni režim rada, pa je još uvijek u upotrebi i CSMA/CD.

10 Gbit/s podržava samo dupleksni režim rada i koristi se većinom u WAN mrežama.

I kod 1 Gbit/s i 10 Gbit/s Etherneta, format okvira je isti kao kod već ranije opisanog IEEE 802.3 standarda

POGLAVLJE 5

Referentni modeli i protokoli Interneta

U ovom poglavlju je dat kratak opis OSI referentnog modela. Prikazan je način prenosa podataka kroz pojedine slojeve arhitekture, enkapsulacija. Mnogo detaljnije je objašnjen TCP/IP protokol stek. Dat je kratak pregled najznačajnijii protokoli iz TCP/IP protokol steka.

5.1. Referentni modeli

Da bi se riješili problemi zbog nekompatibilnosti pri komunikaciji oprema različitih proizvođača, uveden su OSI (Open Sytem Interconnection) i TCP/IP (Transmission Control Protocol/Internet Protocol) referentni modeli. Budući da je TCP/IP danas standard za računarske mreže i Internet, to ćemo mnogo detaljnije obraditi ovaj referentni model.

Cisco: „*Referentni model je konceptualna skica koja nam pokazuje kako komunikacija treba da se odvija. Ovaj model predstavlja sve procese potrebne za upješnu komunikaciju i dijeli ove procese u logičke grupe pod nazivom slojevi. Kada se komunikacioni sistem dizajnira na ovaj način, onda se to naziva slojevitom arhitekturom*“, [76].

Svaki od nivoa slojevitog modela koristi usluge nivoa ispod sebe i pruža usluge nivou iznad sebe.

Ovakva podjela na nivoe omogućava:

- precizno opisivanje pojedinih dijelova kompleksnog sistema,
- laku promjenu realizacije svakog od nivoa bez uticaja na ostale nivoe,
- korištenje jednog nivoa od strane više korisnika na višim nivoima,
- kreiranje kompatibilnih mrežnih uređaja i softvera u formi protokola.

Def.: Protokol predstavlja skup pravila koja definišu neke komunikacione funkcije

Def.: Skup protokola jeste familija protokola koji rade zajedno i omogućavaju komunikaciju između aplikacija, odnosno progama.

Def.: Pojedina realizacija skupa protokola se naziva protokol stek.

Najčešće se između pojmova skup protokola i protok steka u literaturi ne pravi nikakva razlika.

Protokol koji treba da poveže različite mreže treba da zadovolji sledeće zahtjeve:

- autonomnost: interno funkcionisanje same mreže se ne smije promijeniti. Takođe mora biti omogućeno povezivanje mreža različitih proizvođača, izvedenih preko različitih medija,
- pouzdanost usluge: poruke izgubljene u prenosu će se ponovo poslati,
- decentralizovana kontrola: ne postoji globalna kontrola nad međusobnim povezivanjem mreža,
- ruteri bez memorije: ruteri nemaju nikakvu informaciju o cijeloj putanji poruke.

5.1.1. OSI referentni model

OSI referentni model nije fizički model. To je apstraktni model, što znači da stvarna implementacija mreže ne mora da ga striktno slijedi, [11], [42], [16], [76].

Osi je sastavljen od sedam slojeva kako je to prikazano na Sl.5.1.

Slika 5.1: *OSI referentni model*

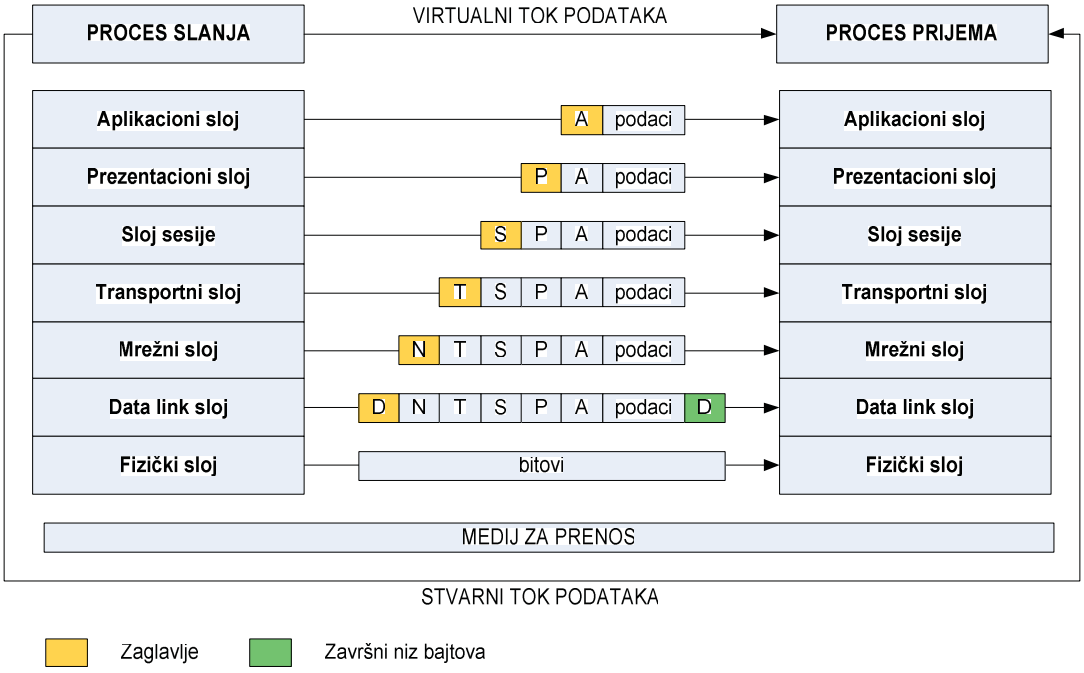
Navest ćemo ukratko funkcije pojedinih slojeva:

- aplikacija: svrha komunikacije (e-mail, prenos datoteka i sl),
- prezentacija: pravila za konverziju podataka (dekompresija podataka i priprema podataka za prenos, odnosno za prijem od strane aplikacije).
- nivo sesije: start, stop i upravlja redoslijedom prenosa,

- transportni nivo: obezbjeđuje isporuku cijele poruke, vrši diobu cijele poruke na blokove i određuje krajnje tačke rutiranja na pojedinim mrežama,
- mrežni: rutiranje podataka između različitih mreža, dioba blokova na okvire,
- nivo voda podataka: prenos podataka od čvora do čvora (upravljanje pristupom mediju, ubacivanje paketa u okvire),
- fizički nivo: prenos bitova duž komunikacionog kanala.

Prilikom slanja podataka od aplikacije sa jednog računara na drugi, podaci se prenose od jednog do drugog nivoa kroz protokol stek.

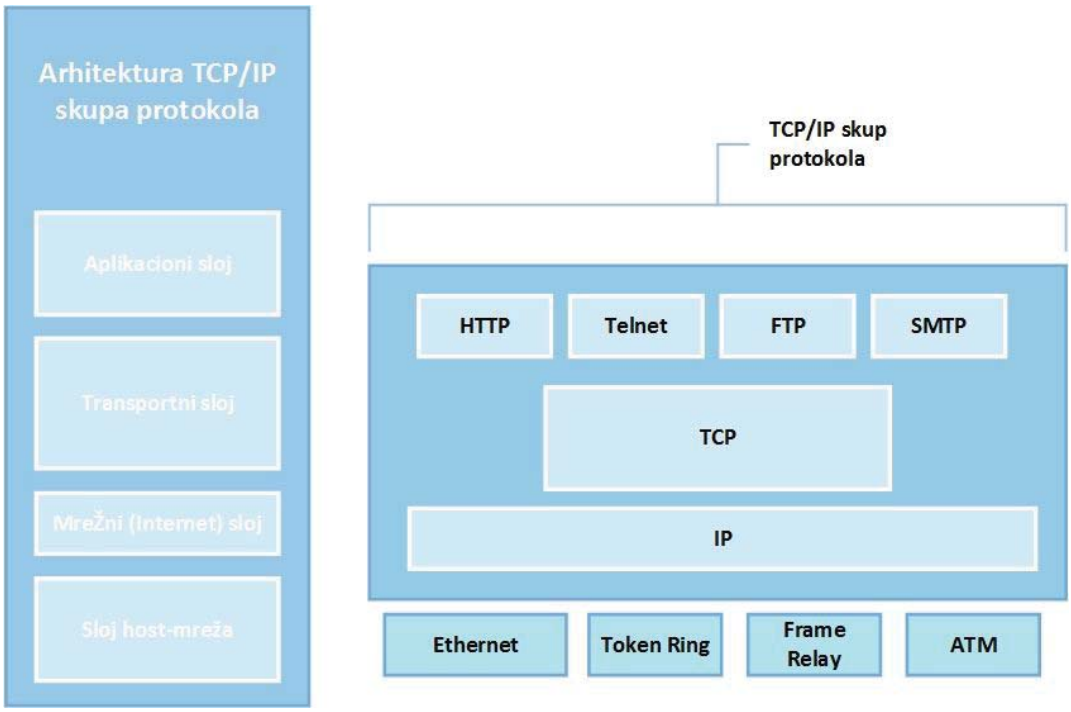
Podaci silaze niz sve slojeve OSI referentnog modela, dok ne stignu na najniži, kad se šalju kroz mrežu. Pri ovom prolazu, svaki od slojeva dodaje svoje zaglavlje (header) na podatke koje primi od višeg nivoa. U zaglavlju se nalaze informacije koje su bitne za dati sloj referentnog modela.



Slika 5.2: *Proces enkapsulacije*

5.1.2.TCP/IP skup protokola

TCP/IP referentni model ili Internet referentni model je napravljen od strane Internet Architecture Board (IAB) i on je danas standard za računarske mreže i Internet, [16],[55].



Slika 5.3:*TCP/IP skup protokola*

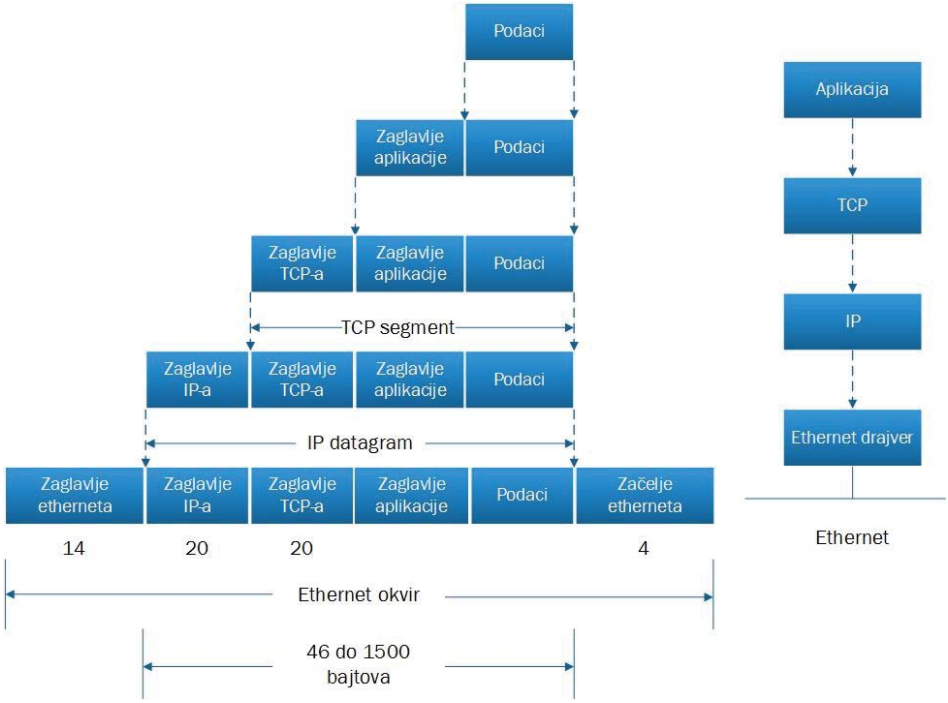
Originalni TCP/IP je prikazan na Sl.5.3. On ima četiri sloja:

- sloj host-mreža: host je povezan na proizvoljnu mrežu preko koje šalje i prima podatke,
- mrežni (Internet) sloj: odgovoran je za kretanje poruka po mreži od izvora do odredišta, pri čemu odredište može biti na istoj ili drugoj mreži; rutiranje podataka se vrši na ovom nivou putem IPv4 i IPv6 (Internet Protocol version 4 and 6),
- transportni sloj: implementira se u krajnjim sistemima (hostovima) u cilju pružanja komunikacionog servisa sloju aplikacije; na ovom nivou djeluju dva protokola i to konektivni, TCP i nekonektivni UDP (User Datagram Protocol) protokol
- aplikacioni sloj: širok skup protokola koji su dizajnirani za podršku različitim aplikacijama, kao što su razmjena elektronske pošte, razmjena fajlova, pretraživanje veba i sl (SMTP, FTP, HTTP, Telnet na Sl.5.3).

U savremenoj literaturi se protokoli Interneta klasifikuju pomoću hibridnog modela kod koga se sloj host-mreža dijeli na:

- sloj linka za podatke (DLL-Data Link Layer) koji se opet može podijeliti na dva podsloja:
  - MAC (Medium Access Control) služi za kontrolu pristupa zajedničkom medijumu koji dijeli više uređaja;
  - LLC (Logical Link Control) koji služi za kontrolu logičkog linka.
- fizički sloj: obuhvata mehaničke, električne funkcionalne i proceduralne karakteristike koje se odnose na prenos nestruktuirane povorke bita po fizičkom medijumu.

Podaci se od aplikacije sa jednog računara ka drugoj, prenose putem enkapsukacije kako je to ranije objašnjeno na primjeru OSI referentnog modela, [11], [16], [42], [52], [76]

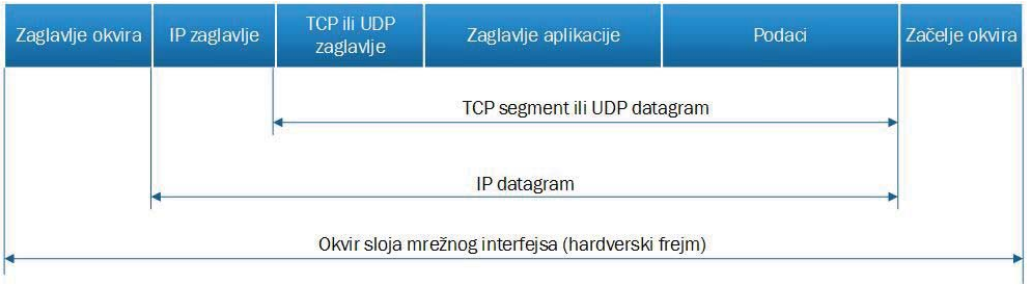


Slika 5.4: *Primjer enkapsulacije podataka kod TCP/IP protokol steka*

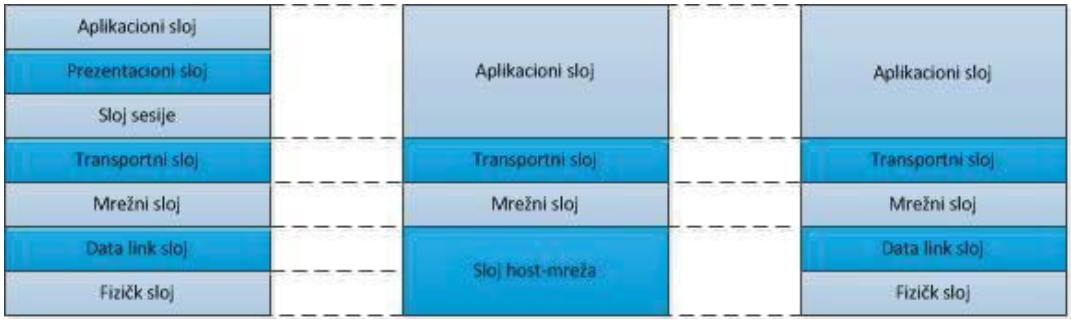
Na Sl.5.4. je prikazano je formiranje karakterističnih jedinica podataka pri prenosu kroz različite slojeve TCP/IP protokol steka.

Jedinice podataka na pojedinim nivoima TCP/IP protokol steka (Sl.5.5) su:

- jedinica podataka koje TCP ili UDP šalje IP-ju naziva se TCP (ili UDP) segment,
- jedinica podataka koje IP šalje mrežnom interfejsu je IP datagram, odnosno IP paket,
- dodavanjem zaglavlja i začelja okvira dobija se Ethernet okvir (ram, frejm),
- okvir predstavlja skup jedinica i nula koje je potrebno kodovati u digitalni signal za prenos kroz mrežu.



Slika 5.5: *Jedinice podataka na pojedinim nivoima TCP/IP skupa protokola*



Slika 5.6:. *Odnos između OSI referentnog modela, klasičnog i hibridnog modela TCP/IP protokol steka*

TCP/IP je naslijedio mnoge mehanizme i tehnike od već postojećih algoritama:

- algoritam „klizećeg prozora“,
- slanje potvrda (acknowledgements);

ali je morao da savlada i neke probleme koji se nisu pojavljivali na lokalnim mrežama:

- pristizanje poruka u različitom rasporedu od poslatog,
- različita vremena kašnjenja pojedinih paketa,
- različite veličine paketa na različitim mrežama.

5.1.2.1. Aplikacioni nivo TCP/IP protokol steka

Na Sl. 5.3 prikazani su neki od protokola na aplikacionom nivou TCP/IP protokol steka. O HTTP-u, FTP-u, Telenetu i SMTP-u će biti šire govora u poglavlju u kojem budemo govorili o Internet servisima, [16], [55].

Neki od protokola koji mogu djelovati na ovom nivou su još, recimo:

- SNMP (Simple Network Management Protocol) koji obezbjeđuje upravljanje i nadgledanje računarske mreže,
- BOOTP (BOOTstrap Protocol), pomoću koga se dobijaju informacije o konfiguraciji, uključujući i IP adrese.

5.1.2.2. Transportni nivo TCP/IP protokol steka

Postoje dvije osnovne klase servisa, odnosno načina komunikacije između računara i to:

- bez uspostavljanja veze (conectionless): nema ugovaranja veze između računara niti pošiljaoc zna da li je primaoc uspješno primio poruku,
- sa uspostavljanjem veze (connection-oriented): prije početka razmjene poruka između računara se uspostavlja logička veza, put ili ruta, poruke bi na odredište trebale stići bez greške i redom kako su poslate.

U skladu sa dva gore iznesena principa komunikacije između računara, razlikujemo i dva protokola transportnog nivoa koja ćemo opisati u nastavku izlaganja.

5.1.2.2.1. TCP

TCP je puni dupleksni, pouzdan protokol transportnog nivoa, sa uspostavljanjem veze (connection-oriented), kojim se ostvaruje logička veza sa „kraja na kraj“ između dva programa, [16], [38], [42], [52], [55], [76].

Podatke preuzete sa aplikacionog nivoa TCP rastavlja na segmente. Svaki segment se numeriše, kako bi TCP protokolu na odredišnom računaru bilo olakšano formiranje originalne poruke.

Za svaki poslati segment TCP očekuje potvrdu o njegovom prijemu. U slučaju da poruka o prijemu nije stigla u unaprijed određenom intervalu (timeout interval), segment se šalje ponovo. TCP baš zbog te svoje osobine, slanja potvrde za svaki segment poruke nije pogodan za komunikaciju u realnom vremenu kakva je prenos govora.

U slučaju dobrih uslova u mreži, može se ubrzati rad TCP-a i to na taj način da se iskoristi vrijeme poslije slanja segmenta od strane pošiljaoca do slanja potvrde o prijemu

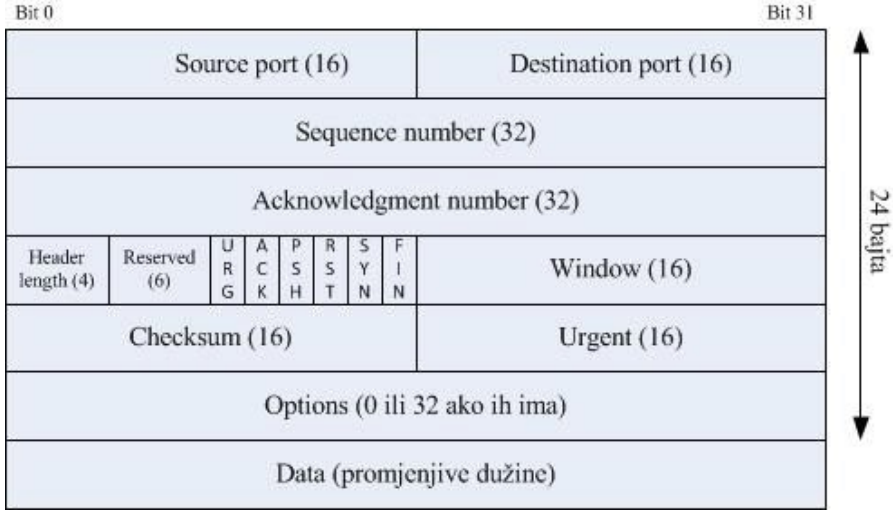
prethodnog segmenta na strani primaoca za slanje novih segmenata podataka. Za tu namjenu se koristi metod klizećeg prozora (sliding window).

Broj segmenata (ili tačnije broj bajtova) koje pošiljaoc može da pošalje bez primanja potvrde o njihovom prijemu određen je veličinom prozora. Tako recimo, ako konfigurišemo prozor veličine dva, dozvoljava se prenos dva segmenta podataka prije nego što stigne potvrda o prijemu. Poljem *acknowledgment number* se vrši potvrda prijema poslednjeg ispravno primljenog bajta. Svaka ACK poruka sadrži veličinu prozora (izraženu u bajtima) koju je prijemnik preman da primi u tom trenutku.

Dakle, TCP može podešavati prenosnu brzinu u zavisnosti od stanja mreže. tj. ako ne dobije pozitivan odgovor od odredišnog hosta, TCP redukuje prenosnu brzinu smanjivanjem veličine prozora do veličine 1, kod koje opet računar pošiljaoc čeka potvrdu od primaoca za svaki primljeni segment.

Podešavanjem veličine prozora se vrši i kontrola zagušenja, jer ako pošiljaoc pošalje previše podataka koje primaoc ne stigne da obradi, primaoc ima na raspolaganju jedino mogućnost baferovanja podataka, ali ako se bafer prepuni, svi novopristigli podaci će biti odbačeni.

TCP konekcija podrazumijeva tačno dva kraja koji komuniciraju, tako da koncept *broadcasting*-a i *multicasting*-a (što će biti objašnjeno u nastavku) nije primjenjiv.



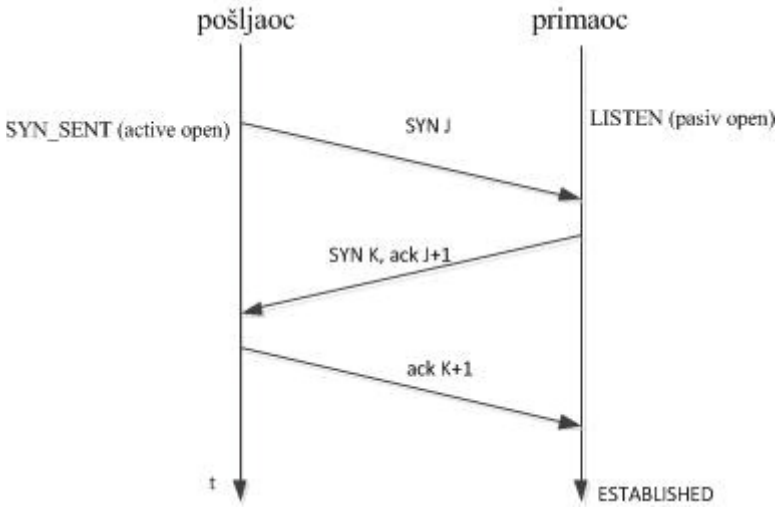
Slika 5.7: *Format TCP segmenta*

Na Sl.5.7 je prikazan format TCP segmenta. Sa slike se vidi da je zaglavlje TCP-a dužine 20 ili 24 bajta (sa opcijama). Najznačajniji bit, MSB je označen na slici sa 0, dok je najmanje značajan označen sa 31. Prvo se prenose najznačajniji biti.

TCP segment čine sledeća polja:

- Source/Destination port (port izvora i odredišta): služe za identifikovanje aplikacije na predajnoj i prijemnoj strani; brojevi porta zajedno sa IP adresama predajnika i prijemnika jedinstveno određuju svaku TCP konekciju,
- Sequence number (redni broj): služi za identifikovanje svakoj bajta podatka u TCP segmentu; vrijednost ovog polja u sebi sadrži ISN (Initial Sequence Number), koji je računar odabrao za datu konekciju; prilikom uspostave konekcije SYN fleg je setovan, a broj sekvence prvog bajta podataka je ISN+1,
- Acknowledgment number (broj potvrde): označava redni broj sledećeg bajta (okteta) koji TCP cjelina očekuje da primi,
- Header length (dužina zaglavlja): dužina TCP zglavlja u 32-bitnim riječima,
- Reserved: namijenjeno za buduću upotrebu i trenutno se ne koristi,
- Flags: postoji šest flegova:
    - URG: označava validnost urgent pointera,
    - ACK: ackowledgment number je validan,
    - PSH: prijemnik mora proslijediti podatke do aplikacije što prije,
    - RST: resetovanje konekcije,
    - SYN: setovan je samo prilikom uspostavljanja konekcije,
    - FIN: zahtjev za raskidanjem konekcije,
- Window size: koristi se za kontrolu toka podataka; prijemnik pomoću ovog polja oglašava veličinu prozora u bajtima, tj veličinu slobodnog prostora u prijemnom baferu,
- Checksum: služi za provjeru ispravnosti poslatog segmenta (i podataka i zaglavlja)
- Urgent pointer: validan je samo ako je URG bit setovan; kada se ova vrijednost doda na redni broj segmenta dobije se vrijednost poslednjeg bajta u sekvenci podataka koje je potrebno hitno isporučiti aplikaciji,
- Options: dužina ovog polja je varijabilna; najčešće se koristi za označvnje maksimalne dužine segmenta (MSS-Maximum Segment Size) koju je jedan kraj konekcije spreman da primi,
- Data: u ovo polje se smiještaju podaci primljeni od aplikacije; polje je promjenjive dužine.

Prije otpočinjanja slanja segmenata uspostavlja se komunikacija između računara pošiljaoca i računara primaoca na način prikazan na slici 5.8.



Slika 5.8: *Uspostava TCP sesije*

Prilikom uspostave veze, šalju se tri segmenta (three-way handshake). Strana koja prva šalje SYN segment (pošiljaoc, klijent), odnosno traži zahtjev za uspostavu sesije, vrši aktivno otvaranje, dok druga strana vrši pasivno (primaoc, server) otvaranje veze

Klijent šalje SYN segment sa brojem porta servera sa kojim želi da uspostavi vezu i sa svojim ISN-om (Initial Sequence Number) koji je na slici je označen sa J.

Server odgovara sa svojim SYN segmentom koji sadrži serverov ISN (na slici označen sa K). Server u istom segmentu potvrđuje klijentov SYN slanjem ACK na klijntov ISN (slanjem J+1).

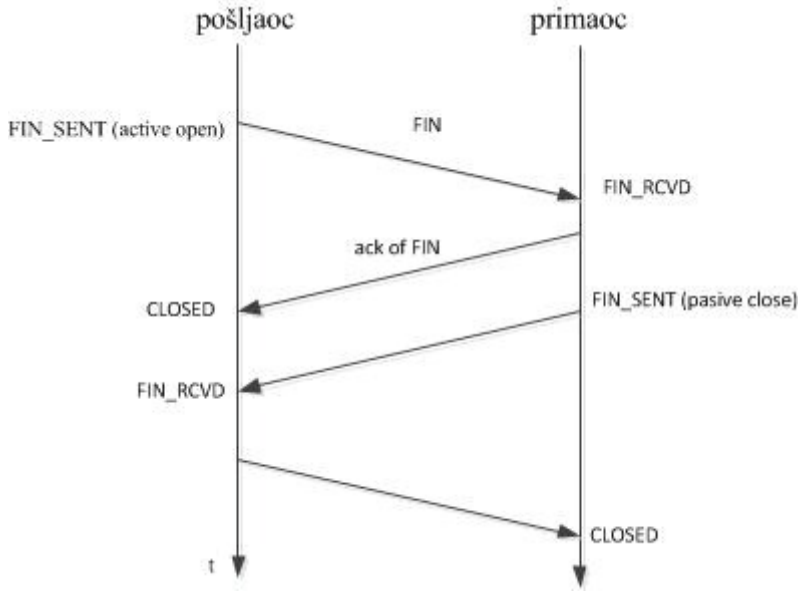
Klijent potvrđuje serverov SYN slanjem ACK na serverov ISN (slanjem K+1).

Poslije razmjene ova tri segmenta upostavljena je logička veza između klijenta i servera. Na ovaj način je osigurano da obje strane u komunikaciji budu spremne na prijem podataka, tj da postoji konekcija u oba smijera.

TCP konekcija je potpuni dupleks, ali je moguće ostvariti prekid konekcije u jednom smijeru. U tom slučaju strana koja je prekinula vezu u jednom smijeru (half-closed) više ne šalje segmente sa podacima, ali je sposobna da ih prima.

Za potpuni prekid konekcije koriste se četiri segmenta, kako je to prikazano na Sl.5.9.

Strana koja prva šalje FIN segment vrši aktivno, a druga strana pasivno zatvaranje. Zahtjev za raskidaljem konekcije može pokrenuti bilo koja strana.



Slika 5.9: *Raskid TCP konekcije*

Recimo da pošiljaoc (klijent) nema više podataka za slanje. On ka primaocu (serveru) šalje segment u kome je FIN fleg setovan, tzv, FIN segment.

Prijemom FIN segmenta, klijent šalje serveru potvrdu o prijemu. Poslije ova dva segmenta veza je zatvorena u jednom smijeru, tako da klijent ne može više slati podatak dok se veza ponovo ne uspostavi, ali i dalje može slati potvrde.

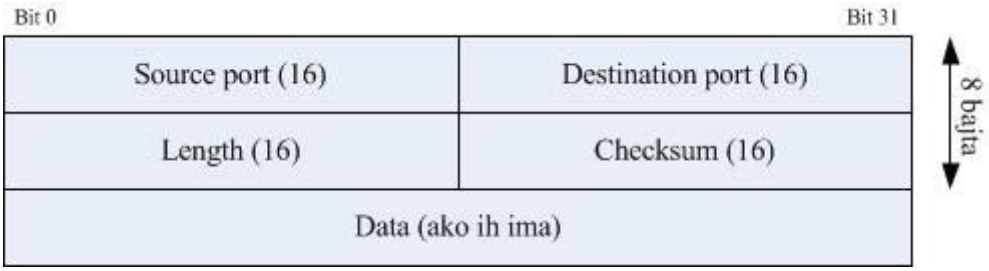
U slučaju da server takođe nema podataka za slanje pristupa zatvaranju veze šaljući FIN segment klijentu.

Klijent poslije prijema ovog segmenta odgovara na serverov FYN segment čime se veza prekida i u drugom smijeru.

5.1.2.2.2. UDP

UDP ne zahtijeva prethodno uspostavljenu vezu između izvora i odredišta (conectionless), tako da nema kontrole toka.

UDP ne obezbjeđuje pouzdanost (to je zadatak sloja aplikacije), ne bilježi koji su segmenti poslati, niti se očekuje potvrda njihovog prijema. UDP zauzima mnogo manje propusnog opsega mreže u odnosu na TCP, pa je stoga i ekonomičniji, [16], [37], [42], [52], [55].



Slika 5.10: *Format UDP segmenta*

UDP segment čine sledeća polja:

- Source port: identifikuje program koji šalje podatke,
- Destination port: identifikuje program koji prima podatke,
- Length: definiše dužinu UDP zaglavlja i UDP podataka u bajtima; minimalna dužina ovog polja je 8 (slučaj kad UDP poruka nema podataka).
- Checksum: služi za provjeru ispravnosti UDP zglavlja i UDP podataka.

5.1.2.3. Mrežni (Internet) sloj TCP/IP protokol steka

Na mrežnom nivou TCP/IP protokol steka radi IP protokol. On predstavlja „radnu snagu“ TCP/IP protokol steka. Sve poruke viših nivoa se prenose unutar IP paketa, datagrama.

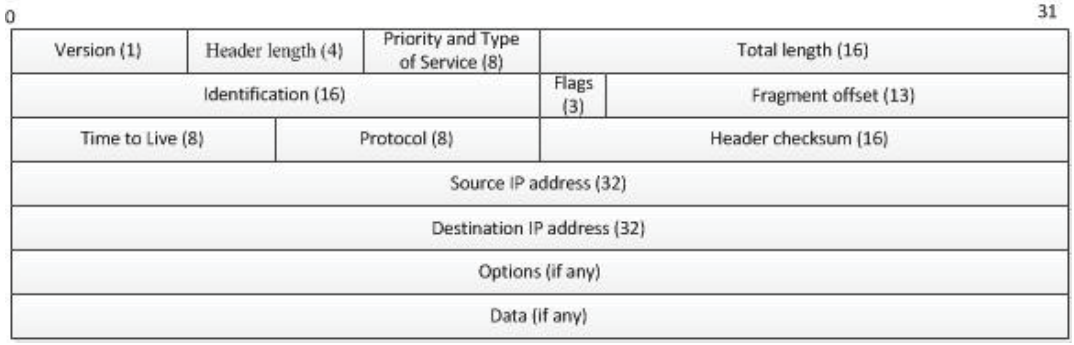
IP protokol se definiše kao servis bez upostavljanja veze, budući da ne postoji veza između paketa koji se šalju na isto odredište. IP pregleda adresu svakog paketa, zatim na osnovu tabele rutiranja, odlučuje gdje da pošalje paket birajući najbolju putanju. Paketi se nezavisno šalju i oni ne moraju stići na odredište redom kojim su poslani.

IP je nepouzdan protokol jer ne postoji garancija da će paket da stigne do odredišta.

Najvažnija funkcija IP protokola je rutiranje. Rutiranje predstavlja nalaženje putanje (rute) od izvora ka odredištu. Na podatke koje IP šalje nižem sloju dodaje se IP zaglavlje.

Ovdje ćemo predstaviti zaglavlje IPv4 (Internet Protocol Version 4) protokola i IPv6 (Internet Protocol Version 6), [16], [34], [76].

5.1.2.3.1. Zaglavlje IPv4



Slika 5.11: *Polja IPv4 zaglavlja*

Na Sl.5.11 su prikazana polja [34], IPv4 zaglavlja:

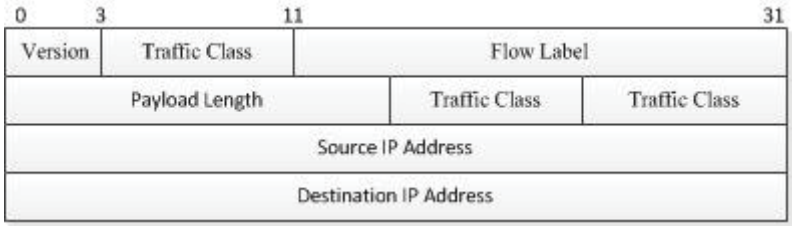
- Version: trenutna verzija IP protokola, ovdje je to 0100 (IPv4),
- Header Length: broj 32-bitnih riječi u IP zaglavlju, uobičajena vrijednost ovog polja je 5,
- Priority and Type of Service: prioritet i tip servisa za dati datagram; samo jedan od sledećih tipova servisa se može izabrati:
  - minimilno kašnjenje (minimize delay),
  - maksimalna brzine (maximize throughput),
  - maksimalna pouzdanost (maximize reliability)
  - minimizacija novčanih troškova (minimize monetary cost),
- Total length: predstavlja ukupnu dužinu IP datagrama; na osnovu ovog polja i polja *Header length* može se odrediti pozicija i veličina podataka u IP datagramu,
- Identification: ovo polje služi za identifikaciju datagrama koji se šalje; sadržaj polja se uvećava za jedan svaki put kada se pošalje novi datagram; u slučaju fragmentacije svaki od dijelova originalnog datagrama će imati isti identifikacioni broj;
- Flags:
  - prvi bit se ne koristi;
  - drugi bit, DF (Dont't Fragment): označava da li je dozvoljena fragmentacija (nije setovan),
  - treći bit, MF (More Fragments) označava da li to poslednji fragment (nije setovan)
- Fragment offset: označava poziciju fragmenta u originalnom datagramu, tj. udaljenost datog fragmenta u bajtima od početka originalnog datagrama,
- Time to Live: predstavlja „vrijeme života" datagrama (hop counter), odnosno gornji limit broja rutera kroz koje datagram može proći; izvor inicijalizuje

vrijednost ovog polja pri čemu se vrijednost smanjuje svaki put kada datagram prođe kroz neki ruter; datagram sa vrijednošću TTL-a nula se odbacuje čime se izbjegava mogućnost da datagram ostane u mreži beskonačno dugo,

- Protocol: ovo polje sadrži identifikator protokola (ICMP, TCP, UDP) kome treba isporučiti podatke prospjelog datagrama, što se naziva demultipleksiranje,
- Header checksum: služi za provjeru validnosti zaglavlja datagrama; provjerava se u svakom od rutera i u slučaju da je došlo do greške datagram se odbacuje pri čemu se ne šalje nikakvo obavještenje pošiljaocu datagrama,
- Source IP address/Destination IP adress: svaki datagram sadrži IP adresu izvora i odredišta;
- Options: dužina ovog polja je varijabilna; trenutno su definisane sledeće opcije:
  - opcije vezane za sigurnost datagrama,
  - snimanje rute :ruter kroz koji datagram prolazi upisuje svoju IP adresu,
  - timestamp: ruter upisuje IP adresu i vrijeme,
  - loose source routing: definiše se lista IP adresa koje datagram mora proći pri čemu može koristiti i druge IP adrese,
  - strict source routing: definišu se IP adrese kroz koje datagram smije proći,
- Data: sadrži segment primljen od višeg sloja.

5.1.2.3.2. IPv6

IPv4 raspolaže sa malim brojem raspoloživih adresa, pa uvažavajući činjenicu da je broj korisnika Interneta u naglom porastu bilo je potrebno uvesti protokol koji će omogućiti mnogo veći adresni prostor. To je osnovni zadatak IPv6 protokola. Uz to IPv6 ima i mnogo manje zaglavlje u odnosu na IPv4, što omogućava efikasnije rutiranje, jer kraće zaglavlje omogućava ruterima bržu obradu paketa. IPv6 je donio veliki napredak na polju sigurnosti implementacijom *IPSec* protokola. IPv6 ima ugrađenu podršku za kvalitet servisa (QoS-Quality of Service), [16], [34].



Slika 5.12: *Zaglavlje IPv6 protokola*

Na Sl.5.12. su prikazana polja IPv6 zaglavlja:

- Version: verzija IP protokola, ovdje je to 0110 i označava da je u pitanju verzija 6,
- Traffic Class: ima isto značenje kao polje *Priority nad Type of Service* kod IPv4,

- Flow Label: ovo polje nije bilo kod IPv4 i njegova namjena je da omogućava diferenciranje paketa na mrežnom sloju, dodjeljujući pakete određenom toku podataka između izvora i odredišta čime je omogućeno aplikacijama na krajnjim sistemima da lako razdvoje saobraćaj i ostvare potreban kvalitet servisa (QoS),
- Payload Length: polje označava ukupnu dužinu podataka u paketima,
- Next Header: slično polju Protocol kod IPv4; određuje koja vrsta informacije slijedi poslije osnovnog zaglavlja kod IPv6 (može biti dodatno zaglavlje IPv6, ICMPv6, podaci sa transportnog nivoa),
- Hop Limit: kao TTL kod IPV4,
- Source IP Address/Destination IP Address: IPv6 adresa izvora i odredišta.

5.1.2.3.3. IP fragmentacija

Većina mreža posjeduje gornje ograničenje u pogledu maksimalne količine podataka koje se kroz nju mogu prenijeti u okviru jednog okvira. Ovo ograničenje se naziva MTU (Maximum Transmission Unit). Za prenošenje većih datagrama koristi se tehnika koja se naziva fragmentacija, [16], [34], [52].

***Def.**: Fragmentacija je proces dijeljenja datagrama (na ruteru) dužine veće od MTU na pakete čija je dužina manja od MTU.*

Fragment ima isti format kao i ostali datagrami. DF biti u polju *Flags* daju informacije u tome da li je fragmentacija dozvoljena.

Na svaki fragment dodaje se kopija IP zaglavlja, tako da oni postaju nezavisni datagrami. Budući da svaki fragment sadrže kopiju zaglavlja originalnog datagrama, svi fragmenti imaju istu adresu odredišta kao originalni datagram.

***Def.**: Proces ponovnog stvaranja kopije originalnog datagrama iz fragmenata na mjestu prijema se naziva sastavljanje (reassembly).*

Datagram koji nosi poslednji fragment ima setovan MF bit u polju *Flags.*

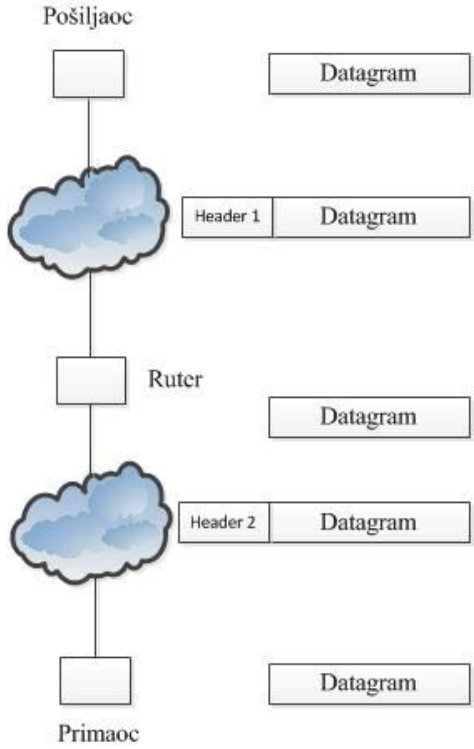
Na odredištu se prispjeli fragmenti sastavljaju na osnovu identifikacionog broja, odnosno polja *Identification* iz IP zaglavlja, koje jedinstveno određuje originalni datagram. Svaki fragment tog datagrama ima isti identifikacioni broj. Polje *Fragment offset* iz IP zaglavlja dodatno određuje redoslijed datagrama.

U slučaju gubitka nekog od fragmenata svi ostali fragmenti se brišu.

Fragmentacija se može vršiti na izvoru, ali i na bilo kojem ruteru na putu do odredišta budući da datagram može prolaziti kroz različite mreže sa različitim MTU-ovima na putu do odredišta.

Pri prenosu IP datagrama, pošiljaoc enkapsulira cijeli IP datagram u odgovarajući fizički okvir mreže kroz koju se on prenosi. Potrebno je izvršiti i prevođenje IP adrese u odgovarajuću fizičku adresu i slanje datagrama kroz fizičku mrežu.

Sa Sl.5.13, se vidi da na putu do odredišta datagram prolazi kroz još jednu mrežu. Tu se obavlja deenkapsulacija i datagram se izvlači iz prethodnog okvira i ubacuje u novi na putu do odredišta, gdje se iz novog okvira izvlači datagram.



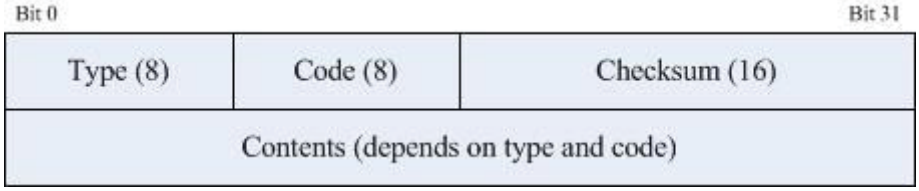
Slika 5.13: *Prenos datagrama preko Interneta*

5.1.2.3.4 ICMP

ICMP (Internet Control Message Protocol) je sastavni dio IP-a i mora postojati u svakom IP modulu, istovremeno ICMP koristi IP na isti način kako to čine i viši protokoli. ICMP paketi se pakuju u IP datagrame, sa oznakom protokola 1.

ICMP se koristi za prijavljivanje grešaka, ali on ne čini IP pouzdanim. Od viših nivoa zavisi kako će dobijena ICMP poruka biti upotrebljena, [16], [34], [48].

Na Sl.5.14 je prikazano zaglavlje ICMP protokola.



Slika 5.14: *Zaglavlje ICMP-a*

Značenje pojedinih polja iz zaglavlja ICMP-a:

- Type: služi za identifikaciju određene ICMP poruke (postoji 15 različitih poruka),
- Code: za dodatno opisivanje poruke,
- Checksum: računa se za čitavu ICMP poruku i služi za provjeru ispravnosti primljenog ICMP paketa,
- Contents: zavisi od tipa i koda poruke, ali se u ovo polje uvijek bilježi:
  - IP zaglavlje,
  - najmanje 8 bajta poruke koja je prouzrokovala ICMP poruku; ovo omogućava primaocu ICMP poruke da poruku dodijeli odgovarajućem protokolu (na osnovu polja *Protoco*l u IP zaglavlju) i određenoj aplikaciji (na osnovu polja *Port number* u TCP ili UDP zaglavlju),

Navest ćemo neke od ICMP zahtjeva:

- zahtjev za eho (type 8, code 0),
- eho odgovor (type 0, code 0),
- zahtjev za mrežnom maskom (type 17, code 0),
- odgovor na taj zahtjev (type 18, code 0),

Neke od ICMP poruka greške (error message):

- nedostižna destinacija (type 3),
  - nedostižna mreža (code 0),
  - nedostižan računar (code 1),
  - nedostižan protokol (code 2),
- vrijednost TTL-a je nula (type 11)

- problemi sa parametrima (type 12):
  - IP zaglavlje je loše (code 0),
  - zahtijevana opcija nedostaje (code 1).

Da bi se izbjeglo neograničeno povećanje poruka u mreži, ICMP poruka se nikad ne generiše kao odgovor na druge ICMP poruke.

ICMP se koristi za:

- popunjavanje sadržaja tabele rutiranja,
- otkrivanja MTU-a neke putanje,
- dijagnostiku problema u mreži (ping, tracert i path ping programi),
- podešavanje inteziteta saobraćaja da bi se izbjeglo preopterećenje rutera.

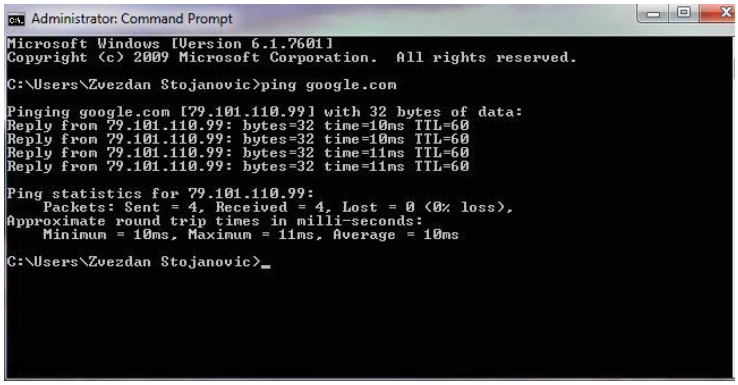
5.1.2.3.4.1. Ping

Kada se konektujemo na Internet, najprije treba da znamo da li možemo sa nekim da obavljamo komunikaciju, tj da li je računar sa kojim želimo da komuniciramo dostupan.

Komanda *ping* se može koristiti za određivanje:

- dostupnosti nekog računara,
- puta datagrama kroz mrežu,
- Round Trip Time, tj. vremena potrebnog da stigne potvrda o prijemu poruke od strane drugog računara,
- IP adresa na osnovu imena.

Na Sl.5.15 je prikazan primjer pokretanja komande ping. Pokrećemo je ukucavanjem u Command Prompt-u (na putanji Start/Accessories/Command Prompt) komande ping poslije koje ide razmak pa URL adresa (u ovom slučaju servera čiju dostupnost ispitujemo), [16], [90].



Slika 5.15: *Primjer upotrebe komande ping*

Ako u Command Prompt-u unesemo samo komandu *ping*, dobićemo spisak svih raspoloživih opcija. Upisom komande ping (Sl.5.15) ovaj program šalje ICMP paket *Echo Request* na odredišnu IP adresu da bi se provjerilo da li je TCP/IP pravilno konfigurisan i da li je udaljeni TCP/IP sistem dostupan.

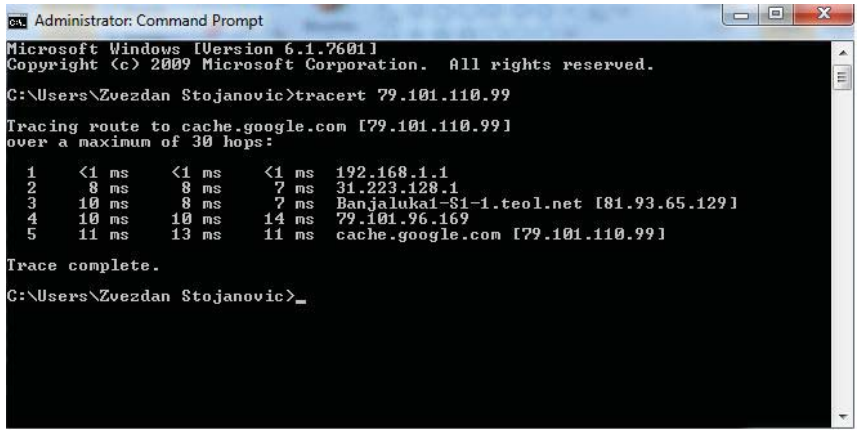
Na primjer ako unesemo-*w timeout*, to će nam omogućiti podešavanje dužeg vremena za čekanje odgovora (u milisekundama). Podrazumijeva se čekanje do jedne sekunde za dobijanje odgovora prije nego što se obustavi čekanje.

5.1.2.3.4.2. Tracert

Tracert omogućava praćenje puta koji datagram prolazi kroz mrežu, tj. bilježi rutere kroz koje je datagram prošao. *Tracert* koristi IP polje TTL (Time to Live) u ICMP paketu *Echo Request* i ICMP poruke *Time Exceeded* kako bi se odredila putanja od izvora do odredišta kroz međusobno povezane IP mreže, [16], [90].

TTL predstavlja gornju vremensku granicu egzistencije datagrama u Internet sistemu. TTL polje postavlja pošiljalac datagrama i ono se redukuje pri prolasku svakog hosta na ruti do odredišta. Ako vrijednost TTL polja padne na nulu prije nego što datagram dođe na odredište šalje se ICMP poruka *Time Exceeded* do pošiljaoca.

Prilikom pinganja preko simboličkog imena www.google.com DNS razrešivač (DNS Resolver) nam je dao IP adresu 79.101.110.99 koja odgovara tom imenu i koju smo iskoristili prilikom pokretanja komande tracert (Sl.5.16).



Slika 5.16: *Primjer upotrebe komande TRACERT*

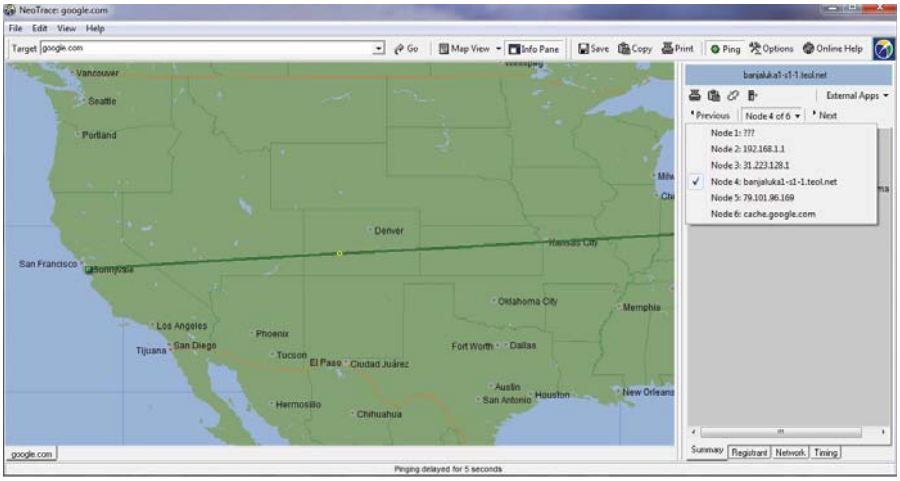
Značenje pojedinih kolona sa Sl.5.16:

- prva kolona predstavlja broj hopa,
- naredne tri su RTT vrijednosti u ms,

- peta je ime hosta.

Sva vremena odziva do 500ms smatraju se prihvatljivima, ali u slučaju da su veća to može upućivati na problem sa ruterom u toj tački.

Program Neo Trace pored funkcija koje ima *Tracert* je uveo i grafičku predstavu putanje datagrama između izvora i odredišta (Sl.5.17).



Slika 5.17: *Primjer primjene Neo Trace programa*

5.1.2.4. Fizički nivo

Fizički i data nivo (hibridni TCP/IP koji se danas koristi) uključuje u sebe mrežnu karticu i odgovarajuće drajvere koji su zaduženi za hardverske detalje pomoću kojih računar pristupa na mrežni kabl, bez obzira koji se medijum koristi, [55].

Na ovom sloju se šalju i primaju bitovi podataka i zavisno od vrste medijuma po kojem se prenose, ovi bitovi se predstavljaju na različite načine. Za svaku vrstu medijuma, potrebni su specifični protokoli da bi opisali koji će se šablon bitova prenositi.

Za fizički i data nivo je definisano više protokola koje može podijeliti na:

- protokole koji definišu LAN-ove (recimo Ethernet),
- protokole za modemsku komunikaciju (PPP, SLIP...),
- protokole koji se koriste u mrežama sa komutacijom paketa (X.25),
- HDLC (High Level Data Link Control).

U poglavlju u kojem smo govorili o računarskim mrežama, ali i u nastavku izlaganja orijentisali smo se na Ethernet kao danas najzastupljeniju LAN i WAN mrežu

POGLAVLJE 6

Adresiranje na Internetu

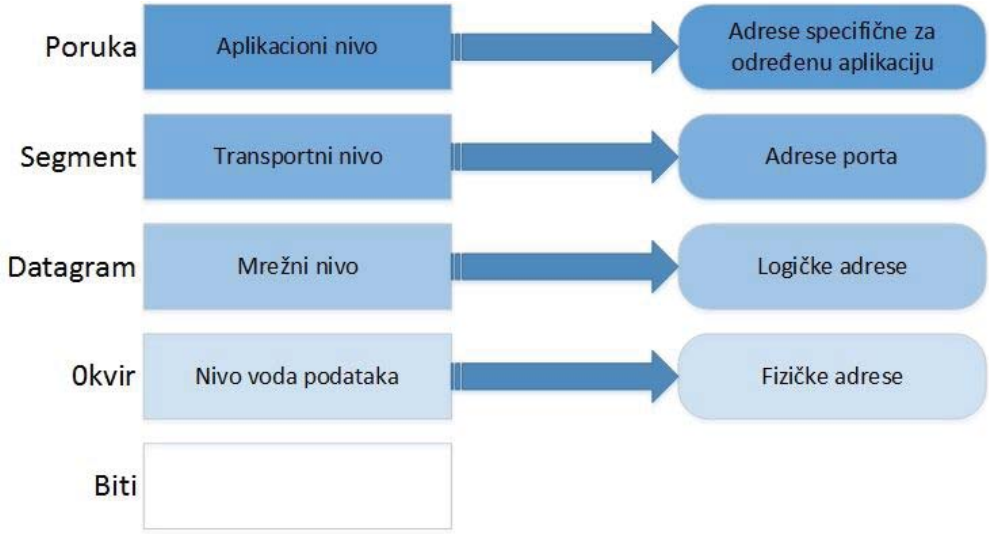
Da bi dva računara spojena na Internet mogli međusobno da komuniciraju, odnosno da bi se mogli prenijeti podaci između njih, potrebno je da se koriste određene adresne šeme. U prethodnom poglavlju smo opisali nivoe TCP/IP protokol steka. Svakom nivou odgovara određena šema adresiranja i one će ukratko biti opisane u ovom poglavlju.

6.1. Adresiranje na Internetu

Kod računarskih mreža koje koriste TCP/IP skup protokola koriste se sledeća četiri nivoa adresiranja:

- fizička adresa,
- logička adresa,
- port adresa,
- aplikaciono specifična adresa.

Svaka od adresa je u vezi sa nekim od nivoa TCP/IP arhitekture.



Slika 6.1: *Adresiranje kod TCP/IP skupa protokola*

6.1.1. Fizička adresa (MAC adresa)

Fizička adresa, (adresa veze, link adresa) jeste adresa čvora definisanog u okviru LAN-a ili WAN-a. Ona je sastavni dio okvira, (rama, frejma) koji se koristi, predaje, na nivou veze. Kako se vidi sa Sl.6.1, to je adresa najnižeg nivoa. Oblast važenja fizičke, MAC (Media Access Control) adrese je ograničena na LAN ili WAN, [34], [90].

Kod najvećeg broja LAN-ova koristi se 48-bitna (6-bajtna) fizička adresa zapisana u obliku 12 heksadecimalnih cifara.

Fizičke adrese mogu biti tipa:

- *unicast*: jedinstveni primalac okvira,

- *multicast*: okvir se prima od strane grupe primalaca,
- *broadcast*: svi čvorovi u mreži primaju okvir.

Sve mreže ne podržavaju rad sa svim tipovima fizičkih adresa (recimo *multicast* ili *broadcast*). Moguće je da se simulira *broadcast* ili *multicast* adresa korištenjem *unicast* adresa.

6.1.2. Logičke (IP) adrese

Korištenje fizičkih adresa je neadekvatno kod povezivanja većeg broja različitih tipova mreža iz razloga što različite mreže mogu da koriste različite adresne formate.

Uvodi se univerzalni sistem adresiranja kod koga se svaki računar identifikuje na jedinstven način, nezavisno od tipa fizičke mreže. Za ovu namjenu se koriste logičke adrese, [34], [48], [90].

Logička adresa (IP adresa) kod Interneta je 32-bitni broj i ona jedinstveno identifikuje računar povezan na Internet.

IP adrese se zapisuje kao četiri decimalna broja razdvojena tačkama (po jedan za svaki bajt adrese), npr. 192.168.0.1.

I IP adrese mogu biti *unicast*, *multicast* i *broadcast* tipa.

IP adrese su podijeljene u 5 klasa (A,B,C,D,E). Svaka IP adresa ima dva dijela:

- adresu mreže,
- adresu računara (hosta).

Prvobitna podela IP adresa na klase:

- klasa A, za 2^7 velikih mreža sa po 2^{24} računara,
- klasa B, za 2^{14} mreža srednje veličine sa po 2^{16} računara,
- klasa C, za 2^{21} mreža male veličine sa po 255 računara),
- klasa D, adrese rezervisane za *multicasting*, tj. za istovremeno adresiranje grupe računara,
- klasa E, adrese rezervisane za eksperimentalnu upotrebu.

Slika 6.2: *Klase IP adresa*

Opseg IP adresa za pojedine klase mreža je dat u Tabeli 6.1.

Tabela 6.1: *Klase IP adresa*

Klasa	Opseg	
	od	do
A	0.0.0.0	127.255.255.255
B	128.0.0.0	191.255.255.255
C	224.0.0.0	223.255.255.255
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

Ovakvo adresiranje nije bilo efiksano jer je veliki broj IP adresa klase A i B je ostajao neiskorišćen, a rijetke su tako velike mreže.).

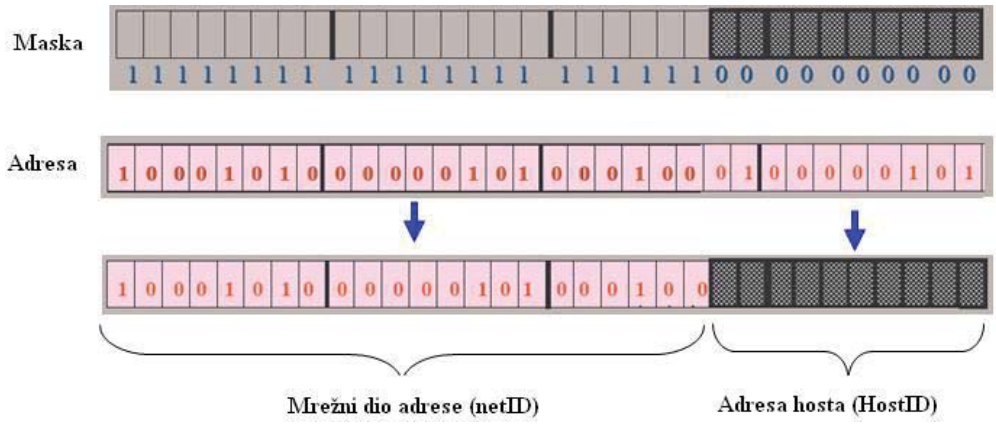
Za efikasnije iskorištenje adresnog prostora vrši se podjela adrese računara na dva dijela:

- adresu podmreže (subnet address),
- adresu računara (host address).

Koji dio IP adrese je Net ID, a koji Host ID određuje podmrežna maska (*subnet mask*). Podmrežna maska je dužine 32 bita, a čini je:

- niz „1“ dužine koja se poklapa sa dužinom adrese mreže (Net ID),
- niz „0“ dužine koja se poklapa sa dužinom adrese hosta (Host ID)

Mrežna maska se često izražava i preko broja jedinica. Tako se za masku sa donje slike kaže da je dužine 22, jer maska ima 22 jedinice.



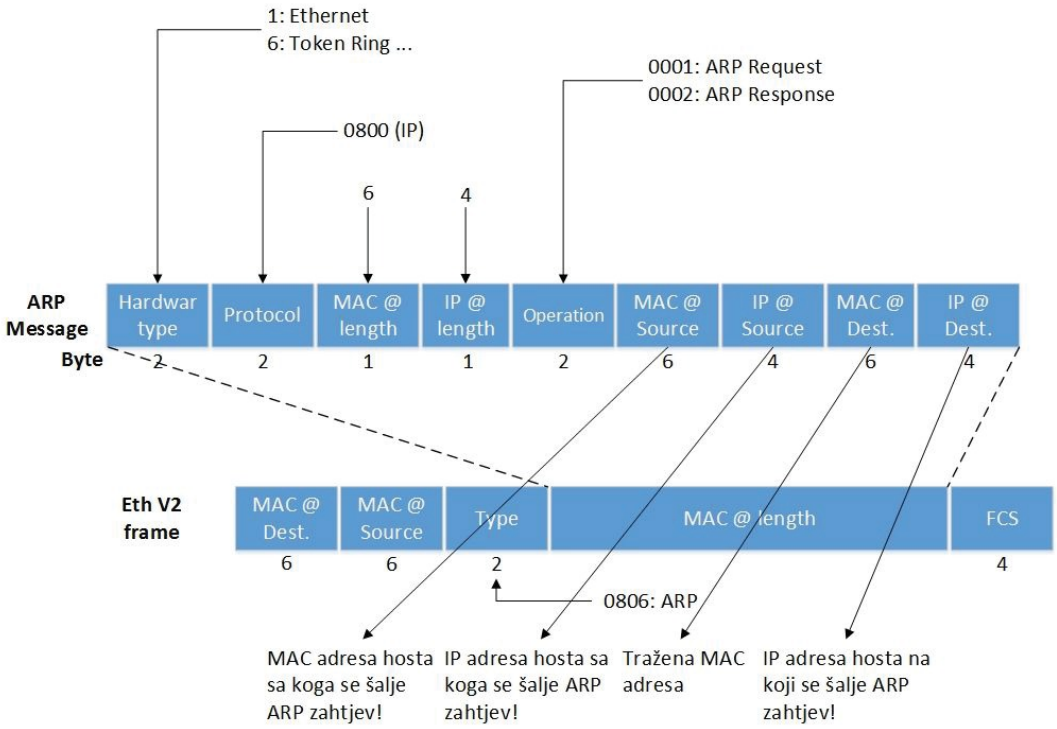
Slika 6.3: *Operacija određivanja mrežnog dijela (AND) operacija*

Adresa hosta sa Sl.6.3 može biti u opsegu 00 00000000 do 11 11111111.

Nulta adresa se uzima kao adresa mreže i ne koristi se za adresiranje računara, dok se poslednja adresa u opsegu koristi za mrežni *broadcast* i ne koristi se za adresiranje računara.

6.1.2.1. Protokol za razrješavanje adresa

Prilikom priključenja računara na mrežu i uspostavljanja veze sa drugim računarem, potrebno je znati i njegovu fizičku i logičku adresu. Pomoćni protokol IP protokola, koji služi za dobijanje informacije o MAC adresi na osnovu IP adrese se naziva protokol za rezoluciju adresa (ARP-Address Resolution Protocol), [34], [48].



Slika 6.4: *Određivanje MAC adrese računara kad je poznata njegova IP adresa*

Recimo da je prilikom uspostave komunikacije između dva računara, prvom računaru poznata samo IP adresa drugog. Šalje se ARP paket *broadcast*-om u mrežu, kako je to prikazano na Sl.6.3. Svi računari u toj mreži prihvataju taj paket a onaj koji je prepoznao svoju IP adresu formira ARP odziv i šalje ga prvom računaru.

6.1.2.2. Podrazumijevani mrežni prolaz

Računari koji se nalaze u istoj mreži (recimo u istom LAN-u) komuniciraju direktno. Međutim ukoliko se ne nalaze u istoj mreži oni onda komuniciraju preko podrazumijevanog mrežnog prolaza (default gateway), [48].

Sve ono što nije namijenjeno računaru unutar sopstvene mreže se šalje preko podrazumijevanog mrežnog prolaza.

Ukucavanjem komande *ipconfig* u Command Prompt-u (Accessories/Command Prompt) bez navođenja parametara dobit ćemo mrežne informacije:

- IP adresa,
- mrežna maska,
- podrazumijevani mrežni prolaz.

Slika 6.5: *Host informacije*

Kako mrežni uređaj (PC, ruter), može da odredi da li je odredište u njegovoj mreži ili van nje?

Vrši se logička operacija AND između sopstvene IP adrese i mrežne maske i odredišne IP adrese i mrežne maske.

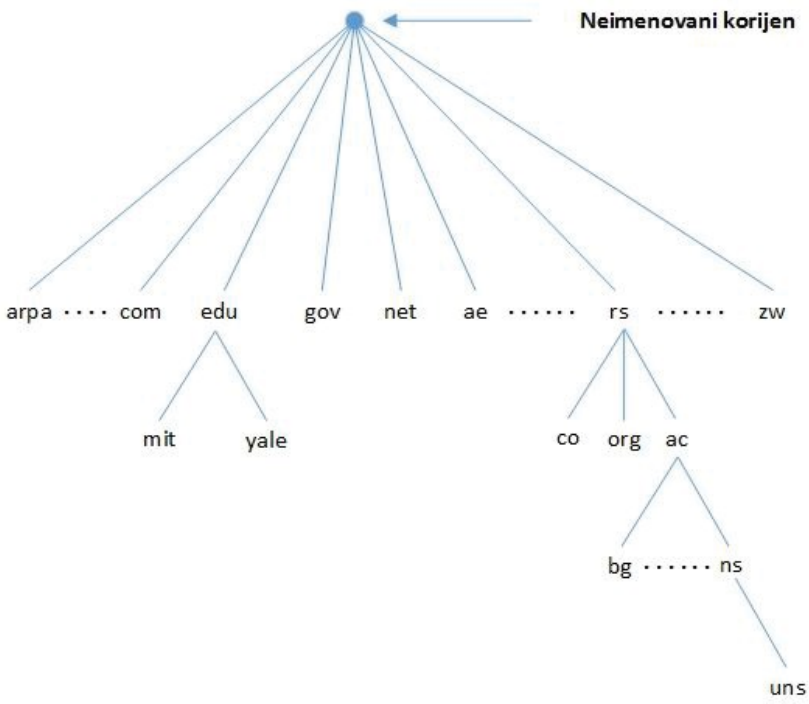
Ukoliko je mrežni dio u oba slučaja isti, to znači da je odredište u sopstvenoj mreži i podaci se šalju direktno, a ako se razlikuje, podaci se šalju preko podrazumijevanog mrežnog prolaza (rutera prvog hopa).

6.1.2.3. Sistem imena domena

Predstava IP adresa preko decimalnih brojeva nije pogodna za pamćenje i ne daje mnogo informacija o računaru, pa su uvedena simbolička imena koja odgovaraju IP adresama, npr (www.google.com, www.yahoo.com i sl.).

Protokol koji omogućava preslikavanje između IP adrese i simboličkih imena se naziva DNS (Domain Name System) protokol.

DNS predstavlja hijerarhijski organizovan sistem Servera imena (Sl.6.6) od kojih svaki posjeduje svoju bazu podataka u koju je smješten dio IP adresa i njima odgovarajućih imena. Nijedan Name Server ne posjeduje informaciju o svim IP adresama nego oni međusobno komuniciraju u cilju određivanja pojedine IP adrese, [34], [39], [48].



Slika 6.6: *Organizacija DNS-a*

TCP/IP modul koji komunicira sa lokalnim Name Server-om i koji na osnovu imena obezbjeđuje IP adresu se naziva DNS razrješavač (DNS Resolver).

Oblik Internet adresa na koji smo mi navikli, koji nam je lakši za pamćenje i sa kojim se susrećemo svakodnevno ima sledeći oblik: USERID@DOMAIN, pri čemu USERID predstavlja korisničko ime (koje nam je dodijelio naš ISP), dok DOMAIN predstavlja ime računara. Da bi dali više podataka o računaru kojim pristupamo Internetu uvode se sub-domain-i (poddomeni)

Posmatrajte sada sledeće adrese e-pošte:

zvezdan@uns.ns.ac.rs

Svaki dio domena odvojen tačkom (.) se naziva poddomenom, pri čemu onaj koji se nalazi na krajnoj desnoj strani se naziva top-level domain, odnosno domenom najvišeg nivoa.

Domen najvišeg nivoa u adresi e-pošte zvezdan@uns.ns.ac.rs, je **rs** i to je oznaka zemlje, odnosno regiona.

Neka imena domena najvišeg nivoa ćemo dati u Tabeli 6.2.

Tabela 6.2: *Imena domena najvišeg nivoa*

IME DOMENA	ZNAČENJE
COM	Privredna organizacija
EDU	Obrazovna institucija
GOV	Vladina institucija
MIL	Vojna grupacija
NET	Glavni centar za podršku u mreži
Zemlja/oznaka regiona	Pojedina zemlja/region

Znači kao zaključak gore izloženog: potpuno je svejedno da li pingamo simboličku adresu google.com (adresa danas najpopularnije pretraživačke mašine) ili 79.101.110.39 jer će DNS resolver prevesti simboličku adresu google.com u IP adresu 79.101.110.39 (Sl.6.7). Ovaj proces se odvija automatski.

Slika 6.7: *Prevođenja simboličkog imena u IP adresu preko DNS razrješavača*

Postoji centralna ustanova koja brine o IP adresama. To je InterNic (Internet Network Information Center). InterNIC je odgovoran za mrežu i registraciju domena. Samo provajderi i velike korporacije direktno konkurišu kod InterNIC za dobijanje IP adrese i domena. Sajt InterNIC-a je: http://www.internic.net .

6.1.3. Portovi i *socketi*

Za uspješan prenos podataka od izvora do odredišta potrebne su i fizička adresa i logička adresa.

Računari mogu istovremeno da izvršavaju više aplikacija. Potrebno je ostvariti komunikaciju između njih (Sl.6.8).

Računar A može da komunicira sa B koristeći Telnet, A može da komunicira i sa C koristeći FTP.

Da bi dvije aplikacije mogle da komuniciraju međusobno potrebno je da postoji metod pomoću kojih će se izvršiti njihovo obilježavanje. Uvodi se 16-bitni identifikacioni broj koji se naziva port, [48].

Na osnovu porta protokol transportnog nivoa može da utvrdi kojoj od aplikacija ili kom protokolu višeg nivoa treba da proslijedi pristigle poruke. Na ovaj način više aplikacija može koristiti usluge istog protokola transportnog nivoa, što se naziva multipleksiranje.

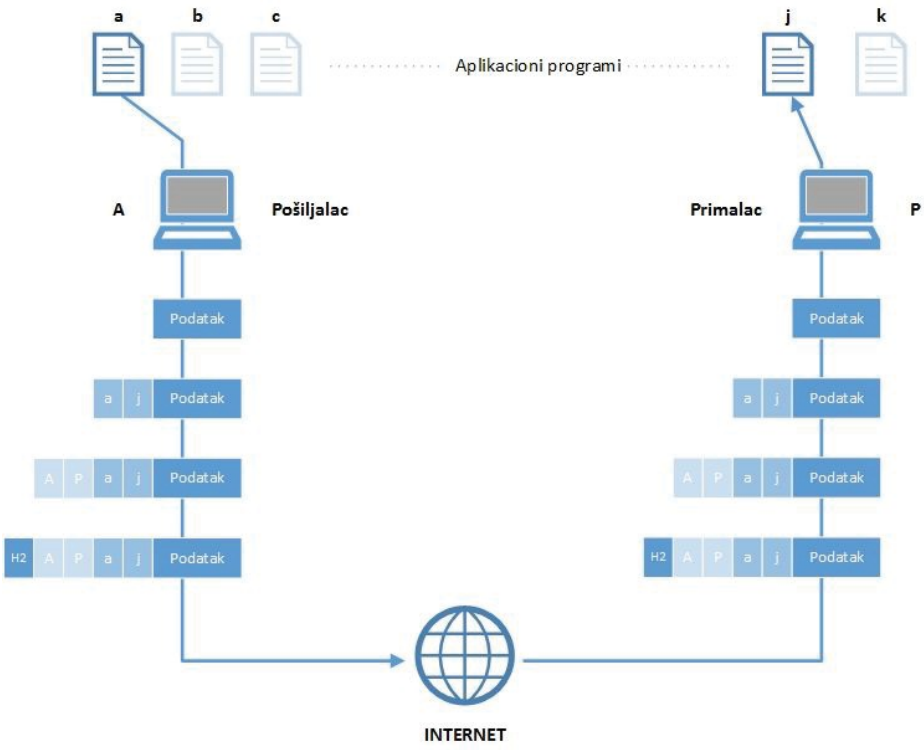
Za sve najčešće korištene aplikacije rezervisane su unaprijed neke vrijednosti portova, tako da ih klijent unaprijed zna kada se obraća određenom serveru.

Rezervisani portovi (well-known) definisani su u međunarodnim organizacijama. Portovi na strani klijenta se dinamički dodjelju, tj. uzima se prvi slobodan port iz skupa nezavisnih portova (1024-65535).

TCP i UDP koriste isti princip portova, ali se razlikovanje ova dva protokola vrši na osnovu polja protokola u IP zaglavlju.

IP adresa i port jednoznačno određuju jednu stranu u komunikaciji, kombinacija ova dva broja se naziva *socket*, [48].

Socket je interfejs između aplikacionog i transportnog nivoa unutar jednog računara. Često se za *socket* kaže da je API (Application Program Interface), tj. softverski interfejs između programa i Interneta. Povezivanje dva programa u potpunosti je opisano parom njihovih *socket*-a.



Slika 6.8: *Komunikacija između više aplikacija pokrenutih na istom računaru*

Na Sl.6.8 je prikazan način na koji dva računara komuniciraju preko Interneta. Računar predajnik istovremeno izvršava tri aplikacije, **a**, **b** i **c.** Računar prijemnik izvršava istovremeno dvije aplikacije čije su adrese **j** i **k**. Aplikacija **a** računara predajnika treba da komunicira sa aplikacijom **j** računara prijemnika. Iako oba računara koriste istu aplikaciju, FTP, port adrese se razlikuju, jer se jedna odnosi na klijent program, a druga na server program. Podaci se prenose od aplikacije **a** računara predajnika, ka aplikaciji **j** na strani prijemnika. Na transportnom nivou se vrši enkapsulacija podataka u paket koji pored Data polja sadrži i dvije port adrese **a** i **j**, dvije logičke adrese **A**i **P**.

6.1.4. Adrese specifične za određene aplikacije

Neke od aplikacija koriste dobro poznatu formu adresa koje se koriste kod specifičnih aplikacija. Tipični primjeri su adrese e-pošte, npr zvezdan@uns.ns.ac.rs, URL adrese, www.evropskiuniverzitet-brcko.com.

Prva adresa se koristi da definiše primaoca e-pošte i o njoj ćemo više reći u Poglavlju 7 kad budemo govorili o elektronskoj pošti, dok ćemo drugu ovdje ukratko objasniti.

URL (Universal Resourc Locator) adresa određuje bližu poziciju određenog dokumenta na nekoj Internet adresi.

URL adresa se sastoji od:

- protokola,
- adrese računara,
- porta,
- imena direktorijuma,
- imena same datoteke koju tražimo.

Primjer URL adrese:

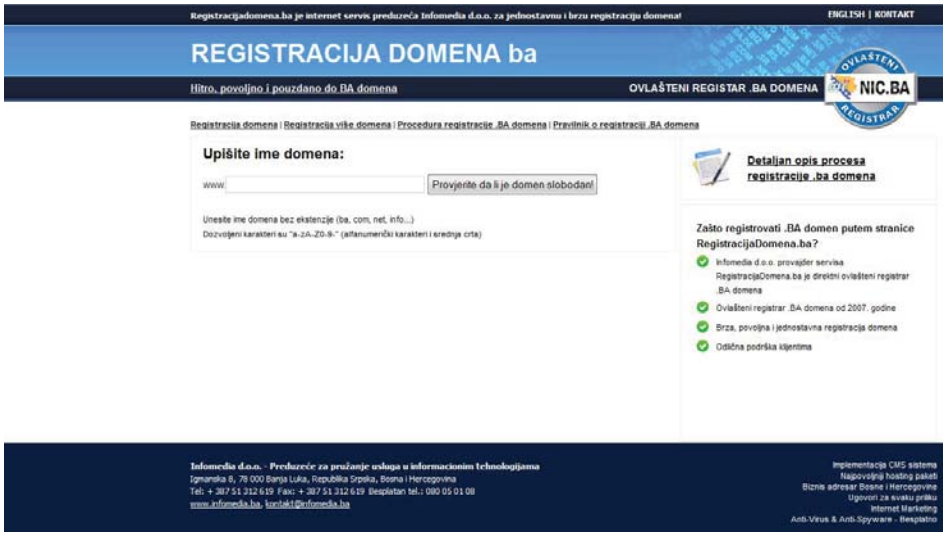
http://81.93.88.10:8080/fajlovi/dokumenti.doc

pri čemu je http iz gornje URL adrese oznaka protokola, 81.93.88.10 predstavlja adresu računara na kojoj se nalazi odgovarajući folder koji tražimo, 8080 port adresa koju koristi protokol http, fajlovi predstavljaju direktorijum u kojem se nalazi datoteka *dokumenti*.

6.2. Registracija imena domena

Poslovi pri registraciji domena:

- registracija domena,
- promjena podataka o registraciji domena,
- produženje registracije domena,
- prenos domena između ovlaštenih registara,
- prenos registracije domena,
- aktiviranje zaštite podataka o kontaktu za domen,
- prestanak (brisanje) domena.



Slika 6.9: *Primjer registracije domena*

Registraciju domena obavljaju firme zadužene za to. Recimo za BiH registracija top level domena **.ba** obavlja Infomedia (RegistracijaDomena.ba).

Na stranici RegistracijaDomena.ba se može provjeriti da li je željeni domen slobodan . Uobičajeni koraci prilikom registracije domena su dati na Sl.6.10.

Detaljan opis procesa registracije .ba domena — Zatvori ili pritisni Esc.

	Akcija	Vi	Mi	Nic	Detaljno	Vrijeme
Korak 1	Narudžba	☑			Popunite formu za registraciju domena	Odmah
Korak 2	Rezervacija		☑		Rezervišemo domen(e) i pošaljemo Vam dalja uputstva i predračun	Odmah
Korak 3	Dokumentacija i uplata	☑			Pošaljete tražena dokumenta po datom uputstvu i uplatite po datom predračunu	Zavisi od Vas
Korak 4	Aktivacija i slanje računa		☑	☑	Registar aktivira domen i mi Vam ga predamo i pošaljemo račun	1-2 radna dana

Slika 6.10: *Koraci pri registraciji domena*

POGLAVLJE 7

Internet servisi

Internet servisi, kao što su elektronska pošta, WWW, prenos datoteka i Telnet su već odavno našli široku primjenu u svakodnevnom životu čovjeka, ali uveliko imaju i poslovnu primjenu. Navedeni servisi, kako smo vidjeli u Poglavlju 1 su istorijski gledano i neki od najstarijih, ali još uvijek i najviše korištenih servisa Interneta. Pored njih u ovom poglavlju ćemo malo detaljnije objasniti i servise iz *triple play* koncepta o kojima smo govorili u Poglavlju 2, budući da je većina operatera kako u našoj zemlji, tako i okruženju, usvojila princip pružanja paketa servisa preko jedinstvenog mrežnog priključka. U ovom poglavlju ćemo objasniti i princip funkcionisanja virtuelnih privatnih mreža čijoj primjeni pribjegavaju velike kompanije u cilju povećanja efikasnosti poslovanja.

7.1. Telnet

Telnet je program koji omogućava da se direktno logujemo sa našeg računara (Telnet klijenta) na neki udaljeni računar (Telnet server) i da koristimo programe instalirane na tom računaru. Naš računar u tom slučaju služi samo kao terminal za udaljeni (host) računar. U ovom slučaju bi se sva obrada podataka obavljala na host računaru, dok bi kontrola rada bila sa terminala.

Da bismo se priključili na udaljeni računar, treba da imamo korisničko ime i lozinku na tom računaru. Kada smo se jednom ulogovali na udaljeni računar, onda možemo koristiti sve usluge koje su nam dozvoljene sa otvaranjem naloga. Računar sa kojeg smo se logovali izigrava neki tip terminala i ponekad je potrebno da izaberemo koji tip terminala emuliramo. Neki od raspoloživih tipova su recimo VT100 i VT220. Obično se kao default Telenet program koristi HyperTerminal koji se nalazi na putanji Accessories/Communications/HyperTerminal, [34], [90].

7.2. FTP

Ideja daljinskog prenosa datoteka uz upotrebu odgovarajućeg protokola predstavlja i samu suštinu Interneta. Čak je i zamisao o elektronskoj pošti nastala kasnije.

Protokol za prenos datoteka se označava sa FTP (File Transfer Protocol), dok se sajtovi sa kojih se mogu preuzeti datoteke nazivaju FTP sajtovima. FTP sajtovi se ne smiju poistovjetiti sa veb sajtovima koji predstavljaju drugačiji izvor podataka, [34], [40].

Neki su FTP sajtovi na Internetu privatni i pristup njihovim datotekama ograničen je na manji broj ovlaštenih korisnika, ali je daleko veći broj javnih FTP sajtova s datotekama kojima može pristupati načelno svaki korisnik Interneta (dakako, pod određenim finansijskim i drugim uslovima).

Kad se povežemo na računar koji nam omogućava prenos fajlova (FTP server), moguće je preuzeti informacije, grafike ili programe i smjestiti ih na naš računar. FTP nam takođe omogućava i da stavimo fajlove na FTP server kako bi oni bili dostupni i drugima. Sve vrste fajlova možemo preuzeti sa Interneta putem FTP servera. On se takođe koristi kako bi preuzeli novi softver kako bi poboljšali sposobnosti našeg računara.

Da bismo mogli da koristimo FTP, moramo imati korisničko ime (ID) na serveru (hostu) i lozinku. Nakon sprovedene autorizacije korisnik može slati datoteke sa svog računara ili ih primati sa FTP servera.

Internet Explorer se može povezati na FTP stranice na isti način kao kad se povezujemo sa veb sajtovima. U ovom slučaju URL (Uniform Resource Locator) počinje sa ftp://... umjesto sa http://...

Sa FTP sajtova na Internetu možemo da preuzmemo *shareware* i *freeware* programe. Autori *shareware* prezentuje ove programe na Internetu i bilo ko ih može preuzeti, instalirati i probati. Ovi programi nisu besplatni. Obično je dozvoljen neki probni period za njihovo korištenje ili je dozvoljeno preuzimanje neke nepotpune verzije softvera. Kad istekne određeni probni period, ako smo se odlučili da kupimo softver (da odgovorimo na zahtjev za registracijom) distributer softvera nam obično pošalje putem elektronske pošte elektronski ključ koji je potreban za aktiviranje softvera.

Na Internetu postoje takođe hiljade softverskih programa *freeware* koje je moguće preuzeti sa Interneta besplatno.

Ovdje ćemo definisati još dva pojma koji se često sreću a to su *download* i *upload***.** Preuzimanje fajlova (datoteka) sa udaljenog host računara se naziva *download***,** dok se slanje fajlova sa našeg računara na neki drugi naziva *upload***.**

Budući da ima jako mnogo fajlova koje možemo preuzeti (downloading) sa Interneta, koristi se Archie program koji ima namjenu da pregleda baze podataka na mreži u potrazi za traženom datotekom. Archie vrši pretragu po imenu fajla ili njegovom dijelu, a ne prema ključnim riječima ili opisu, [91].

FTP se pokreće na dva porta 20 i 21 i isključivo preko TCP-a.

Neke od komandi koje koristi FTP:

- **GET_ime-datoteke**: prenos sa udaljenog računara određene datoteke kojoj znamo ime,
- **PUT_ime-datoteke**: komanda kojom se šalje datoteka sa određenim imenom na udaljeni računar,
- **CLOSE**: kraj sesije sa udaljenim računarom,
- **OPEN**: otvaranje nove sesije,
- **BYE**: izlazak iz FTP programa.

Konačno, unazad nekoliko godina programi za daljinski prenos podataka ugrađuju se u tzv. veb čitače (Web Browser) iako se mogu koristiti i neki namjenski FTP programi, kao što su WS_FTP i CuteFTP za Windows operativni sistem ili NetFinder i Anatchie za Macintoch, [91].

Daljinski prenos datoteka može se koristiti u najrazličitije svrhe. Najčešće su, ipak, sledeće primjene:

- prenos binarnih datoteka između udaljenih računara,
- prenos tekstualnih (ASCII) datoteka između udaljenih računara,
- preuzimanje programa s udaljenih računara,
- prenos multimedijalnih datoteka (slike, video zapisa i zvuka).

Najveći je problem pronaći FTP sajt na kojem se nalazi tražena datoteka. Pri tome će od koristi biti različiti direktoriji FTP sajtova i njihovih sadržaja. U slučaju da se traže neke „uobičajene“, „popularne“ ili „opštepoznate“ datoteke, preporučuje se posjeta sledećem sajtu

http://tile.net/ftp-list/

U komplikovanijim slučajevima možda će od koristi biti informacije sistema *Archie*, u kojem se mogu naći informacije o milionima datoteka lociranih na računarima posvuda u svijetu.

http://archie.icm.edu.pl

7.3. Elektronska pošta

Danas elektronska pošta uz WWW predstavlja najznačajniji servis Interneta. Neki od razloga za to su:

- slanje poruke elektronskim putem na bilo koju lokaciju na svijetu nas košta mnogo manje nego da tu istu poruku, istog obima šaljemo nekad uobičajenim načinom (putem pisama i sl),
- bilo gdje da se nalazimo (na odmoru, poslovnom putu i sl), možemo pristupiti našem računaru kod kuće, odnosnu serveru našeg ISP-a i pročitati prispjele poruke; sve što nam je potrebno jeste telefonska linija i računar, a danas većina hotela i restorana omogućava svojim gostima pristup Internetu,
- poruka koju smo poslali na ovaj način stiže gotovo istovremeno na odredište.

Spomenut ćemo još i to da se pored slanja poruka lične prirode putem e-pošte može poslati i bilo koji drugi vid podataka sa kojima računar radi (slika, zvuk, video zapis, programi, i sl), s tim što ove podatke obično pridružujemo poruci kao dodatak (attachment), [90], [91].

Svi korisnici Interneta imaju svoju jedinstvenu adresu e-pošte. Ona se sastoji iz dva dijela: imena korisnika i imena domena. Dijelovi su međusobno odvojeni znakom @. Adrese su obično pisane malim slovima, a prilikom pisanja adrese ona se mora unijeti potpuno tačno, vodeći dakle računa i o veličini slova.

Prilikom izbora imena korisnika moguće je izabrati bilo koje ime koje nije već registrovano kod našeg ISP-a. Potom slijedi znak @, pa ime pružaoca Internet usluga. Treba napomenuti da ni u imenu korisnika niti u imenu davaoca usluge ne smije ostati prazan prostor. Stavljaju se tačke. Tačke u imenu davaoca usluge razdvajaju različite domene.

Komunikacija putem elektronske pošte na Internetu se može uspostaviti između bilo koja dva subjekta (pretplatnika) prijavljena kod nekog provajdera Internet usluga (ISP-a), koji im je dodijelio odgovarajuću adresu. Adrese su tipizirane (standardizirane) i jednoobrazne, bez obzira na to koji je provajder u pitanju, a sastoje se iz dva osnovna dijela:

ime@organizacija.područje

Primjer adrese e-pošte je:

zvezdan.stojanovic@spu.ba

Ime korisnika određuje korisnik proizvoljno. Oznake područja razlikuju se u SAD od onih u ostatku svijeta, pa se tako u SAD-u koriste sljedeće oznake:

- **com**–komercijalne i profitne organizacije,
- **org**–mješovite i neprofitne organizacije,
- **net**–internetska infrastruktura i davaoci internet usluga.
- **edu**–fakulteti,
- **gov**–federalne vladine agencije.

U ostalim dijelovima svijeta oznaka područja je ujedno oznaka zemlje u kojoj se korisnik registrovao za rad sa Internetom. Primjeri takvih oznaka su:

- **ba**–Bosna i Hercegovina,
- **rs**–Srbija,
- **at**–Austrija,
- **au**–Australija,
- **it**–Italija,
- **de**–Njemačka.

Postupak slanja elektronske pošte teče na sledeći način:

- korisnik pokreće svoj program za elektronsku poštu; svi standardni programi za elektronsku poštu podržavaju dva komunikaciona protokola i to POP (Post Office Protocol), kao protokol za primanje i pohranjivanje ulaznih poruka, te SMTP (Simple Mail Transport Protocol), kao protokol za distribuciju izlaznih poruka,
- program odmah pri aktiviranju dojavljuje korisniku ima li kakvih ulaznih poruka za njega,
- ako se u tzv „Inbox-u“ nalaze novopristigle poruke, korisnik ih može otvoriti ili pročitati; korisnik može odgovoriti na poruku(e) ili ih proslijediti nekome

drugom; korisnik može eventualno i memorisati poruke za koje misli da će mu trebati kasnije, a one nepotrebne briše,

- ako želi poslati nekome poruku one se smiještaju u „Outbox“.

Danas su najčešći programi za elektronsku poštu Microsoft Outlook i Outlook Express.

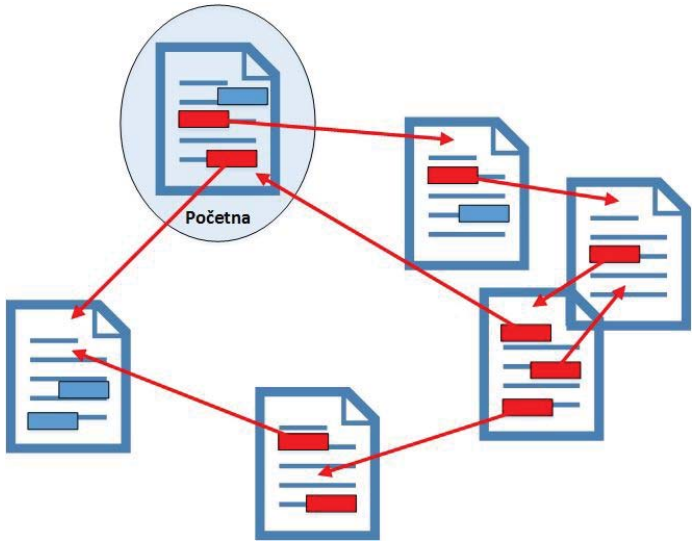
7.4. WWW

WWW (World Wide Web, u nastavku veb) predstavlja najpopularniji i najveći dio Interneta, sastavljan od miliona veb stranica koje svakodnevno posjećuju milioni korisnika širom svijeta.

Veb stranice se izrađuju pomoću HTML-a (Hypertext Markup Language) jezika. Veb se može uporediti sa nekom globalnom bibliotekom. U osnovi veb-a je hipertekst.

Def.: *Hipertekst je metod prezentovanja informacija gdje izabrane reči u tekstu imaju vezu (link) ka drugim informacijama tako da jednostavnim klikom tastera miša na neku od aktivnih riječi ili neki drugi objekat (najčešće sliku), možemo da se prebacujemo na lokacije na sasvim drugom kraju svijeta.*

Hipertekst integriše multimedijalne sadržaje u hipertekst dokument. Da bi smo se mogli kretati po vebu (surfing) potrebno je da imamo ostvarenu vezu sa Internetom (otvoren nalog kod našeg ISP-a) i potreban nam je veb čitač.



Slika 7.1: *Demonstracija hiperteksta*

Veb se zasnova na klijent/server modelu sa sledećim osobinama:

- URI (Uniform Resource Identifier): standard za predstavljanje resursa na Internetu,
- HTTP (Hypertext Transfer Protocol): standardni protokol za transfer podataka sličan FTP-u, ali se primarno koristi za prenos HTML dokumenata,
- HTML (HyperText Markup Language): jezik za pisanje prezentacija na vebu; danas postoji i niz drugih programa kao što su XML, Java, JavaScript, Visual Basic...

7.4.1. Jedinstveni identifikator resursa (URI)

URI predstavlja niz karaktera koji idenfifikuju putanju (URL-Uniform Resource Locator) ili imenuju resurs na internetu (URN-Uniform Resource Name), dakle URI se sastoji iz URL-a i URN-a. Osnovni cilj uvođenja URI-a jeste da se omogući interakcija između resursa na Internetu.

URL određuje bližu poziciju određenog dokumenta na nekoj Internet adresi.

Dijelove URL adrese smo vidjeli ranije, ali evo još jednog primjera. URL adresa se sastoji od:

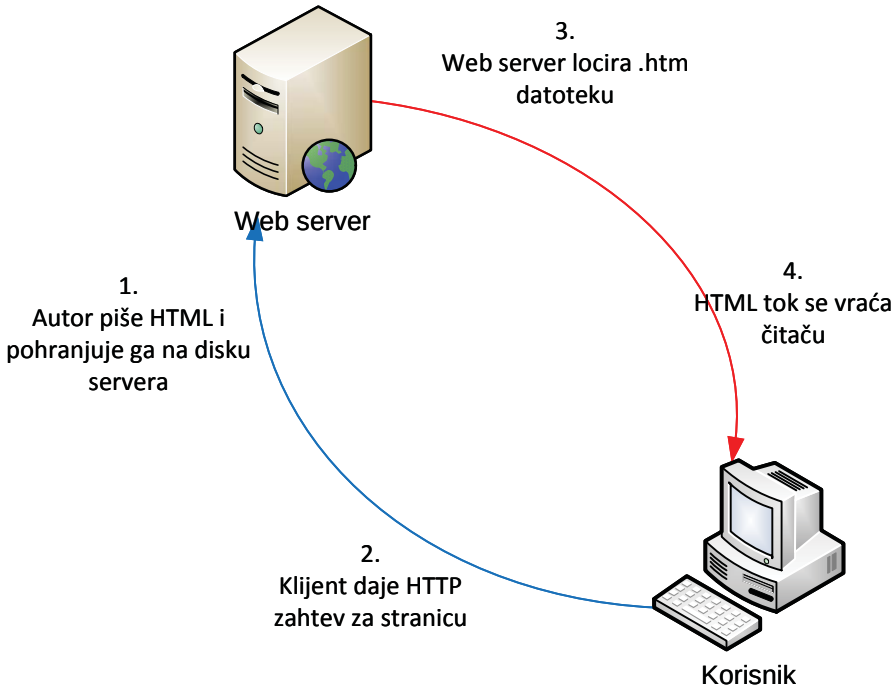
- imena protokola (npr http(s), ftp)
- adrese računara (www.evropskiuniverzitet-brcko.com)
- putanju do tražene datoteke (/Raspored/)
- ime same datoteke (Raspored_nastave.html)
- http://www.evropskiuiniverzitet-brcko.com/Raspored/raspored_nastava-html

URN određuje ime, odnosno identitet resursa na Internetu a tipičan primjer je ISBN (International Standard Book Number) sistem identifikovanja knjiga.

7.4.2. HTTP

HTTP predstavlja protokol za prenos informacija preko Interneta. HTTP definiše niz standardnih pravila za prezentaciju, signaliziranje, autentifikaciju i otklanjanje grešaka prilikom slanja informacija preko Interneta, [34].

HTTP funkcioniše po principu zahtjev/odgovor između klijenta i veb servera. Klijent generiše zahtjev koristeći veb čitač ka serveru koji kao odgovor šalje uskladišteni resurs, pri čemu je taj resurs fajl, ali to takođe može biti dinamički generisan rezultat upita, odnosno izlaz iz nekog CGI (Comom Gateway Interface) skripta.



Slika 7.2*: Komunikacija između klijenta i servera putem HTTP-a*

7.4.3. HTML

HTML služi za izradu statičkih veb stranica, što znači da se nisu uzimale u obzir informacije koje su pristigle od korisnika i na osnovu kojih bi se trebao generisati odgovor.

HTML se koristi za opis logičke strukture dokumenta. To se postiže kombinovanjem ključnih riječi, tagova (tags) i sadržaja koji treba da se prikaže.

Sadržaj se prikazuje pomoću čitača veba (brauzera) i od konkretnog brauzera zavisi konačan prikaz dokumenta.

Tag (privjezak, obilježje, marker, etiketa, ključna riječ, …) engleska riječ ili skraćenica ograđena „streličastim“ zagradama (<, >).

Primjer:

```
<html>
<head>
<title>Pozdravna poruka</title>
</head>
```

<body>Pozdrav svima!</body>
</html>

7.4.4. Veb čitači

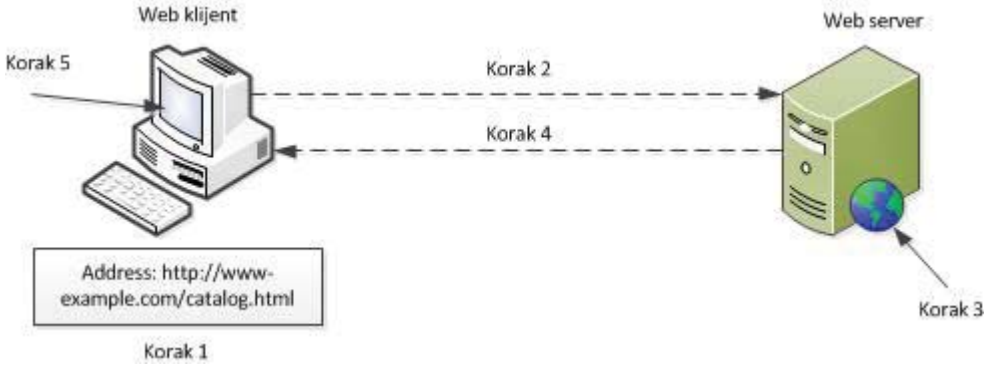
7.4.4.1. Princip rada veb čitača

Veb čitač (Web Browser) predstavlja program koji je instaliran i koji se pokreće na našem računaru i koji nam omogućava da pregledamo veb stranice.

Osnovni princip rada veb čitača jeste da čitač instaliran na našem računaru uspostavi komunikaciju sa informacionim serverom putem HTTP protokola, odnosno kreira se zahtjev za određenim resursom na serveru koji se može nalaziti bilo gdje na Internetu (Sl.7.3). Kao odgovor server šalje uskladištene resurse, pri čemu to mogu biti neke datoteke, ali i dinamički generisan rezultat upita kao rezultat rada nekog programa instaliranog na serveru (Sl.7.4).

Prilikom preuzimanja neke stranice sa Interneta uz upotrebu čitača uvijek dolazi do razmjene nekoliko poruka između našeg računara i drugog sa kojeg preuzimamo podatke.

Koraci prilikom preuzimanja nekog resursa uz upotrebu čitača sa veb servera na kome se nalazi instaliran PHP i koraci prilikom preuzimanja resursa bez primjene PHP se razlikuju što se može vidjeti sa Sl.7.3.



Slika 7.3*: Komunikacija između klijenta i servera bez upotrebe PHP-a*

Na strani servera se većinom koristi PHP (Personal Home Page) kao skript jezik za pisanje CGI skriptova, dok se na strani korisnika većinom koristi JavaScript.

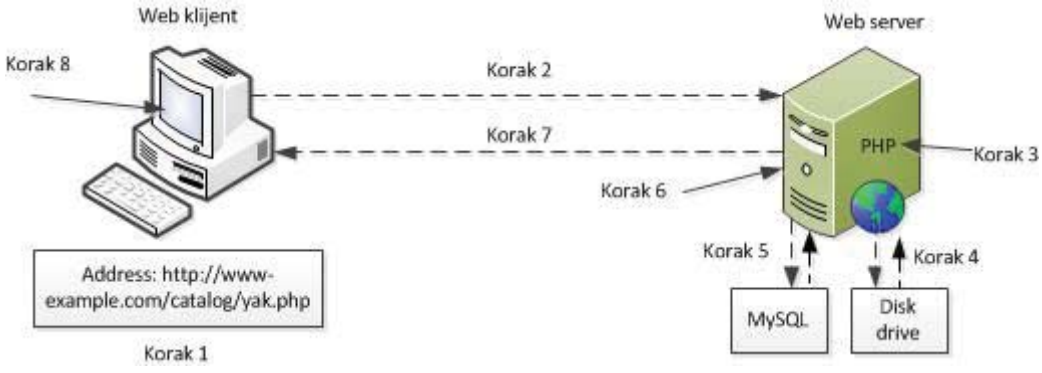
Objašnjenje koraka sa Sl.7.3:

1. Stavlja se adresa www.example.com/catalog.html u *address bar* čitača.
2. Čitač šalje poruku preko Interneta do računara sa imenom www.example.com (servera na kome je instaliran Apache program) i pita ga za stranicu /catalog.html.
3. Apache, program na www.examle.com računaru, dobija poruku i čita catalog.html datoteku sa diska.
4. Apač šalje sadržaj datoteke nazad do našeg računara preko Interneta kao odgovor na naš zahtjev.
5. Čitač prikazuje stranicu na ekranu.

U slučaju da je instaliran i neki CGI program (recimo PHP) i baza podataka (recimo MySQL) na serveru, potrebno je preduzeti još nekoliko dodatnih koraka.

Objašnjenje koraka sa Sl.7.4 (uz upotrebu PHP-a i MySQL-a):

1. Stavlja se www.example.com/catalog/yak.php u *address bar* čitača.
2. IE šalje poruku preko Interneta do računara sa imenom www.example.com i pita ga za stranicu /catalog/yak.php.
3. Apache, program na www.example.com računaru, dobija poruku i pita PHP-ov interpreter, dakle drugi program koji se pokreće na www.example.com računaru da mu iščita kod yak.php
4. PHP-ov interperter čita datoteku */catalog/yak.php* sa diska.
5. PHP interpreter pokreće komande u yak.php i moguće je razmjenjuje podatke sa programom baze podataka kakav je MySQL.
6. PHP-ov interpreter uzima yak.php program i šalje ga Apache serveru kao odgovor na njegovo pitanje „What does */catalog/yak.php* look like?“
7. Apache šalje sadržaj stranice koju je dobio od PHP interpretera nazad našem računaru kao odgovor na zahtjev IE-a.
8. IE prikazuje stranicu na ekranu.



Slika 7.4: *Komunikacija između klijenta i servera uz upotrebu PHP-a i MySQL-a*

U Tabeli 7.1 su dati najpopularniji veb čitači.

Tabela 7.1: *Najpopularniji veb čitači*

Čitač	Logo	Kratak opis
Internet Explorer		Internet Explorer predstavlja Microsoft-ov veb čitač. Pušten je u komercijalnu upotrebu 1995.
Firefox		Firefox predstavlja Mozilla-in veb čitač. Realizovan je 2004.
Google Chrome		Google Chrome je besplatan veb čitač koga je razvio Google. Realizovan je 2008.
Apple Safari		Ovo je default čitač za Mac operativne sisteme. Koristi se kod malih uređaja kao što su mobilni telefoni.
Opera		Opera je čitač koji je lansirala Norveška. Mali je i brz, u saglasnosti sa svim novim standardima i radi sa većinom operativnih sistema. Opera se smatra idealnim rješenjem za mobilne telefone i prenosive računare.
Mozilla		Čitači zasnovani na Mozilla kodu predstavljaju danas po brojnosti najbrojniju familiju čitača (budući da je i Firefox zasnovan na Mozilla kodu).
Netscape		Predstavlja prvi komercijalni veb čitač, pušten u rad 1994. Prestao se razvijati 2008. godine.

Procenat zastupljenosti gore najbrojanih čitača u Internet zajednici nije jednostavno utvrditi. Najrelevantniji pokazatelji su ipak pokazatelji onih firmi koje imaju najposjećenije veb stranice. Oni se razlikuju u svega nekoliko procenata, od jedne firme do druge, tako da su podaci navedeni u Tabeli 7.2. mogu smatrati relevantnim.

Tabela 7.2: *Statistike danas najpoznatijih čitača*

2013	Internet Explorer	Firefox	Chrome	Safari	Opera
Maj	12.6%	27.7%	52.9%	4.0%	1.6%
April	12.7%	27.9%	52.7%	4.0%	1.7%
Mart	13.0%	28.5%	51.7%	4.1%	1.8%
Februar	13.5%	29.6%	50.0%	4.1%	1.8%
Januar	14.3%	30.2%	48.4%	4.2%	1.9%

7.4.2. Mašine za pretraživanje

Danas postoji više miliona veb stranica i pretraživanje veba može da bude teško i dugotrajno. Pretraživanje veba možemo vršiti preko veb direktorija (srodnih tematskih područja) ili što je mnogo zastupljeniji slučaj, preko pretraživačkih mašina (search engines). Iako različiti programi za pretraživanje koriste različite tehnike za pretraživanje veba, većina radi na istim principima. Većina koristi *speader*-a, komad softvera koji neprekidno radi, kontaktira veb stranice i indeksira njihov sadržaj, [90].

U procesu indeksiranja se svakom dokumentu preuzetom pomoću *speader*-a dodjeljuje jedinstven identifikacioni broj, a sve riječi iz tog dokumenta se parsiranjem izdvajaju iz dokumenta i smještaju u tabelu Lexicon. Ako neka riječ ne postoji u Lexicon-u, ona se ubacuje u tabelu i dodjeljuje joj se jedinstveni ID. Kada korisnik unese neku riječ u polje za pretragu, prvo se provjerava sadržaj tabele Lexicon, tj da li ta riječ već postoji u tabeli, pa ako riječ ne postoji u tabeli korisniku se vraća kao odgovor na upit da ne postoji nijedan dokument sa zadanom riječi. Indeksiranjem se značajno ubrzava proces pretrage.

Svaka mašina za pretraživanje koristi različit kriterijum i nijedna ne može naći sve što se može naći na vebu. Da bi pronašli određenu informaciju potrebno je nekada konsultovati jedan ili više programa za pretraživanje.

Dva osnovna kriterijuma za pretragu su:

- prema ključnim riječima (keyword searching) i najbolji za ovu vrstu pretrage su Excite i Google;

- pretraga prema oblastima (Yahoo).

Tabela 7.3*: Najpoznatiji pretraživači*

Tip	Pretraživači	Kratak opis
Sve-namjenske pretraživačke mašine	Google	**Google** – Danas najpopularnija pretraživačka mašina.
	YAHOO! SEARCH	**Yahoo!Search**: Poslije Google-a najpopularnija pretraživačka mašina.
	Live Search	**Live Search** (ranije *Windows Live Search* i *MSN Search*) Microsoft-ova pretraživačka mašina napravljena kao konkurencija Google-u i Yahoo-uDolazi kao sastavni dio IE pretraživača.
E-mail	eMail-Search.org	**Email-Search.org**: sadrži brojne alate za traženje e-mail adrese.
	TEK TIME EQUALS KNOWLEDGE	**TEK search engine:** omogućava pretraživanje veba uz poznavanje samo e-mail-a.
Source Code	Google	**Google Codesearch:** traži javno dostupne kodove primjenom različitih kriterijuma.
	JavaScriptSearch.org	**JavaScriptSearch.org**: najbrži način za pronalaženje nekog JavaScrip koda.
	PHP Classes	**PHP Classes Repository:** najpoznatiji sajt koji se tiče PHP programskog jezika.

Novosti	Google news	**Google News:** za pretraživanje preko 4500 izvora informacija koji se neprekidno ažuriraju.
	topix	**Topix:** vrši kategorizaciju novosti po temama i geografskoj pripadnosti.
	YAHOO! NEWS	**Yahoo News**: za pronalaženje najnovijih novosti, aktuelnih priča iz svijeta politike, biznisa i slon top stories, world, business, politics...
Pronalazak osobe	Finding-People.com	**Finding-People.com**: najbolje mjesto za otpočinjanje potrage za nekim na Internetu.
Igre	Cheatsearch.org	**Cheatsearch.org**: moguće je pronaći šifre za gotovo sve igrice.
Posao	CV Fox	**CV Fox:** za prikupljanje CV-a na Internetu
	YAHOO! hotjobs	**Hot Jobs (Yahoo):** pronalaženje posta, poređenje zaradakod pojedinih poslodavaca i sl.
	monster	**Monster.com**: najveća svjetska baza podataka kratkih poslovnih biografija.
MultiMedia	YouTube Broadcast Yourself™	**YouTube:** najveći multimedijalni sajt.
	blinkx	**blinkx:** za pretraživanje preko 18 miliona sati video materijala.

Obrazovanje	THE COLLEGE SEARCH ENGINE	**The College Search Engine.com:** Pronalaženje veb sajtova univerziteta širom svijeta.
Nauka	SCIRUS	**Scirus:** najopsežniji za pronalaženje naučnih žurnala, časopisa, kurseva, patenata i sl.
Kupovina	Google product search	**Google Product Search:** (ranije Froogle) use Google to search for the best deals on products when you are shopping.
	msn shopping	**MSN Shopping:Comparison shopping made easy:** Nudi 33,155,627 proizvoda iz preko 8,000 prodavnica na jednom mjestu i preko 470 stranica savjeta prilikom kupovine koje trebaju pomoći da se napravi pravilan izbor.
	Shopping.com	**Shopping.com:** eBay-ov direktorijum za kupovinu.

Danas su najpoznatiji programi za pretraživanje na vebu Yahoo (http://www.yahoo.com) i Google (http://www.google.com). U Tabeli 7.3 su pored ova dva dati još neki programi za pretraživanje.

7.5. Korisničke diskusione grupe

Korisnička diskusiona grupa okuplja osobe sličnih interesovanja. Korisnik šalje ili prezentuje grupi svoje poruke koje po ozbiljnosti i sadržaju mogu varirati od gotovo beznačajnih sadržaja (viceva i anegdota), pa do ozbiljnih naučnih rasprava ili polemika. Korisnik može odgovarati na poruke koje je primio iz grupe pa može komunicirati sa milionima, najčešće nepoznatih ljudi širom svijeta, [90], [92].

Rasprava u diskusionim grupama nije ničim ograničena budući da većinom nema nikakvog posrednika ili moderatora koji bi je vodio u nekom smijeru. Međutim ponekad

diskusione grupe imaju moderatora (istina u znatno manjem broju slučajeva) čiji je zadatak da poslate poruke odobri prije slanja u grupu, da provjeri da li se one slažu tematski sa interesovanjem grupe u koju su poslate i sl.

Vrlo sličan servisu diskusionih grupa jeste servis razmjene novosti u grupi (Newsgroup Service). Suptilne razlike proizlaze iz karaktera poruka razmjenjivanih unutar grupe: u grupama za razmjenu novosti naglasak je na brzoj cirkulaciji što svježijih informacija, dok se klasične diskusione grupe bave temama koje pobuđuju trajni, ili barem dugoročni interes, pa su i poruke što se u njima razmjenjuju dugovječnije. Unutar diskusionih grupa razmjenjuju se, po pravilu, samo tekstualne informacije, a ne i multimedijalne, pa se za njihov prenos koristi i drugačiji komunikacioni protokol-NNTP (Network News Transport Protocol), a ne HTTP koji se koristi kod World Wide Web servisa. Zato se u stručnoj literaturi serveri diskusionih grupa često nazivaju i NNTP serverima.

Korisnici koji žele pristupati NNTP serverima moraju imati u svojim klijent računarima posebne namjenske programe (baš kao što ih, npr. moraju imati i za korištenje servisa elektronske pošte). Najpopularniji internet čitač, Microsoft Internet Explorer, ima ih već ugrađene u sebi kao opcije, ali postoje i različiti „samostalni“ programi te vrste, kao što su u Windows okruženju su WinVN, Gravity i Free Agent, dok su u klasi Macintosh računara njihov pandan programi NewsWatcher i Nuntius, [90], [92].

Servisi za razmjenu novosti u grupi su hijerarhijski organizovani. Krečući se slijeva nadesno, nizovi znakova označavaju sve uža i uža područja interesa. To je takozvano inkrementalno („korak po korak“) traženja grupe od interesa, pri čemu se specificiraju prvo najšire teme, koje se potom sve više i više „produbljuju“, do najnižeg nivoa (grupe vrlo uskih interesa). Tako, npr. adresa koja glasi **com.protocols.tcp-ip.dns** označava podgrupu korisnika zainteresovanih za razmjenu informacija o DNS protokolu, unutar grupe koja se bavi TCP/IP protokol stekom, odnosno unutar šire grupe koja se bavi računarskim protokolima, [90], [92].

Osnovne teme su sljedeće:

- **comp:** računari, informatika,
- **humanities:** društvene nauke, umjetnost, kultura,
- **misc:** teme koje nisu „pokrivene“ ostalim grupama, kao što su, npr., zapošljavanje,
- **news:** tematika vezana za Usenet grupe, administriranje, stvaranje novih grupa i sl.,
- **rec:** rekreacija, sport, hobby, muzika, igre,
- **sci**: nauka i tehnologija,
- **soc:** društvene teme i kultura,
- **talk:** diskusije, rasprave.

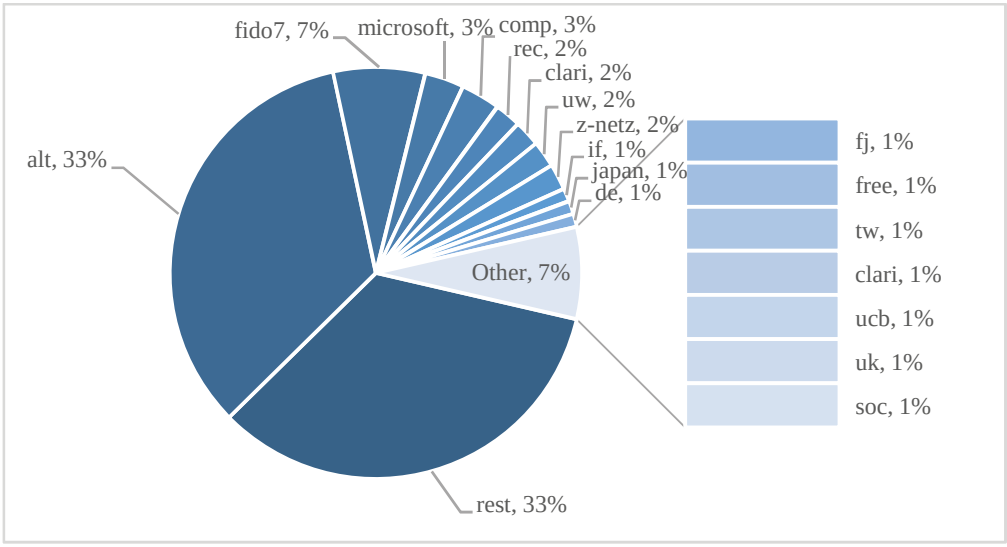
Prethodne nabrojane osnovne teme čine takozvanu veliku osmorku, ali danas postoje teme koje se takođe svrstavaju u prvi nivo hijerarhije, kao što su:

- **alt:** nekonvencionalne (alternativne) teme koje, uprkos raširenom pogrešnom uvjerenju, ne moraju biti nemoralne, nakaradne, opscesne, itd., nego zanimljive, često sasvim nove i neistražene,
- **bionet:** biologija,
- **fido:** stari BBS (Buliten Board System) sistemi,
- **gnu:** grupe za razmjenu besplatnih računarskih programa,
- **mag:** grupe za raspravu o časopisima.

Na Sl.7.5 je prikazan dijagram popularnosti pojedinih diskusionih grupa. Na slici možemo primijetiti i da se razne nacionalne hijerarhije nalaze na prvom nivou podjele:

- **de**: grupe za komunikaciju na njemačkom jeziku,
- **it**: grupe za komunikaciju na italijanskom jeziku,
- **fj**: grupe za komunikaciju na japanskom jeziku.

Mnogi korisnici mogu postavljati privremene diskusione grupe s tačno određenim ciljem- npr, pogađanja ishoda nekog sportskog događaja.



Slika 7.5*: Zastupljenost pojedinih diskusionih grupa prvog nivoa*

7.6. Ćaskanje

Ćaskanje (chat) se kao standardni internet servis razvilo iz elektronske pošte. Ostvaruje se na taj način što provajder usluge, koji se u ovom slučaju naziva IRC (Internet

Relay Chat), prihvata pozive korisnika koji žele stupiti u direktan (online) kontakt s nekim drugim, poznatim ili nepoznatim korisnikom, [90], [92].

Korisnici se prijavljuju IRC serveru, te navode neke informacije iz kojih se može zaključiti s kojim ili kakvim partnerom bi željeli komunicirati, o čemu, pod kojim uslovima itd. Zadatak IRC servera jeste da nastoji spojiti korisnike sličnih komunikacionih interesa.

Učesnici u čat sesiji komuniciraju na pisani način, slično kao u elektronskoj pošti, ali to čine u tzv. realnom vremenu, tj. u neposrednom dijalogu. Nakon prijema neke poruke odmah slijedi odgovor, pa odgovor na odgovor i tako do prekida veze.

S obzirom na broj učesnika u sesijama ćaskanja, razlikuju se dva modaliteta ćaskanja: grupni i privatni.

- u prvome slučaju IRC server okuplja korisnike prijavljene za uključivanje u sesiju u tzv.*chat room*, kao svojevrsnu ad hoc diskusionu grupu, u kojoj veći broj ljudi istovremeno priča (zapravo, piše na tastaturi),
- u određenom trenutku par učesnika u komunikaciji se može izdvojiti u privatnu čat sesiju i nastaviti razgovarati sasvim diskretno, neometano od drugih.

U svjetskim razmjerima firme America Online (AOL) i CompuServe organizuju najposjećenije čat sesije. Njihove adrese su:

www.aol.com/iwww.compuserve.com/

Upotrebom softverskih alata poput ICQ-a (I Seek You-tražim te) stvaraju se i održavaju liste osoba sa kojima često komuniciramo. Pomoću njih se može jednostavno utvrditi da li neka od tih osoba upravo aktivna na Internetu (i gdje), mogu se jednostavno pozvati, te provjeriti je li neko od njih zvao vas. Može se preuzeti sa adrese:

www.icq.com/

Noviji servisi Internet čatovanja omogućavaju i zvučnu (telefonsku), pa čak i video komunikaciju među partnerima u realnom vremenu.

Od opreme, osnovnoj je konfiguraciji računara potrebno dodati mikrofon, zvučnike i digitalnu videokameru. Neophodan softver za potrebe zvučne (telefonske) komunikacije, npr, u sistemu IPhone, može se preuzeti od firme VocalTecs sa Internet adrese

www.vocaltec.com/

Još sofisticiraniji sistemi „multimedijalnog čatovanja“, bilo u parovima (bilateralno) ili u obliku telekonferencije ili videokonferencije, dakle, multilateralno, ostvariv je, npr, uključivanjem u interaktivni sistem **CU-SeeMe** (što se izgovara kao: “See You, See Me”), razvijen na američkom univerzitetu Cornell. Detaljnije informacije o tom sistemu mogu se naći na adresi:

www.wpine.com/

7.7. VoIP

Iako se sam Internet zasniva na prenosu paketa podataka, pristup Internetu se i dalje u najvećoj mjeri zasnivao na postojećim javnim telefonskim mrežama (PSTN) i na primjeni modema, [9], [35], [44], [90].

Dva glavna nedostatka PSTN-a su:

- neefikasna upotreba resursa mreže, uspostava kanala konstantne širine propusnog opsega koji se daje jednoj konekciji za svo vrijeme trajanja poziva,
- visoki telefonski računi za individualne i poslovne korisnike.

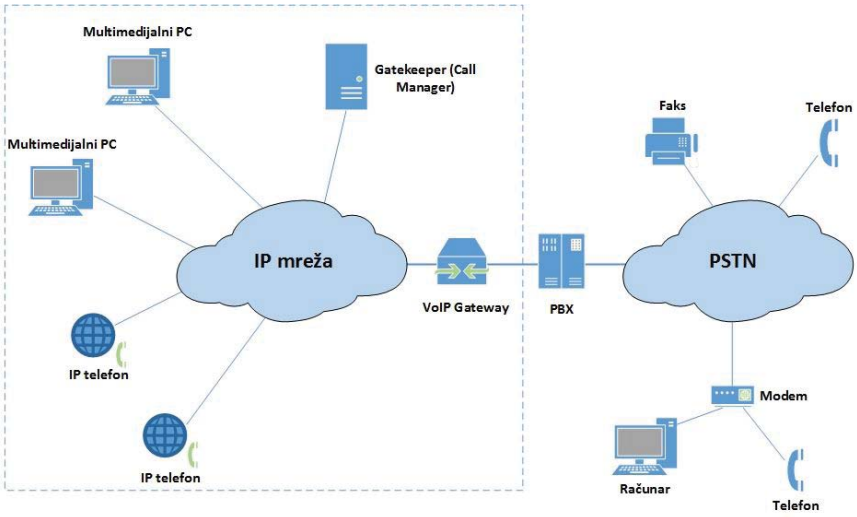
Mreže zasnovane na Internet protokolu (IP) nude rješenja za takve probleme i sve više se koriste kao alternativa za tradicionalne servise sa komutacijom kola. U literaturi se često ne pravi razlika između pojmova kao što su VoIP, Internet telefonija i IP telefonija. Na početku ćemo definisati sva tri pojma.

Def.: *Kad se privatna mreža (većinom WAN mreža), koja se zasniva na IP protokolu koristi za prenos govora, u zatvorenom mrežnom okruženju nekog operatera sa mogućnošću kontrolisanja kvaliteta (QoS-Quality of Service) kažemo da se radi o VoIP servisu.*

Def.: *Servis kod koga se vrši prenos govora preko otvorene mreže (Interneta) koja se zasniva na IP-u, u kojoj nema mogućnosti kontrolisanja kvaliteta (ne mogu se primijeniti algoritmi za sprečavanje i izbjegavanje zagušenja), usljed čega može doći do značajne degradacije kvaliteta prenošenog govora, se naziva Internet telefonijom.*

Def.: *IP telefonija predstavlja širi koncept u odnosu na VoIP i Internet telefoniju jer omogućava prenos govora, podataka i video signala, kako preko javne, tako i privatne mreže (obuhvata dakle i VoIP i Internet telefoniju), pa bi se moglo reći da ona dovodi do integracije mreža za prenos govora, videa i podataka.*

Međutim, ovdje ćemo se opredijeliti za analizu VoIP-a kao servisa iz *triple play* koncepta koji se pruža u zatvorenom mrežnom okruženju jednog operatera. Primjer arhitektura VoIP mreže je dat na Sl.7.6.



Slika 7.6: *Arhitektura VoIP mreže*

Sa Sl.7.6. se mogu vidjeti osnovni elementi arhitekture VoIP mreže (uz primjenu H.323 signalizacionog protokola):

- Internet mreža sa svim pripadajućim elementima (podmrežama i ruterima),
- javna telefonska mreža (PSTN) sa svojim prenosnim putevima i komutacionim čvorovima,
- mrežni prolazi (qateway),
- kontroleri mrežnih prolaza (gatekeeper),
- terminalni uređaju (PC računari, klasični i IP telefoni),

O nabrojanim komponentama mrežne arhitekture će biti više riječi u nastavku.

Da bi se govor koji je analogni signal, mogao prenijeti preko IP mreže, potrebno ga je prethodno obraditi. To se odvija u više koraka. Budući da se prenos VoIP-a odvija u zatvorenom mrežnom okruženju operatera koji garantuje kvalitet prenošenog signala (QoS) to prenošeni govor uz primjenu odgovarajućih algoritama ne bi smio izgubiti

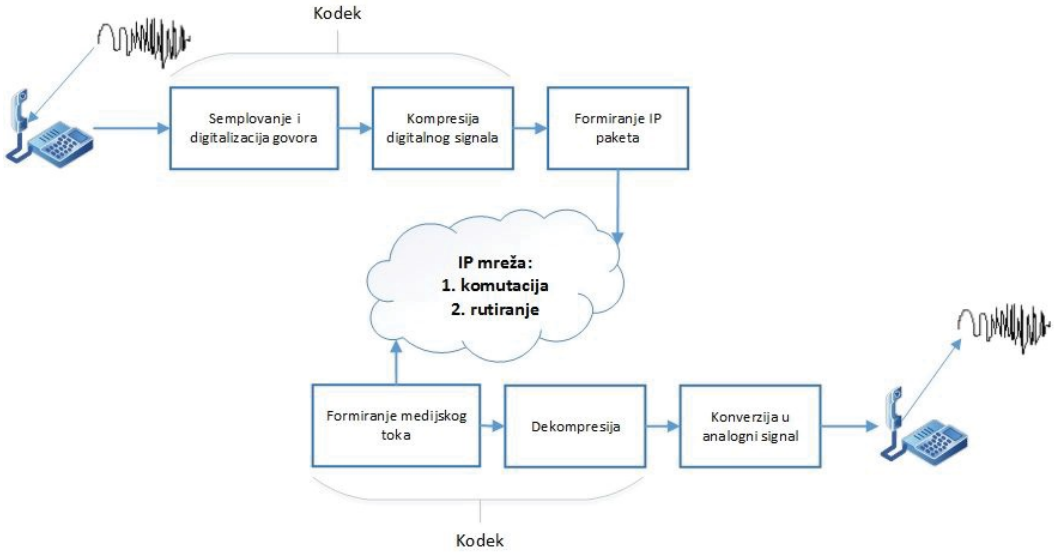
gotovo ništa na razumljivosti. Sada ćemo objasniti kako se vrši prenos govora putem IP mreže i koji sve faktori utiču na kvalitet VoIP poziva.

7.7.1. Faktori koji utiču na kvalitet govora

Na kvalitet VoIP poziva utiču mnogobrojni faktori kao što su: upotrebljeni govorni kodeci, paketizacija, gubitak paketa, kašnjenje, varijacija kašnjenja, raspoloživi propusni opseg, mrežna arhitektura koja treba da ispuni odgovarajuće zahtjeve za kvalitetom servisa (QoS), upotrebljeni CAC algoritmi (Call Admission Control), upotrebljeni signalizacioni protokoli ali treba voditi računa i o sigurnosnim aspektima, [35], [44].

7.7.1.1. Kodeci

Primarna funkcija kodeka jeste konverzija analognog signala u digitalni i obrnuto (Sl.7.7.). Kodeci takođe obezbjeđuju i kompresiju govora čime se redukuju zahtjevi za propusnim opsegom potrebnim za prenos preko digitalne mreže. Osnovni kompresioni algoritam jeste impulsna kodna modulacija (PCM-Pulse Code Modulation). Uvođenjem naprednijih kompresionih algoritama usložnjava se postupak obrade okvira, unosi dodatno kašnjenje pa samim tim i narušava kvalitet prenošenog govora. Govor se prenosi u realnom vremenu pa je jako osjetljiv na povećanje kašnjenja. Na Sl.7.7 je prikazan tok poziva sa jednog na drugi kraj veze.



Slika 7.7: *Tok VoIP poziva*

Mada VoIP uvodi prenos digitalizovanog govora u paketima, sam telefon na Sl.7.7 može biti ili analogni ili digitalni. Govor se može digitalizovati i kodovati prije ili tokom paketizacije. Zavisno od upotrebljene mreže, funkcije kodovanja i kompresije se mogu

obavljati u ruteru/mrežnom prolazu ako je u pitanju analogna mreža ili te funkcije može vršiti i sama digitalna centrala, [35], [44], [49].
Kvalitet govora za različite kodeke se obično mjeri subjektivnim testiranjem u kontrolisanim uslovima uz učešće većeg broja slušalaca i određivanjem subjektivne mjere za kvalitet različitih kodeka-MOS (Mean Opinion Score). Neki od faktora koji imaju najviše uticaja pri određivanju MOS-a za određene kodeke su: efekat šuma okoline, efekat degradacije kanala (gubitak paketa) i efekat transkodovanja (digitalno-digitalna konverzija) usljed rada sa drugim mrežama, kako žičnim tako i bežičnim. MOS je najveći za PCM i iznosi 4,1 a smanjuje se povećanjem složenosti algoritma kompresije (Tabela 4.4), tako da recimo za G.729 (CS-ACELP) iznosi 3,92 za G.723.r53 iznosi 3,65.

Bitska brzina PCM kodeka iznosi 64 kbit/s dok je za G.723.r53 svega 5,3 kbit/s (Tabela 4.4.). Dakle složeniji algoritam kompresije će zahtijevati manji propusni opseg, ali će za njih MOS biti manji. Nakon analogno-digitalne konverzije (Sl.7.7) formiraju se PCM odbirci koji se potom propuštaju do algoritma kompresije. Ovaj analizira blok PCM odbiraka koji može biti različite dužine zavisno od upotrijebljenog kodeka. Na primjer osnovna veličina rama za kodovanje kod G.729 algoritma iznosi 10ms, mada se mogu koristiti i oni od 20, 30, 40, 50 i 60 ms, dok je kod G.723 default vrijednost rama 30ms.

Tabela 7.4: *Najčešći kodni standardi i algoritmi kompresije govora*

Kodni standardi	Algoritam kompresije govora	Protok	Iznos MOS-a
G.711	PCM (Pulse Code Modulation)	64 Kbit/s	4,1
G.726	ADPCM (Adaptive Differential Pulse Code Modulation)	16, 24, 32	3,85
G.728	LDCELP (Low-Delay Code Excited Linear Prediction)	16	3,61
G.729	CS-ACELP (Conjugate Structure Algebraic Code Excited Linear Prediction)	8	3,92
G.729a	CS-ACELP	8	3,7
G.723.1	MP-MLQ (Multipulse Maximum-Linkelihood Quantization)	6,3	3,9
G.723.1	ACELP	5,3	3,65

Algoritmi kompresije omogućavaju efikasnije iskorišćenje propusnog opsega ali na račun dužeg vremena potrebnog za formiranje paketa i složenijih algoritama. Time se narušava kvalitet prenošenog govora kod VoIP-a. Dakle, potrebno je naći kompromis između efikasnije upotrebe propusnog opsega i povećanja kašnjenja, između kvaliteta govora i cijene propusnog opsega. Naime, što je veći propusni opseg kodeka, to je veća cijena prenosa svakog poziva kroz mrežu. Nejčešći kodni standardi i algoritmi kompresije govora su dati u Tabeli 7.4, [15], [35], [44], [49].

7.7.1.2. Gubitak rama

VoIP ramovi moraju putovati IP mrežom koja je nepouzdana. Okviri se mogu odbaciti usljed zagušenja mreže ili grešaka nastalih u prenosu podataka. Za saobraćaj u realnom vremenu, poput govora, retransmisija izgubljenih okvira nije praktična zbog dodatnih kašnjenja. Govorni terminali moraju raditi sa propuštenim govornim okvirima. Efekat gubitka govornih okvira (frame erasures) na kvalitet govora zavisi od toga kako će terminali rukuju sa njihovim gubitkom, [6], [35], [44].

Postoje različite tehnike koje se koriste u slučaju gubitka okvira:

- u najjednostavnijem slučaju, kad nedostaje okvir, terminal će ostaviti „džepove“ u govornom toku,
- ako je previše okvira izgubljeno, govor će postati nerazumljiv jer će nedostajati pojedini slogovi i riječi; u slučaju da nedostaje samo nekoliko okvira primijenit će se strategija ponavljanja prethodnog okvira,
- u slučaju da postoji više grešaka koristi se interpolacija; na osnovu prethodnih okvira dekoder će predvidjeti onaj koji nedostaje; ova tehnika je poznata kao tehnika prikrivanja izgubljenih paketa (PLC-Packet Loss Concealment); bafer pamti izvjestan broj prethodnih govornih okvira koji se potom koriste za generisanje sintetizovanog signala koji će popuniti „džep“;
- pošto je kod paketskih mreža gubitak paketa korelisan tako da u slučaju gubitka paketa neće biti izgubljen samo jedan paket već nekoliko uzastopnih, učešljavanjem (interleaving-om) govornih okvira može se smanjiti ovaj efekat, ali se time povećava kašnjenje jer je potrebno skupiti nekoliko okvira da bi bili učešljani.

7.7.1.3. Kašnjenje i varijacija kašnjenja

Prilikom prenosa paketizovanog govora, na njegov kvalitet uveliko utiče i kašnjenje. Neki izvori kašnjenja se mogu unaprijed predvidjeti, dok su drugi promjenjive prirode i ne mogu se unaprijed predvidjeti (Sl.7.8), [6], [15], [35], [44].

Fiksni izvori kašnjenja su:

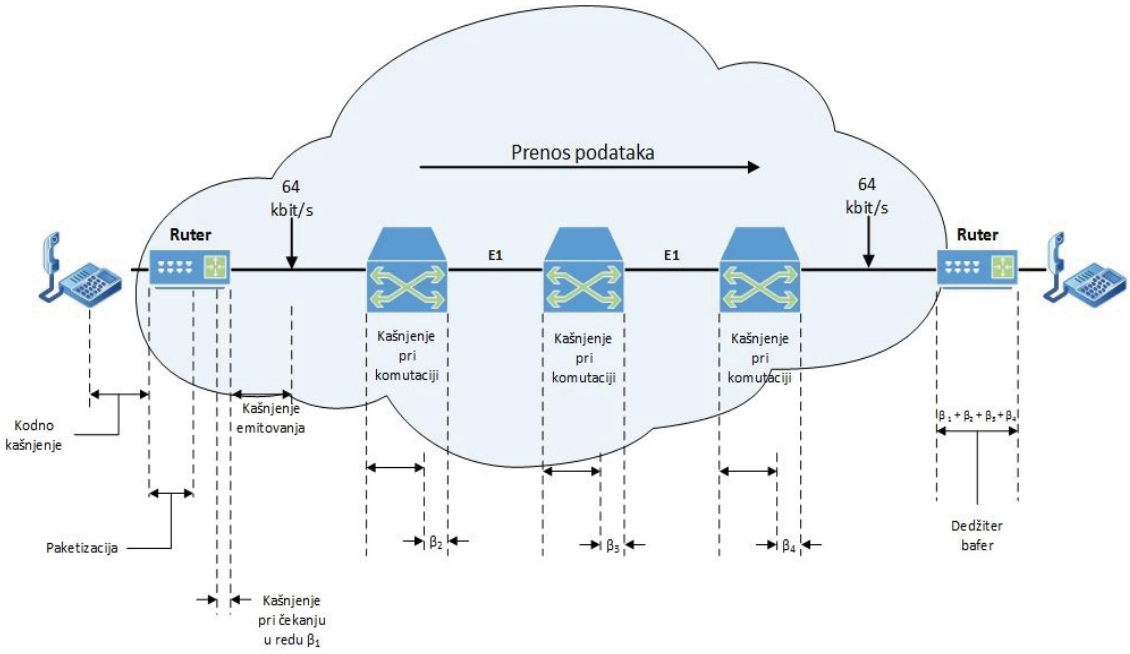
- paketizacija: vrijeme koje je potrebno za popunjavanje korisnog (payload) dijela paketa sa kodovanim/komprimovanim govorom; govorni odbirci se obično prvo akumuliraju prije njihovog stavljanja u prenosni ram radi smanjenja iznosa zaglavlja; RFC 1890 specificira da je period paketizacije 20 ms; za G.711 to znači da će se 160 odbiraka prvo akumulirati i prenijeti u jednom ramu,
- kodno kašnjenje: to je vrijeme koje je potrebno DSP (Digital Signal Processor) da koduje jedan ili više govornih odbiraka; ovdje pod kodovanjem podrazumijevamo A/D konverziju i kompresiju bloka PCM govornih odbiraka određenim kodnim algoritmom; u Tabeli 7.5 date su vrijednosti kodnih kašnjenja kod pojedinih kodnih standarda,
- kašnjenje pri emitovanje (serialization delay): kašnjenje na mrežnim interfejsima; to je vrijeme u kojem ruter analizira zaglavlje govornog paketa, pretražuje tabelu rutiranja i prosleđuje paket na odgovarajući izlazni interfejs,
- propagacija: ovo je vrijeme koje je potrebno električnom ili optičkom signalu da pređe prenosni medijum i u funkciji je geografske udaljenosti; kašnjenje usljed propagacije u kablu je 4 do 6 μs po kilometru; za satelitske komunikacije kašnjenje je 110ms za satelit koji se nalazi na visini od 14000 km i 260 ms za satelit koji se nalazi na visini od 36000 km.

Tabela 7.5*:Kodno kašnjenje za različite kodne standarde*

Kodni standardi	Bitska brzina kodeka (kbit/s)	Interval semplovanja kodeka (ms)	Najbolji slučaj kodnog kašnjenja (ms)	Najlošiji slučaj kodnog kašnjenja (ms)
ADPCM G.726	32,0	10	2,5	10
CS-ACELP G.792A	8,0	10	2,5	10
MP-MLQ G.723.1	6,3	30	5	20
MP-ACELP G.723.1	5,3	30	5	20

Promjenjivi izvori kašnjenja:

- kašnjenje usljed komutacije kroz mrežu β_n:
  - kašnjenje u posredničkim uređajima (centralama, svičevima, ruterima),
  - kašnjenje pri čekanju u redu na obradu u mrežnim baferima (prihvatnicima).



Slika 7.8*: Izvori kašnjenja u VoIP mreži*

Varijacija u vremenu dolaska paketa (džiter), nastaje kao posljedica različitog prenosnog kašnjenja kroz mrežu. Prenosno kašnjenje nastaje zbog vremena provedenog u čekanju u redu i vremena obrade koje može varirati zavisno od ukupnog opterećenja u mreži; čak i ako izvorni mrežni prolaz (gateway) generiše govorne okvire u regularnim vremenskim intervalima (recimo svakih 20 ms), odredišni mrežni prolaz neće primiti okvire u regularnim vremenskim intervalima zbog džitera, [35], [42], [44].

Džiter će dovesti do džepova u ulaznom toku podataka. Generalna strategija pri radu sa džiterom je da se dolazni okviri drže u baferu za amortizaciju kašnjenja (playout*)* baferu tako dugo dok i najsporiji okvir ne dođe, u vremenu u kojem je moguće korektno izvesti sekvencu. Što je veći džiter, duže će se neki okviri držati u baferu što opet povećava kašnjenje. Da bi se minimiziralo kašnjenje usljed baferovanja, većinom se koristi adaptivni bafer. Drugim riječima, ako je iznos džitera u mreži mali, veličina bafera će biti mala. Može se procijeniti veličina de-džiter bafera kao zbir svih kašnjenja β_n , tj $\beta_1+\beta_2+\beta_3+\beta_4$.

Ako džiter poraste uslijed povećanja mrežnog opterećenja, veličina bafera će automatski narasti kako bi se kompenzirao porast džitera. Džiter u mreži će pogoršati kvalitet govora srazmjerno povećanju kašnjenje usljed bafera za amortizaciju kašnjenja. Ponekad, kad je džiter preveliki, bafer za amortizaciju kašnjenja može da dozvoli gubitak nekih okvira kako kašnjenje ne bi postalo preveliko, [6].

Kao posljedica kašnjenja dolazi do degradacije i pogoršanja kvaliteta prenošenog govora. Kao posljedica degradacije kvaliteta govora uzrokovano kašnjenjem nastaje efekat eha. Eho nastaje uslijed lošije veze između slušalice i zvučnika u telefonskom aparatu. Ovo se naziva akustičnim ehom. On može nastati i kao posljedica refleksije signala na hibridnom kolu pri prelasku sa četvorožičnog na dvožični prenos na interfejsima klasičnih TDM (Time Division Multiplexing) centrala. Ovo je poznato kao hibridni eho.

Ako je jednosmijerno kašnjenje sa kraja na kraj veze malo, koji god eho da je u pitanju, on će se tako brzo vratiti govorniku da se neće ni primijetiti. Suzbijanje eha nije potrebno ako je jednosmijerno kašnjenje manje od 25ms. Međutim, ovo kašnjenje je u većini slučajeva veće od 25 ms pa je potiskivanje eha potrebno.

Čak i pri besprijekornom potiskivanju eha, prenošenje dvosmijernog razgovora postaje otežano kad je kašnjenje previše dugo zbog preklapanja govornika (talker overlap-a). Ovo je problem koji se dešava kad jedna strana prekida razgovor drugoj strani zbog prevelikog kašnjenja.

ITU-T preporukom G.114 je definisana granica jednosmijernog kašnjenja (uz kontrolisan eho prema G.131) i to:

- 0-150 ms je prihvatljivo za većinu korisnika;
- 150-400 ms prihvatljivo za međunarodne veze;
- veće od 400ms neprihvatljivo u većini slučajeva.

7.7.2. Protokoli VoIP-a

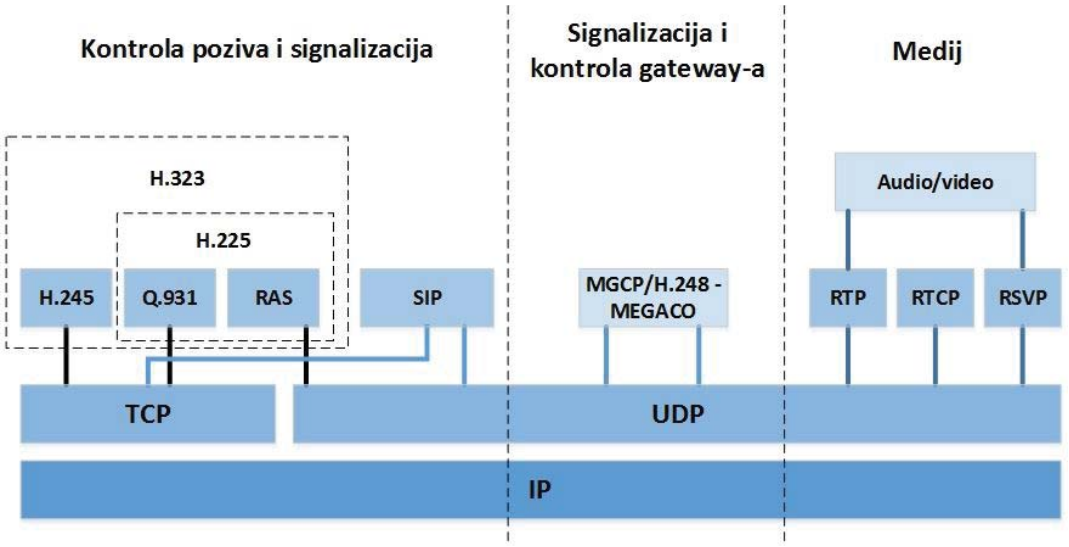
Na Sl.7.9. dat je pregled najznačajnijih protokola koji se koriste kod VoIP-a.

H.323 verzija 1 i 2 podržavaju H.245 preko TCP-a, Q.931 preko TCP-a i RAS preko UDP-a, [34].

H.323 verzija 3 i 4 podržavaju H.245 preko TCP/UDP-a, Q.931 preko TCP/UDP-a i RAS preko UDP-a.

SIP podržava i TCP i UDP.

H.323 predstavlja složen protokol koji je sastavljen od čitavog skupa protokola, ali su na slici predstavljena samo tri koji zajedno imaju približno istu funkciju kao SIP.



Slika 7.9: *Pregled najznačajnijih protokola koji se koriste kod VoIP-a*

7.7.3. Protokoli transportnog nivoa

Protokole transportnog nivoa smo već razmatrali u Poglavlju 5. Takođe smo rekli i da se kao transportni protokol kod VoIP koristi UDP. UDP se u većini slučajeva koristi zajedno sa RTP-om (Real Time Transport Protocol) o kome ćemo sada nešto više reći.

RTP obezbjeđuje prenosne funkcije sa kraja na kraj mreže za aplikacije koje prenose vremenski osjetljive podatke, kao što su audio i video. RTP omogućava prijemniku da detektuje gubitak paketa i da ih u izvjesnoj mjeri ispravi, omogućava kompenzaciju džitera, dinamičku promjenu prenosne brzine zavisno od uslova u mreži (promjenom kodeka), sinhronizaciju multimedijalnih tokova podataka. RTP ne vrši rezervaciju resursa i ne garantuje kvalitet servisa. RTP ne može spriječiti dolazak paketa na odredište u različitom redoslijedu u odnosu na poslati (out-of-sequence). RTP ne može spriječiti ni zagušenje mreže, [26], [34].

RTP se može koristiti sa bilo kojim prenosnim protokolom, mada se u praksi većinom koristi sa UDP protokolom.

Kontrolni dio RTP-a, RTCP (Real Time Control Protocol), omogućava nadzor linka podataka. RTCP pruža informaciju o kvalitetu servisa koji su obezbijeđeni preko RTP-a. RTCP skuplja statistike o medijskoj konekciji i informacije o primljenim i poslatim bajtovima, izgubljenim paketima, džiteru, kružnom kašnjenju. Aplikacije koriste ove informacije radi povećanja kvaliteta servisa, recimo upotrebom kodeka sa manjim stepenom kompresije, umjesto onih sa velikim stepenom kompresije.

7.7.4. Signalizacioni protokoli VoIP-a

Osnovni zadatak signalizacije je da omogući prenos potrebnih informacija kroz mrežu (bilo da je u pitanju IP mreža ili PSTN) u cilju pravilnog uspostavljanja, kontrole i raskidanja veza između pretplatnika, kao i za upravljanje mrežom. Signalizacija je u tijesnoj vezi sa prenosom podataka, ali prenos podataka nije dio signalizacionog protokola. Trenutno postoje dva standardizovana signalizaciona protokola za VoIP:

- H.323 kojeg je razvio ITU-T (International Telecommunications Union Telestandardization Sector),
- SIP (Session Initiation Protocol) je razvio IETF (Internet Engineering Task Force); ova dva protokola predstavljaju različite pristupe istom problemu: signalizaciji i kontroli multimedijalnih konferencija.

Često se u kombinaciji sa njima, ili samostalno koristi i MGCP/MEGACO (Media Gateway Control Protocol/Media Gateway Controller), ali će naše razmatranje biti skoncentrisno na SIP i H.323.

Tokom poslednjih godina porasla je popularnost SIP-a budući da ga je i 3GPP (Third Generation Partnership Project) izabrao za upotrebu u trećoj generaciji mobilnih mreža pa je za očekivati da će SIP dominirati u VoIP-u.

H.323 i SIP imaju približno istu mrežnu arhitekturu.

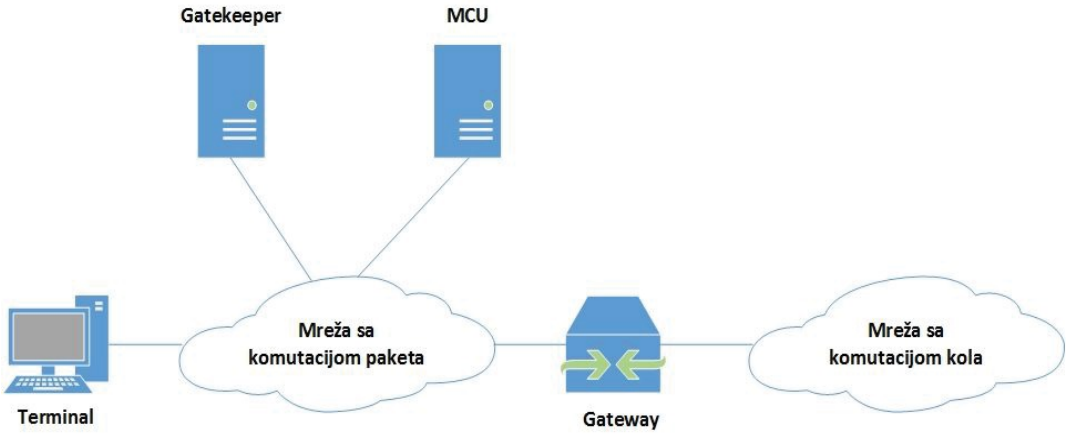
Kod H.323 protokola definišu se četiri tipa entiteta: terminali, kontroleri mrežnog prolaza (gatekeeper), mrežni prolazi (gateway) i MCU (Multipoint Control Unit).

SIP definiše sledeće entitete: korisničke agente (User Agent), servere za preusmjeravanje (Redirect Server), *proxy* servere i registracione servere (Registrar Server). Ovdje se mrežni prolazi razmatraju kao specijalni slučaj korisničkih agenata. Osnovna konfiguracija i kod H.323 i SIP-a se sastoji od najmanje dva terminala povezana na LAN. Međutim, u praktičnim aplikacijama neophodno je dodati neke druge entitete kako bismo dobili efikasni komunikacioni sistem koji se tada vezuje na vanjski svijet. Svaki entitet donosi više funkcionalnosti mreži.

7.7.4.1. H.323

Na Sl.7.10 dati su osnovni elementi H.323 mreže. Terminali, ili korisnički agenti, su krajnje tačke u komunikaciji sposobne da generišu i primaju bidirekcione informacione tokove u realnom vremenu. I kod H.323 i SIP protokola, terminali moraju podržati govorne komunikacije, dok su video i komunikacije podataka opcione. H.323 terminal se može implementirati kao programska aplikacija na računaru (Microsoft NetMeeting) ili kao samostalni uređaj (telefon). H.323 terminal je mrežni element koji omogućava dvosmijernu govornu, video i komunikaciju podatka sa drugim H.323 terminalima, sa

mrežnim prolazom ili MCU (Multipoint Control Unit) jedinicom razmjenjujući sa njima poruke protokola H.225 CS i H.245 dok sa kontrolorom mrežnih prolaza razmjenjuje i H.225.0-RAS poruke, [34], [90].



Slika 7.10*: Komponente H.323 protokola*

Mrežni prolazi obezbjeđuju dvosmijernu komunikaciju u realnom vremenu između H.323 terminala na IP mreži i drugih ITU terminala u mrežama sa komutacijom kola ili drugim H.323 mrežnim prolazima. Oni služe kao prevodioci, tj. omogućavaju prevođenje između različitih prenosnih formata, npr. sa H.225 na H.221. Mrežni prolazi su interfejsi između PSTN-a i Interneta. Oni su sposobni da vrše prevođenje između audio i video kodeka. Na primjer u PSTN mreži se uglavnom koristi G.711, dok se kod H.323 mogu koristiti različiti algoritmi kompresije (G.711, G.729, G.723,...). Mrežni prolaz vrši prevođenje između signalizacionih protokola koje se koriste u H.323 mreži i onih koji se koriste na PSTN mreži. U jednoj LAN mreži, mrežni prolazi nisu potrebni jer tu terminali mogu direktno međusobno komunicirati, međutim, za komunikaciju sa krajnjim tačkama na nekoj drugoj mreži, potrebni su mrežni prolazi koji koriste H.245 i Q.931 protokol.

Kontrolori mrežnih prolaza kod H.323 i serveri kod SIP-a imaju slične funkcije. Oni obezbjeđuju servise rutiranja, sigurnosne servise i kontrolu saobraćaja na mreži preko kontrole pristupa i održavanja propusnog opsega.

H.323 mreža je podijeljena u zone. Zona je skup svih terminala, mrežnih prolaza i MCU-a, koje opslužuje jedan kontrolor mrežnog prolaza. Pozivi između zona zahtijevaju upotrebu nekoliko kontrolora mrežnih prolaza. Neke od funkcija kontrolora mrežnih prolaza su:

- prevođenje adrese: vrši prevođenje alias adrese[1]; ovo se radi upotrebom tabele prevođenja koja se ažurira uz upotrebu registracionih poruka,
- kontrola pristupa: može dozvoliti ili zabraniti poziv na osnovu autorizacije poziva, adrese izvora i odredišta ili preko nekog drugog kriterijuma,
- signalizaciju poziva: kontrolor mrežnog prolaza može sam kompletirati signalizaciju poziva sa krajnjim tačkama,
- autorizacija poziva: može zabraniti, tokom određenog perioda vremena pozive do/od određenih terminala ili mrežnih prolaza upotrebom H.225 signalizacije,
- kontrola iskorištenja propusnog opsega: kontroliše broj H.323 terminala koji mogu istovremeno da pristupe mreži; upotrebom H.225 signalizacije mogu se zabraniti pozivi od određenih terminala usljed ograničenja propusnog opsega,
- tarifiranje poziva: kontrolor mrežnog prolaza vrši memorisanje informacija o ostvarenim pozivima u svrhu naplate usluge.

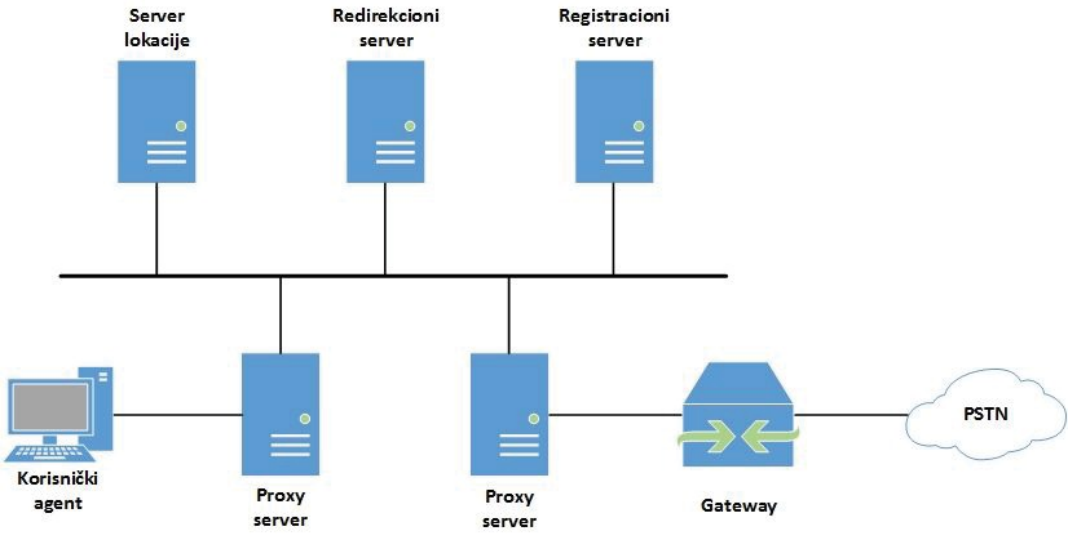
MCU omogućava da tri ili više terminala ili mrežna prolaza učestvuju u konferenciji sa više učesnika. Obavezna komponenta MCU-a jeste Multipoint Controller (MC), dok je opciona Multipoint Procesor (MP). MC je logički element, koji spaja signalizacione kanale i kanale za nadzor konferencije tri i više terminala i mrežna prolaza u topologiju zvijezde. MC određuje moguće načine komunikacije između terminala te na taj način upravlja izborom konferencije i načina komunikacije. MP je logički element čija je uloga u konferencijama spajanje govornih, video i tokova podataka primljenih od različitih terminala i vraćanje multipleksiranog toka terminalima koji učestvuju u konferenciji.

7.7.4.2. SIP

SIP je kontrolni (signalizacioni) protokol aplikacionog nivoa koji omogućava kreiranje, modifikovanje i završavanje sesija sa jednim ili više učesnika. Ove sesije mogu uključivati multimedijalne Internet konferencije, telefonske pozive preko Interneta i distribuciju multimedija. U SIP pozivu se prenosi opis sesije što omogućava učesnicima u sesiji da se usaglase oko kompatibilnih medijskih tipova, [90].

SIP podržava mobilnost korisnika i zahtjevi se usmjeravaju prema trenutnoj lokaciji korisnika preko posredničkog (proxy) i redirekcionog servera. Korisnici registruju svoju trenutnu lokaciju kod servera za registraciju korisnika (Registrar Server). SIP nije povezan ni sa jednim posebnim konferencijskim protokolom. SIP je konstruisan tako da bude nezavisan od protokola prenosnog nivoa i da se može proširivati dodatnim osobinama.

[1]Alias adresa pruža alternativan metod za adresiranje krajnje tačke. To može biti e-mail adresa ili telefonski broj. Krajnja tačka može imati jednu ili više alias adresa koje su jedinstvene unutar zone.



Slika 7.11*: Komponente SIP protokola*

Komponente opisane arhitekture sa Sl.7.11 su:

- korisnički agenti:
  - *User Agent Clients* (UAC): entitet koji inicira poziv;
  - *User Agent Server* (UAS): entitet koji prima poziv;
  - I UAC i UAS mogu završiti poziv.
- server lokacije (Location Server): pruža informacije o mogućoj lokaciji pozvane strane;
- posrednički (Proxy) server: posrednički uređaj koji prima SIP zahtjeve od klijenata i prosleđuje ih drugim uređajima; zahtjevi se servisiraju interno ili se propuštaju do drugih servera; posrednički server može obezbijediti takve funkcije kao što su autentifikacija, autorizacija, pristupna kontrola mreži, pouzdana retransmisija zahtjeva i sigurnost,
- server za preusmjeravanje poziva (Redirect Server): daje informacije klijentu o narednom koraku ili koracima na putu poruke i tada klijent kontaktira server u narenom koraku ili UAS direktno,
- server za registraciju korisnika (Registrar Server), obrađuje zahtjeve koji su pristigli od UAC-a za registraciju njihove trenutne lokacije; smiješta se zajedno sa posredničkim i serverom za preusmjeravanje poziva.

SIP treba da obezbijedi sledeće servise:

- određivanje lokacije krajnje tačke komunikacije,
- koristi SDP (Session Description Protocol) kako bi drugoj strani u komunikaciji saopštio koju vrstu medija prva strana želi da primi (audio, video ili oba), tako da druga strana koduje medijum kako bi prva razumjela šta je poslato i potrebno je

drugu stranu u komunikaciji informisati o adresi i portu gdje želi da se medij isporuči [34],,

- određivanje raspoloživosti krajnje tačke: ako se poziv ne može uspostaviti zato što krajnja tačka nije na raspolaganju, SIP treba da odredi da li je pozvana strana nedostupna zato što je već uspostavila komunikaciju sa nekim ili se nije javila nakon određenog broja pokušaja (zvučnih signala); tada se vraća poruka koja ukazuje na to da krajnja tačka nije na raspolaganju,
- uspostava sesije između početne i krajnje tačke: ako se poziv može kompletirati, SIP uspostavlja sesiju između krajnjih tačaka; SIP takođe podržava i promjene u toku poziva kao što je dodavanje još korisnika u konferenciju ili promjena medijskih karakteristika i kodeka,
- rukovanje prenosom i završavanjem poziva,
- sigurnosni mehanizmi: sprečavanje ometanja pružanja usluge (denial-of-service prevention), proces identifikacije (authentication), zaštita cjelovitosti (integrity protection), kriptografska zaštita (encryption) i zaštita privatnosti (privacy services).

Korisnik SIP mreže je jedinstveno određen SIP adresom. SIP adresa je slična adresi e-pošte i njen format je *sip:userID@gateway.com*, pri čemu *userID* može biti ili ime korisnika ili E.164 broj. Podržavanje E.164 brojeva u DNS-u upotrebom ENUM (Electronic Number Mapping System) protokola, omogućava SIP klijentima i mrežnim prolazima da šalju i primaju telefonske brojeve umjesto SIP URI-a u porukama, te da ih usmjeravaju u razumljivom obliku. Osim SIP URI-a, podržan je i SIPS URI koji podrazumijeva upotrebu sigurnosnih mehanizama, [22], [25], [36], [41].

Primjeri SIP adresa su:

sip:zvezdan.stojanovic@mtel.ba

sips:zvezdan.stojanovic@mtel.ba

Korisnik se registruje kod servera za registraciju upotrebom SIP adrese. Ovaj server daje ovu informaciju serveru lokacije na njegov zahtjev. Pri otpočinjanju poziva, SIP zahtjev se šalje SIP serveru (ili proxy-u ili serveru za preusmjeravanje poziva). Zahtjev uključuje adresu pozivaoca i adresu pozvane strane. Tokom vremena krajnji korisnik SIP-a se može premiještati i može se dinamički registrovati kod SIP servera. Server lokacije može koristiti protokol poput LDAP-a (Lightweight Directory Access Protocol) za lociranje krajnjeg korisnika. Budući da se krajnji korisnik može ulogovati (pristupiti) na više stanica, to se ispitivanjem može dobiti i više adresa krajnjeg korisnika. Ako zahtjev prolazi preko posredničkog SIP servera, posrednički server će probati svaku od vraćenih adresa sve dok ne locira krajnjeg korisnika. Ako zahtjev prolazi preko servera za preusmjeravanje poziva, on prosleđuje sve adrese do pozivaoca, [90].

7.8. IPTV

Danas digitalna televizija sve brže zamjenjuje analognu. U literaturi se često ne pravi razlika između IPTV-a i Internet televizije. Prvo ćemo definisati oba pojma, [84], [90].

Def.: *Kod Internet televizije vrši se prenos signala (digitalizovanog audia, videa i podataka) preko otvorene mreže u formi IP paketa i kod nje se ne može garantovati propusni opseg za prenošeni sadržaj pa je on stoga usljed brojnih ograničenja (zagušenja, gubitaka paketa i sl.) ograničenog kvaliteta.*

Def.: *Za razliku od Internet televizije, IPTV se takođe bazira na IP-u, ali kod IPTV-a se prenos sadržaja vrši u zatvorenom mrežnom okruženju koje garantuje propusni opseg čime se postiže znatno veći kvalitet prenošenog sadržaja.*

Nabavka sadržaja se vrši većinom preko optičkih mreža i satelita. Primjenom IP/MPLS (Multi Protocol Label Switching) u jezgru mreže se postiže zahtijevani QoS (Quality of Service)/QoE (Quality of Experience) što predstavlja važan element za pridobijanje krajnjeg korisnika, [5], [13], [21].

Većina operatera u regionu koristi xDSL (ADSL, ADSL2 i ADSL2+, VDSL) tehnologije u pristupnoj mreži, a samim tim i postojeću mrežnu infrastruktura (bakarne parice). Njihovom primjenom u pristupnoj mreži, otklonila su se u značajnoj mjeri uska grla kao posljedica nedovoljnog protoka za širokopojasne servise koje je potrebno pružiti krajnjim korisnicima, [8].

Uvođenje IPTV-a treba da pruži niz prednosti kako korisniku tako i telekomunikacionim operaterima.

Prednosti koje IPTV pruža krajnjim korisnicima su: slika boljeg kvaliteta u odnosu na postojeću i uvođenje novih personalizovanijih servisa.

Prednost za operatere jeste u tome što su sada u stanju da ponude integrisanu uslugu, tj prenos paketizovanog govora (VoIP), videa i podataka (širokopojasni pristup Internetu) za prenos u jednoj mreži (Triple Play koncept), koja se zasniva na Internet protokolu (IP), čime se mogu postići značajne uštede.

7.8.1. Osnovni elementi arhitekture IPTV-a

Pojednostavljena arhitektura IPTV mreže prikazana na Sl.7.12. Postoje tri glavna tipa IPTV čvorišta (head-end) zavisno od veličine mreže (broja pretplatnika) i zavisno od toga da li se distribucija video sadržaja organizuje na državnom, regionalnom ili lokalnom nivou, tako da su u slučaju manjih mreža sa manjim brojem korisnika, funkcije više čvorišta skoncentrisane u jednom čvorištu. To su SHE (Super Head End), VHO (Video Hub Offices) i VSO (Video Switching Offices), [58], [84], [86],[89], [90].

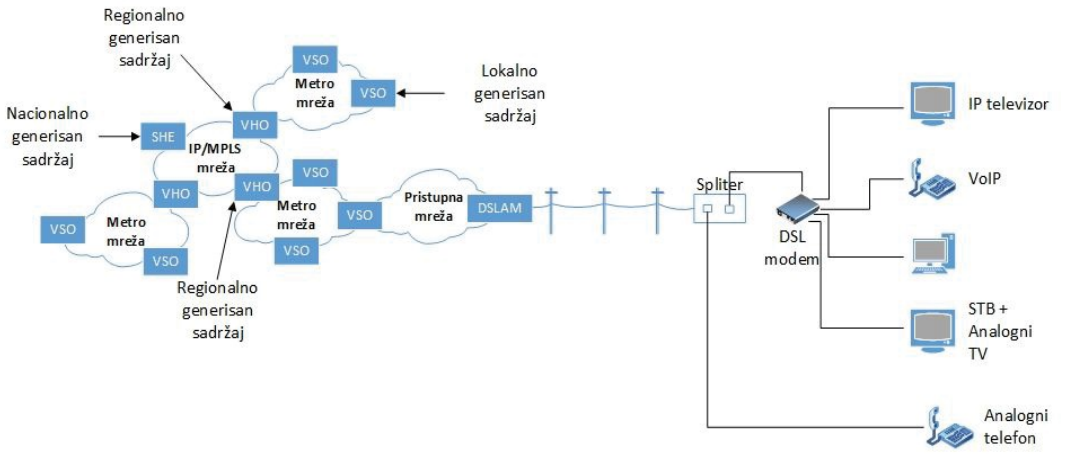
Televizijski signali ulaze u transportnu mrežu preko nacionalnog telekomunikacionog mrežnog čvorišta SHE. Signali se većim dijelom primaju preko satelita i preko optičkih mreža. Tu se obično nalazi i programsko rješenje (IPTV Middleware) koje objedinjuje sve komponenete IPTV sistema, određuje izgled interfejsa prema krajnjim korisnicima, kontroliše pristup korisnika (autentifikacija), vrši obradu zahtjeva pristiglih od strane korisnika, recimo zahtjev za promjenu kanala ili zahtjev za nekim servisom (video na zahtjev).

Poslije obrade primljenih signala (kodovanje, kompresija, enkapsulacija), SHE vrši njihovu distribuciju do VHO preko IP/MPLS mreže.

VHO-ovi vrše agregaciju nacionalnog, regionalnog i lokalnog sadržaja (lokalni kanali, reklame), sa servisima na zahtjev i opslužuju metro oblasti sa velikim brojem korisnika sami ili preko VSO-a sa kojima su povezani preko metro mreže. Postojanje VSO-a nije neophodno i opravdano je samo ako postoji veći broj pretplatnika u nekoj manjoj oblasti. VSO ubrzavaju isporuku sadržaja pretplatnicima jer se recimo neki popularni sadržaji mogu smjestiti kod njih, a oni se u mreži postavljaju bliže pretplatniku. VSO-ovi distribuiraju IPTV programe do pretplatnika preko pristupne mreže.

U pristupnoj mreži se koristi neka od xDSL tehnologija koja može da predstavlja usko grlo zbog relativno malog protoka koji se pomoću tih tehnologija mogu pružiti, čak i uz primjenu tehnologija poput ADSL2 koja teoretski pruža 12 Mbit/s odnosno ADSL2+ sa 24 Mbit/s, o čemu je već bilo govora u Poglavlju 2

Na Sl.7.12 su prikazani i neki krajnji korisnički uređaji koji podržavaju IPTV. IP televizori su specijalno konstruisani uređaji preko kojih je moguće gledati TV kanale preko IP mreže (bez upotrebe adaptera ili medijskih mrežnih prolaza). TV adapteri, STB (Set Top Box) konvertuju digitalne televizijske signale u standardne RF čime je omogućeno gledanje IPTV-a i preko klasičnih TV prijemnika. Multimedijalni računari posjeduju sposobnost audio i video obrade i potrebno je obično instalacija nekog jednostavnijeg softvera (tipa media player-a) radi upotrebe IPTV servisa.



Slika 7.12*: Pojednostavljena arhitektura IPTV-a*

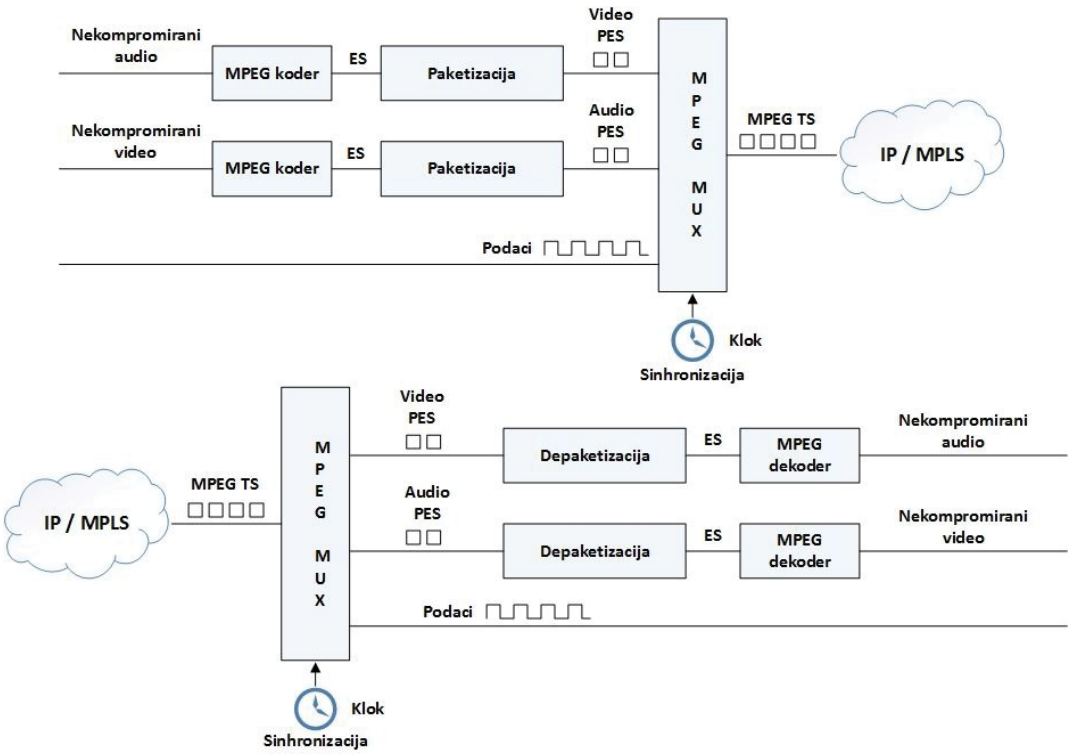
7.8.2. Formiranje transportnog toka

Primljeni sadržaj na lokaciji SHE-a je potrebno pripremiti za dalji prenos preko IP/MPLS mreže. Ako su primljeni video i audio signali u analognom obliku, potrebno je izvršiti njihovo prevođenje u digitalni oblik i njihova kompresija radi boljeg iskorištenja propusnog opsega transportne mreže (najčešće MPEG2, u skorije vrijeme MPEG4), [46].

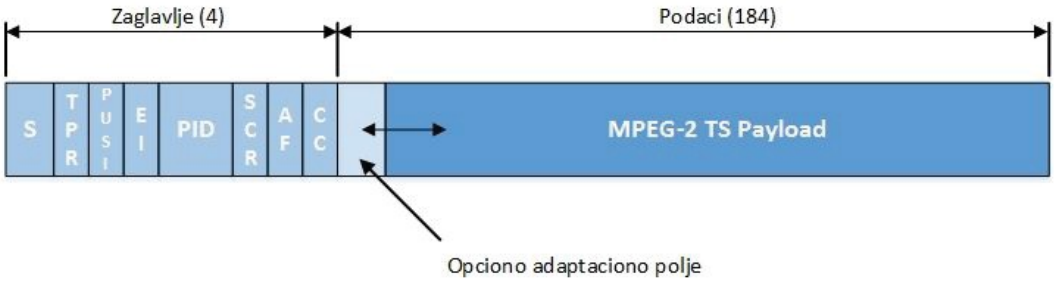
Na izlazu MPEG (Moving Picture Expert Group) kodera se dobija osnovni tok podataka (ES-Elementary Stream). Potom se vrši njegova paketizacija i formiranje paketizovanog osnovnog toka (PES-Packetized Elementary Stream), [4].

Zatim se formirani video i audio PES multipleksiraju sa korisničkim i eventualno kontrolnim podacima i nastaje MPEG-TS (PS-Program Stream) ili SPTS (Single Program Transport Stream), kako je to prikazano na Sl.7.13.

Za prenos kroz IP/MPLS mrežu vrši se ograničavanje nastalih PES paketa na pakete fiksne dužine od 184 bajta i dodavanjem 4 bajta zaglavlja formira se MPEG2-TS paket (Sl.7.14). U zaglavlju se nalazi identifikacioni kod paketa PID (Packet Identification Code) kojim se jedinstveno određuje pripadnost paketa određenom elementarnom toku unutar TS paketa, čime je omogućeno multipleksiranje i demultiplekisiranje bitskih tokova, [4],[31].



Slika 7.13*: Prenos MPEG-TS paketa kroz IP/MPLS mrežu*



Slika 7.14*: MPEG-TS paket*

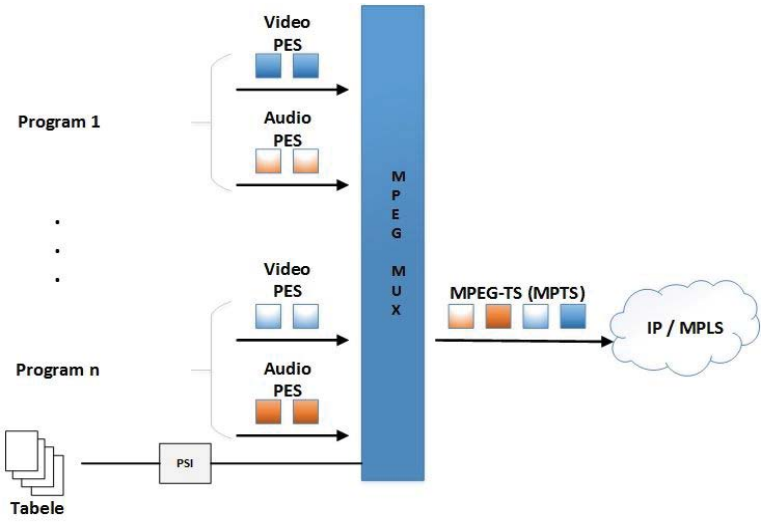
Kako se vidi sa Sl.7.13. mora se uspostaviti sinhronizacija između predaje i prijema na transportnom nivou a to se radi na taj način što MPEG koder generiše 27 MHz-ni sistemski klok koji se prenosi svakih 100 ms u PCR polju (Program Clock Reference) i na koji se sinhronizuju svi medijski tokovi koji čine progam, [85].

Ako je na prijemu MPEG dekoder regenerisao sistemski klok, izdvajanje i filtriranje paketa koji pripadaju određenom medijskom toku (audio ili video) se sprovodi jednostavno preko PID-a.

Bajt S (Synch) omogućava prijemniku da odredi početak MPEG-TS paketa. Preko polja EI (Error Indication) i CC (Continuity Check Index) se može utvrditi da li je došlo do greške pri prenosu.

Da bi se onemogućilo neovlašteno korištenje resursa vrši se skremblovanje podataka, na šta ukazuje SCR (Scrambling Control) polje. Skremblovanje se može primijeniti na svaki elementarni bitski tok, dok se deskremblovanje vrši na odredištu pomoću tajnog ključa. Adaptaciono polje (AF) služi da se dopuni transportni tok (TS) u slučaju potrebe, bitima popune kako bi se postiglo da TS bude uvijek iste dužine. Polje PUSI (Payload Unit Start Indicator) daje informaciju prijemniku da je počeo novi PES.

Na Sl.7.13 je prikazano formiranje jednog programskog toka. U slučaju prenosa više programskih tokova (Sl.7.15) formira se MPTS (Multi-Program Transport Stream). Budući da MPTS prenosi više programa za identifikaciju pojedinačnih koji se prenose u MPTS-u periodično se prenose informacije koje se nalaze u PSI tabelama (Program Specific Information) koju čine PAT (Program Association Table) koja daje listu programa koji se prenose u MPTS-u, dok PMT (Program Map Table) daje informacije o identifikacionim kodovima paketa (PID-Packet Identification Code). Te informacije su dovoljne demultiplekseru i dekoderu na prijemu da odrede koji paketi pripadaju kojem pojedinačnom programu, [46].



Slika 7.15: *Formiranje MPTS-a*

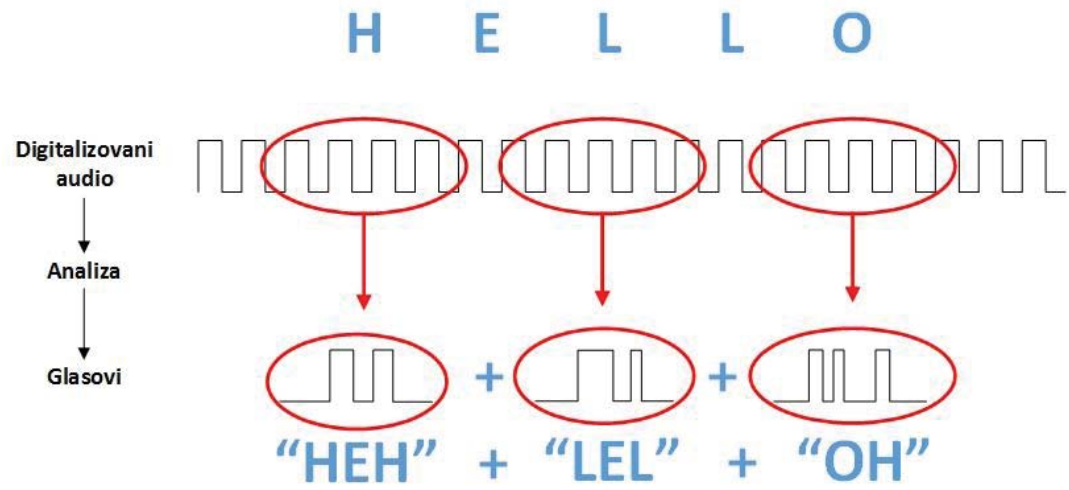
Formirani MPEG-TS paket (Sl.7.14) predstavlja osnovnu jedinicu podataka za enkapsulaciju (payload) po definisanaim slojevima IP modela (RTP/UDP/IP enkapsulacija) i tako formirani IP paketi podataka se prenose do odredišta preko IP/MPLS mreže gdje se sprovodi obrnut proces.

7.8.3. Audio i video kompresija

Kompresija digitalnog audio i video signala predstavlja proces analiziranja tih signala i upotreba dobijenih informacija je u svrhu uklanjanja redudantnih informacija čime se smanjuje potrebni propusni opseg za njegovo prenošenje, [18], [46].

7.8.3.1. Audio kompresija

Kao tehnika za audio kompresiju najčešće se koristi perceptualno kodovanje. Perceptualno kodovanje je proces konvertovanja informacija u oblik koji odgovara sposobnosti ljudskih osjetila da registruju i prihvate određenu informaciju. Na primjer ljudsko uho ne može da čuje istovremeno jak zvuk jedne frekvencije i tih zvuk druge frekvencije. Upotrebom perceptualnog kodovanja mogu se eliminisati zvuci na onim frekvencijama koje ljudsko uho ne može registrovati. Analizom digitalne informacije (Sl.7.16), dobijene digitalizacijom riječi „HELLO“, utvrđeno je da se čitava riječ može predstaviti sa tri glasa „HeH“, „LeL“ i „OH“. Svaki od ovih glasova zahtijeva samo nekoliko digitalnih bita kako bi se ispravno reprodukovao originalni talasni oblik, [46].

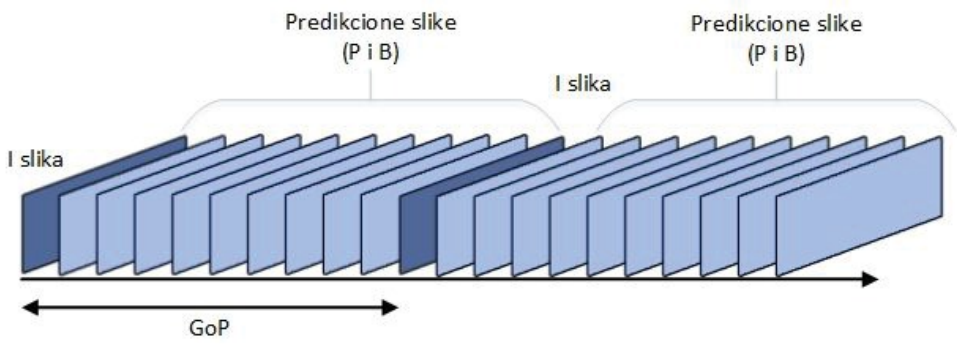


Slika 7.16: *Kompresija digitalizovanog audio signala*

7.8.3.2. Video kompresija

Nekomprimovani digitalni video signal zauzima veliki propusni opseg (čak 270 Mbit/s) što bi predstavljalo nepremostivu prepreku za upotrebu sa postojećim pristupnim tehnologijama i nije ekonomično. Zbog toga se vrši kompresija digitalnog video signala. Najčešće se koristi prediktivna tehnike kompenzacije pokreta. Ova tehnike počivaju na

organizaciji sekvence slika u skupove I slika (intra frame) kao i prediktivnih P i B slika (inter frame), kako je to prikazano na Sl.7.17. I slike se koduju nezavisno od drugih slika u sekvenci, sa tehnikama kompresije koje su slične tehnikama kompresije statičnih slika, kakva je JPEG (Joint Protocol Expert Group). Stepen kompresije je stoga manji jer nema predikcije drugih slika. I okviri se obično nalaze na početku sekvence i na jednakim međusobnim rastojanjima. Razmak između dva I okvira se naziva GoP (Group of Pictures), [46],[58],[72],[85].



Slika 7.17*: Sekvenca okvira pri digitalnoj kompresiji*

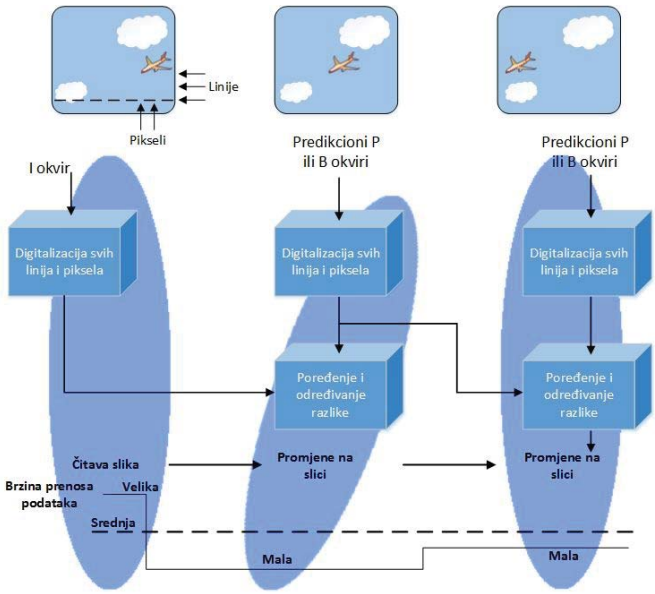
Upotrebom prediktivne tehnike za kompenzaciju pokreta poredi se trenutna slika sa najbližom prethodnom (I ili P) i formira P slika koja poslije služi kao referentna za naredne P ili B slika. U slučaju brzog pomjeranja objekta preko ekrana, odnosno, aviona na Sl.7.18, ove slike će nositi jako malo informacija.

U slučaju da imamo više pokretnih objekata na slici pomoću ovakve kompresije nećemo dobiti dobre rezultate, jer bi razlika između slika sadržala gotovo toliko informacija kao i sama slika.

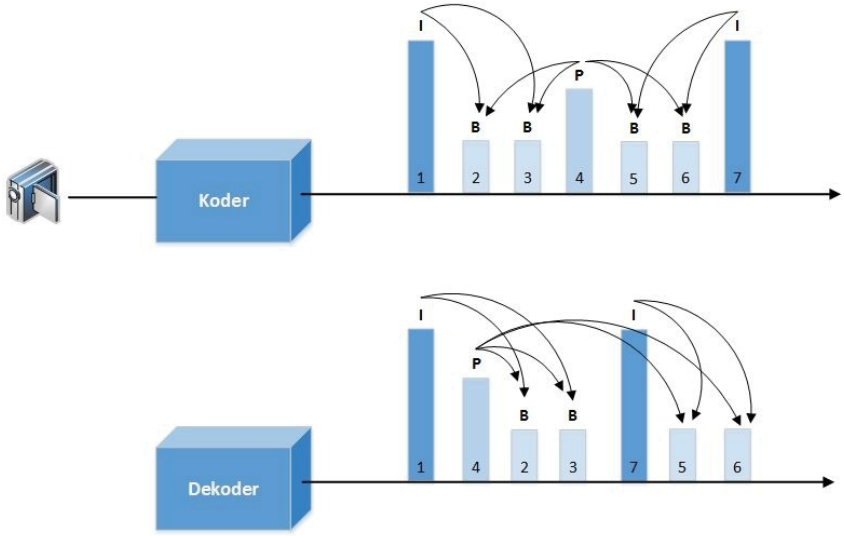
Kompresija kod P slika je dosta veća nego kod I slika. Predikcione B slike koriste bidirekcionu predikciju pokreta u oba pravca radi ostvarivanja još bolje kompresije, predikcija je vezana za prethodnu i narednu sliku, a to mogu biti i I i P slike.

Budući da su neke slike napravljeni na osnovu informacija iz prethodnih (P slike) ili prethodnih i narednih (B slike), greška na nekoj od predikcionih slika će se prenijeti i na naredne slike koje su dobijene predikcijom. Zbog toga se periodično ubacuju I slike, (Sl.7.17) , kako bi se spriječili prenošenje greške na naredne slike, budući da se I slike koduju nezavisno od ostalih. Stoga se može zaključiti da veličina GoP-a ne smije biti prevelika.

Radi uspješnog formiranja sekvence slika nakon dekodovanja, slikama se prilikom kodovanja dodjeljuju oznake (time stamps).



Slika 7.18*: Digitalna video kompresija*



Slika 7.19*: Sekvenciranje slika na prijemu*

Na Sl.7.19 se vidi da se B slike (2 i 3) kreiraju iz I slika (1) i B slika (4). B slike (5 i 6) se kreiraju iz P slika (4) i I slika (7). Na prijemu dekoder mora prvo kreirati I sliku (1) i P sliku (4) prije B slika (2 i 3), dok se P slika (4) i slika (7) koriste za kreiranje B slika (5 i 6), [46].

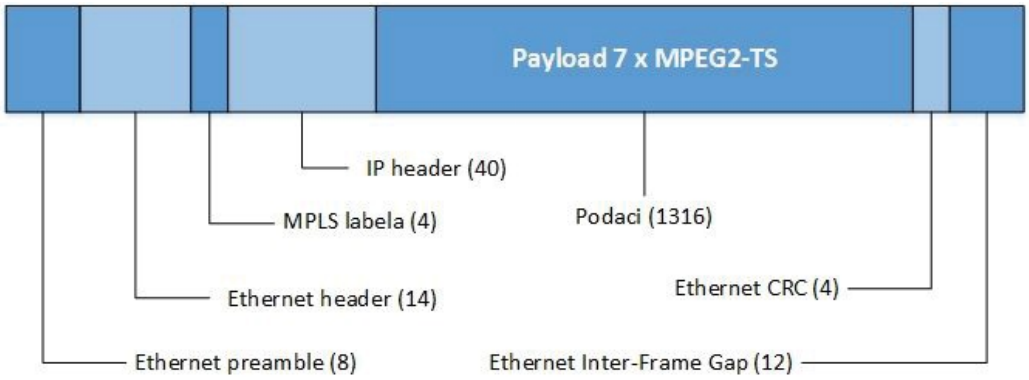
7.8.4. Prenosni protokoli

Kao prenosni protokol koristi se UDP u kombinaciji sa RTP-om. Primjenom MPLS-a (Multi-Protocol Label Switching) u jezgru mreže postignut je efikasaniji način rutiranja kroz mrežu u odnosu na klasični, [86], [90].

Kod klasičnog načina rutiranja paketa kroz mrežu, analizira se zaglavlje svakog paketa koje prolazi kroz mrežu na njegovom putu do odredišta. Za razliku od tog postupka, MPLS koristi postupak nazvan zamjena labela (Label Swapping) za prenos paketa kroz mrežu. Važna prednost ovog postupka jeste da se informacije iz zaglavlja paketa analiziraju samo jednom na rubnom ruteru, LER-u (Label Edge Router) a dalje se postupak usmjeravanja paketa zasniva samo na labelama i odvija preko unaprijed određenih puteva, LSP-ova (Label Switched Path). Labele se dodaju između zaglavlja IP protokola i L2 protokola (u primjeru na Sl.7.20 kao L2 protokol uzet je Ethernet). Primjenom MPLS-a je omogućeno da se pojedinim saobraćajnim tokovima da veći prioritet, moguće je i usmjeravanje saobraćaja zavisno od stanja mreže na manje zagušene puteve (saobraćajni inženjering), a primjenom sa DiffServ-om omogućeno je sotisficirano uvođenje kvaliteta u mreži.

7.8.5. Enkapsulacija

Nakon formiranja MPEG TS-a za prenos preko IP infrastrukture potrebno je izvršiti formiranje IP paketa. Prilikom formiranja IP paketa, korisni dio, sadržaj (payload) za prenos podataka se dobija obično kombinovanjem 7 MPEG transportnih tokova, [90].



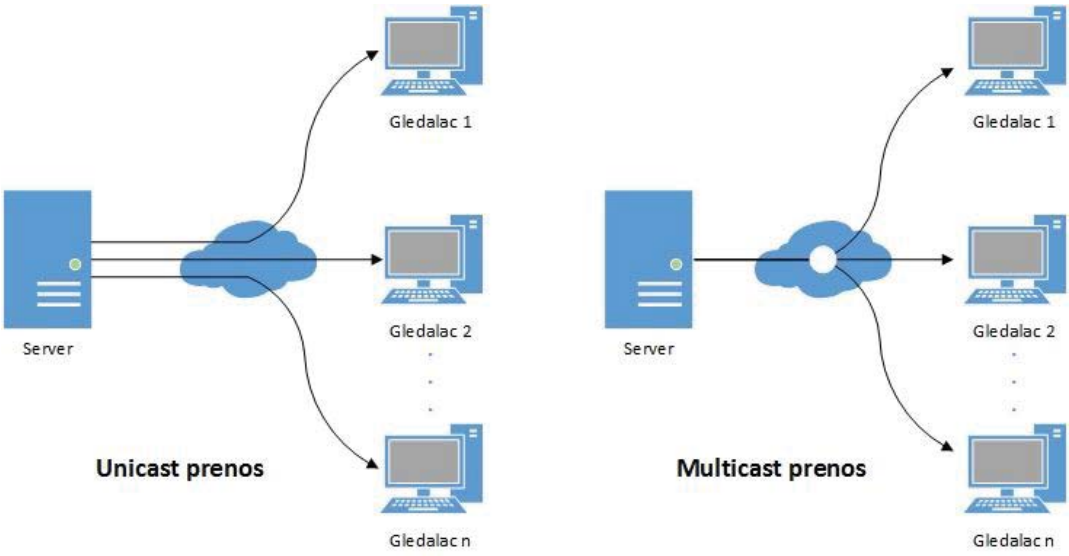
Slika 7.20*: Formiranje Ethernet frejma*

Enkapsulacijom se čitav paket višeg sloja smiješta u tijelo paketa nižeg sloja. Prilikom silaska niz različite nivoe protokol steka svaki od viših nivoa dodaje svoje zaglavlje na korisni dio. Za prenos preko IP infrastrukture izvršena je RTP/UDP/IP enkapsulacija (što je označeno kao IP header na Sl.7.20), [86].

Uz to je između L3 nivoa (IP) i L2 nivoa (Ethernet) ubačena labela podataka MPLS protokola. Za prenos preko optičke mreže kao L2 protokol koristi se PPP (Point-to-Point) protocol.

7.8.6. *Unicast* i *multicast* prenos kod IPTV-a

U slučaju kad je potrebno krajnjem korisniku prenijeti više IPTV kanala (recimo da u jednom domaćinstvu ima više korisnika IPTV-a i više STB-ova) i da oni žele da gledaju različite kanale u isto vrijeme to bi predstavljalo problem zbog nedostatka propusnog opsega u pristupnoj mreži, a u slučaju nekih jako gledanih događaja, recimo prenosa sportske utakmice, kada broj korisnika koji žele da gledaju isti kanal enormno poraste to bi predstavljalo veliki problem i za magistralnu mrežu i predstavljalo bi veliko opterećenje za servere, [14], [86].



Slika 7.21*: Multicast i unicast prenos*

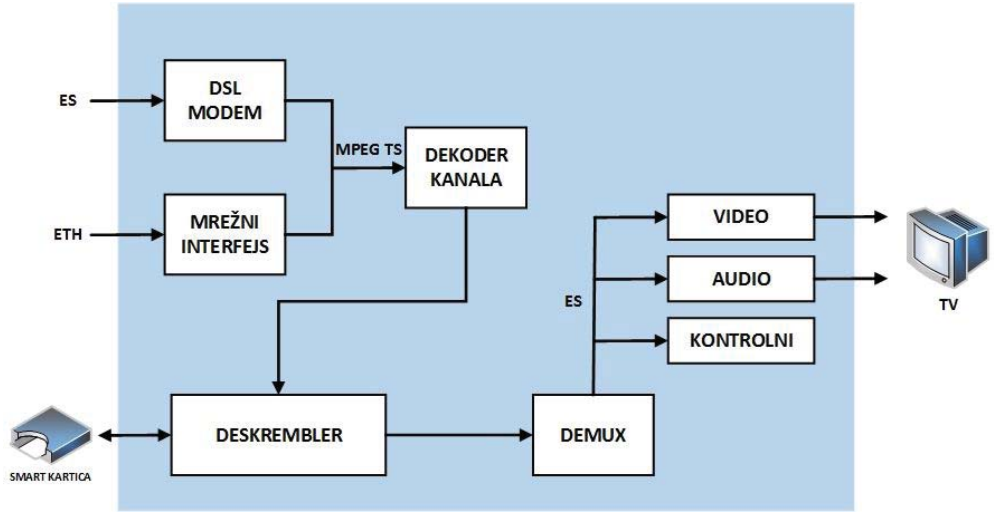
Problem se rješava primjenom *multicast* prenosa. Kod *multicast* prenosa, izvor (server na Sl.7.21) adresira jedan paket koristeći *multicast* adresu, pa potom kopira taj paket i šalje kopije svim adresiranim korisnicima. To u slučaju IPTV-a znači da će od svih korisnika koji su putem svog daljinskog upravljača, uputili poruku *middleware*-u da žele da pređu na određeni kanal, formirati *multicast* grupa, kojoj *middleware* šalje traženi program. To se obavlja preko njihovog lokalnog DSLAM-a sa kime pretplatnici komuniciraju putem IGMP protokola (IP Group Membership Protocol), [48]. Upotrebom *multicast* prenosa se postiže velika ušteda u potrebnom propusnom opsegu u odnosu na primjenu *unicast*-a kod koga bi se traženi programski sadržaj morao isporučivati do svakog pretplatnika posebno.

Kod *unicast* paketa svaki adresirani paket preko unicast adrese se šalje do samo jednog korisnika na koga ukazuje adresa.

Ipak i *unicast* prenos je našao svoju primjenu i to kod servisa video na zahtjev (VoD-Video on Demand). Kod VoD-a korisnik iz elektronskog video kluba koji je formirao provajder IPTV-a bira neki film ili sadržaj koji želi da gleda i koji se *unicast*-om šalje samo njemu.

7.8.7. Uređaji krajnjeg korisnika

Na Sl.7.22. su prikazani uređaji preko kojih korisnik može gledati IPTV programe. Pošto se kod nas uglavnom koriste klasični televizori koji koriste adaptere, STB-ove, za gledanje IPTV programa to ćemo objasniti princip rada STB-a. STB bismo mogli shvatiti ne samo kao hardversku komponentu već i kao računar koji radi obično pod Linuks operativnim sistemom i čiji je rad tijesno povezan sa realizovanim *middleware* rješenjem. STB-ovi obično podržavaju MPEG-2 a noviji i MPEG-4 kompresiju. Princip rada STB-a se može dati kao na Sl.7.22.



Slika 7.22*: STB (Set Top Box)*

STB obično prima pakete koji su enkapsulirani u Ethernet pakete (Sl.7.20). STB izdvaja IP pakete i dobija MPEG TS. Dekoder kanala detektuje greške (ako postoje), vrši njihovu korekciju i propušta TS do deskremblera gdje se na osnovu ključa vrši dekodovanje transportnog toka. Preko demultipleksera i na osnovu PID-a (uz pretpostavku da je uspješno obavljena sinhronizacija predaje i prijema), izdvajaju se ES-ovi za video, za audio, kao i za kontrolne podatke izabranog programa koji formiraju traženi program za prikaz na TV-u krajnjeg korisnika.

7.9. Virtuelne privatne mreže (VPN)

Većina Internet usluga je na raspolaganju svakoj firmi/pojedincu koji ima pristup Internetu. Postoje aplikacije koje sadrže povjerljive informacije i zahtijevaju ograničen pristup ili samo zaposlenim u preduzeću ili autorizovanim korisnicima van njega. Budući da je Internet javni medij, a poslovne komunikacije bi trebale biti privatne prirode, to možemo zaključiti da je od najvećeg značaja obezbijediti zahtijevanu privatnost poslovnih komunikacija uz primjenu javne Internet infrastrukture, [45], [52], [70], [90].

Iz gore navedenog se ogleda značaj primjene virtualnih privatnih mreža (VPN-Virtual Private Network):

Def.: *Virtuelne privatne mreže (VPN) nude sposobnost obavljanja privatne komunikacije preko javne mreže kakva je Internet, sa definisanom raspoloživošću i performansama putem sporazuma o novou servisa (SLA-Service Level Agreement).*

Def.: *VPN predstavlja kombinaciju tehnika i tehnologija koje osiguravaju komunikaciju između dvije krajnje tačke uspostavljanjem tunela koji je neprobojan za prisluškivanje i ometanje.*

Osnovna ideja VPN-a je jednostavna. Neka korporacija može imati veliki broj kompanija koje mogu biti veoma geografski udaljene, čak i na različitim kontinentma. Svaka od tih kompanija može da ima svoju vlastitu mrežu, LAN ili WAN. Povezivanjem ovih odvojenih mreža, koje se nalaze na različitim lokacijama se formira VPN.

VPN omogućava kreiranje specifičnih profila korisnika (definisanjem skupa ovlaštenja i ograničenja za svakog člana VPN-a) u skladu sa potrebom korporacije.

Nosilac VPN-a je osoba koja u potpunosti odlučuje o definisanju mogućnosti za upotrebu nekog korporativnog sadržaja, recimo pristup određenim informacijama, ograničenje pristupa određenim Internet sadržajima sa računara u kompaniji (recimo zabavnim sadržajima, igrama i sl).

7.9.1. Mogućnosti umrežavanja kod VPN-a

IP VPN pruža sledeće mogućnosti umrežavanja:

- intranet,
- ekstranet,
- udaljeni pristup mobilnih korisnika.

7.9.1.1. Intranet

Def.: *Intranet predstavlja privatnu mrežu unutar preduzeća koja koristi Internet standarde i omogućava zaposlenima unutar preduzeća da razmjenjuju informacije putem e-pošte i veba (informacije su ograničene unutar jednog preduzeća).*

Informacije koje se razmjenjuju su vezane za preduzeće u kome rade i to su obično novosti u vezi preduzeća, proizvodi preduzeća, imenik zaposlenih, izvještaj o prodaji, [52].

Osnovna razlika intraneta u odnosu na Internet jeste u vlasničkoj strukturi i u pravu pristupa:

- Internet nije u vlasništvu nijednog preduzeća ili pojedinca, dok je intranet po samoj definiciji privatna mreža određene organizacije,
- pristup Internetu ima svaka osoba koja ima određene tehničke mogućnosti, dok pristup intranetu imaju samo osobe sa ovlašćenjem.

Administratori lokalnih mreža uspješno su iskoristili TCP/IP skup protokola (HTTP, SMTP, POP3 i sl) da u svojoj lokalnoj mreži obezbijede razmjenu elektronske pošte, prenos datoteka i sl.

Intranet je dakle u funkciji samog preduzeća za njene vlastite potrebe, ali sa mogućnošću nadziranog pristupa prema vani i sa vana.

Intranet je interni informacioni sistem zasnovan na klijent-server aktivnostima između pojedinaca i pojedinih sektora organizacije.

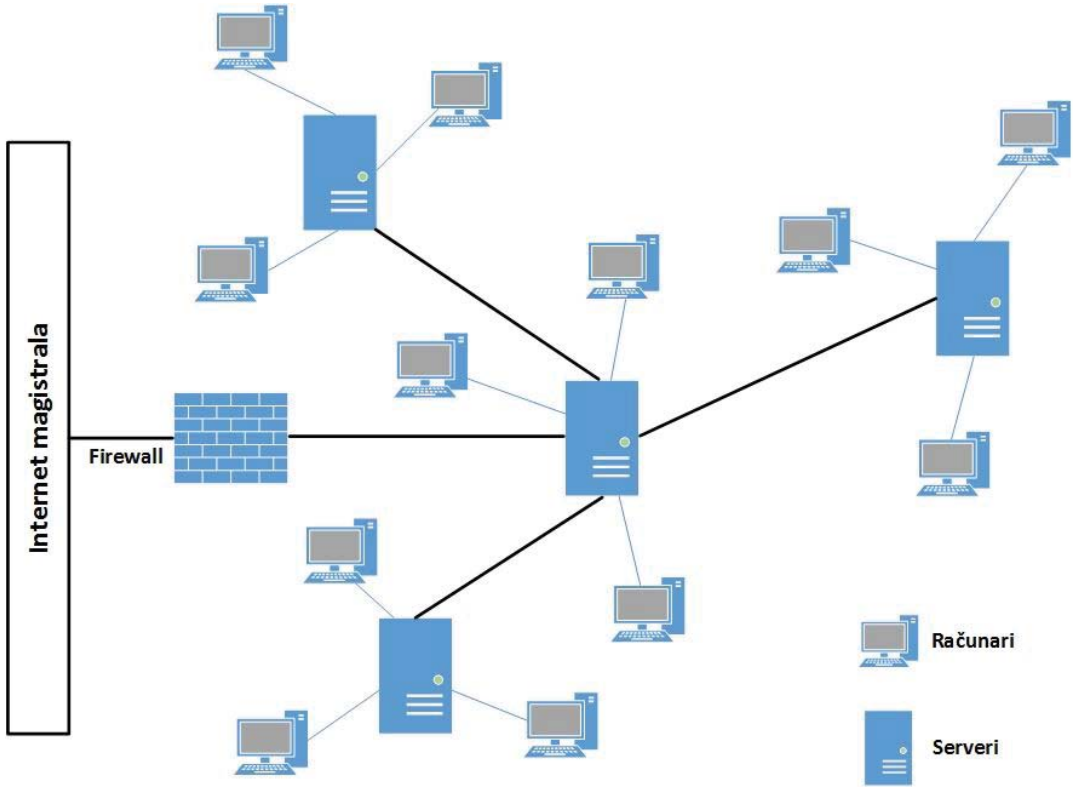
Fizički elementi Intraneta su:

- mreža (može biti LAN ili WAN),
- bar jedan računar sa instaliranim server softverom (uključujući TCP/IP),
- dodatni računari sa klijentskim softverom (uključujući TCP/IP i veb čitač).

Samo uvođenje intraneta povećava sigurnosni rizik ali je nužno u uslovima elektronskog poslovanja. Osobe koje mogu najviše ugroziti sigurnost intraneta su sami zaposleni u preduzeću, firme, saradnici, klijenti ili hakeri.

Sigurnost se može poboljšati osim uvođenjem *firewall*-a i raznim oblicima šifrovanja i autentifikacije.

Intranet obuhvata i *firewall* softver za zaštitu mreže (Sl.7.23). *Firewall* štiti intranet od neautorizovanog pristupa korisnika iz drugih mreža ili organizacija, o čemu će biti više govora u Poglavlju 9.



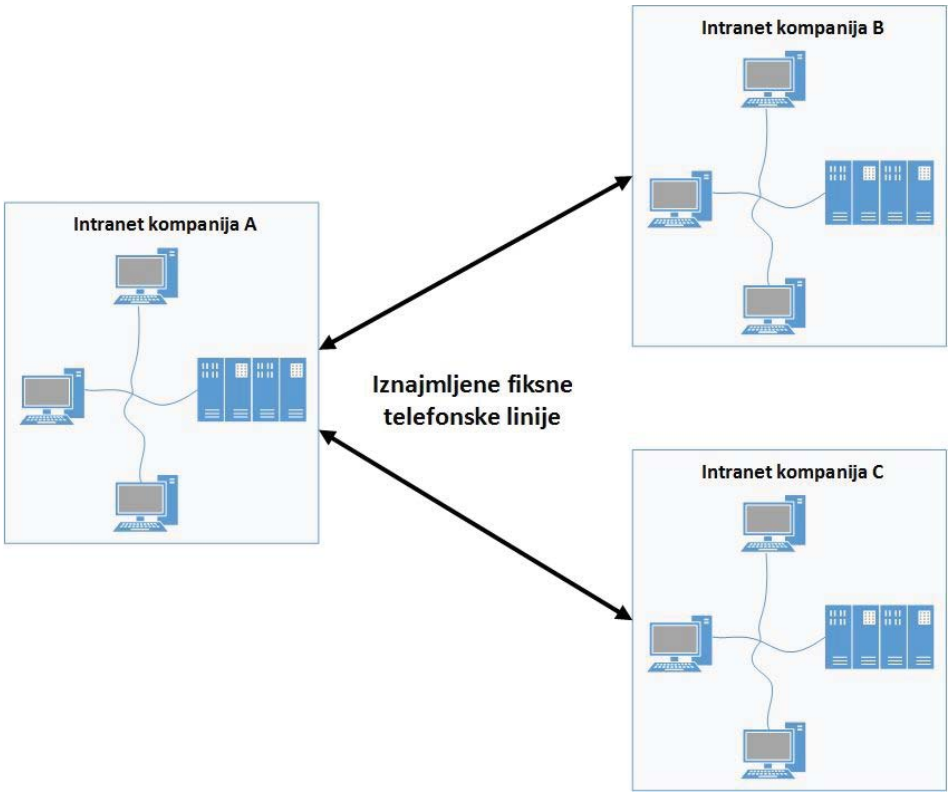
Slika 7.23*: Arhitektura intraneta*

7.9.1.2. Ekstranet

Povezivanjem intraneta jednog preduzeća sa intranetima drugih srodnih preduzeća nastaje ekstranet, čime se dodatno povećava racionalnost zajedničkog poslovanja, konkurentnost proizvoda i usluga, te se samim tim povećava i profit pri poslovanju.

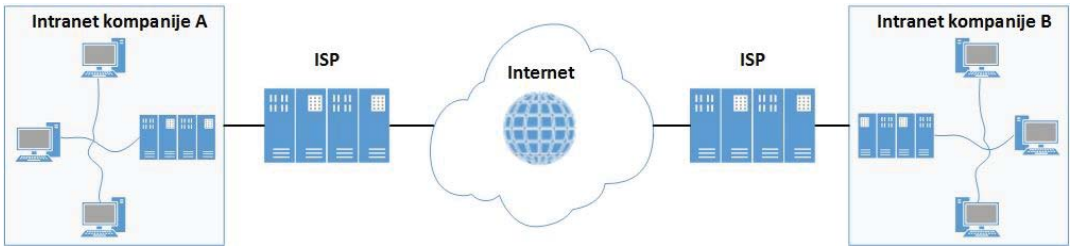
Organizacije mogu uspostaviti ekstranet na tri načina:

- sigurna privatna mreža: fizičko povezivanje više privatnih mreža preko iznajmljenih telefonskih linija;



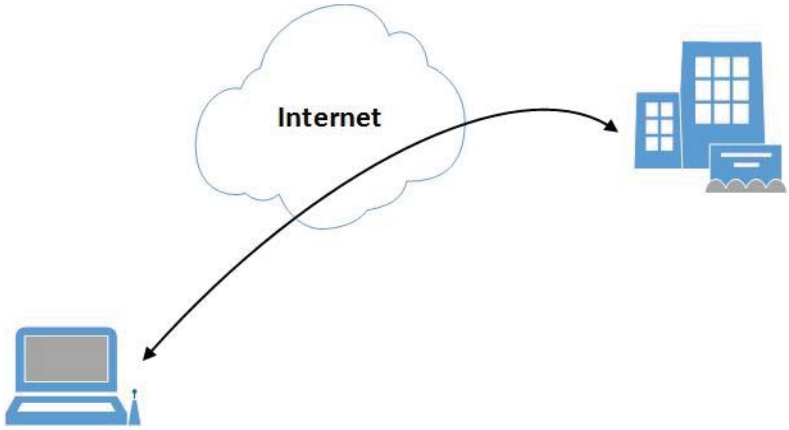
Slika 7.24*: Sigurna privatna mreža*

- javna mreža: upotreba javne komunikacione infrastrukture Interneta (razmatramo IP VPN pa posmatramo samo javnu infrastrukturu Interneta, mada bi se VPN mogao uspostaviti i preko javne telefonske mreže);



Slika 7.25*: Javna mreža*

- povezivanje individualnog prenosnog računara (radne stanice) preko Interneta na privatnu mrežu; u ovom slučaju, funkcija VPN se implementira kao softver unutar prenosnog računara.

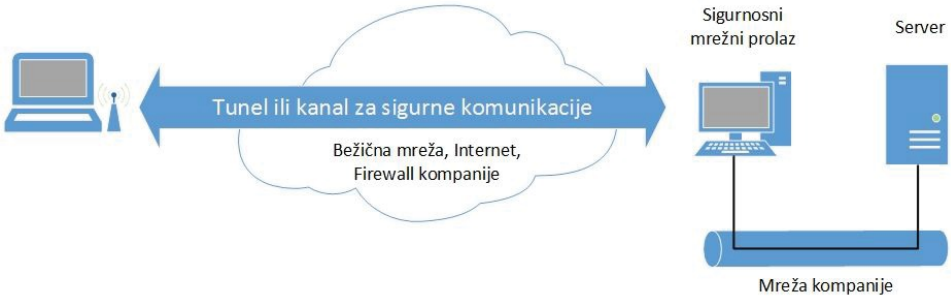


Slika 7.26: *Povezivanje udaljenog zaposlenog sa sjedištem kompanije*

7.9.2. Uspostava VPN tunela

U VPN vezi, može da se pojavi sledeći niz događaja:

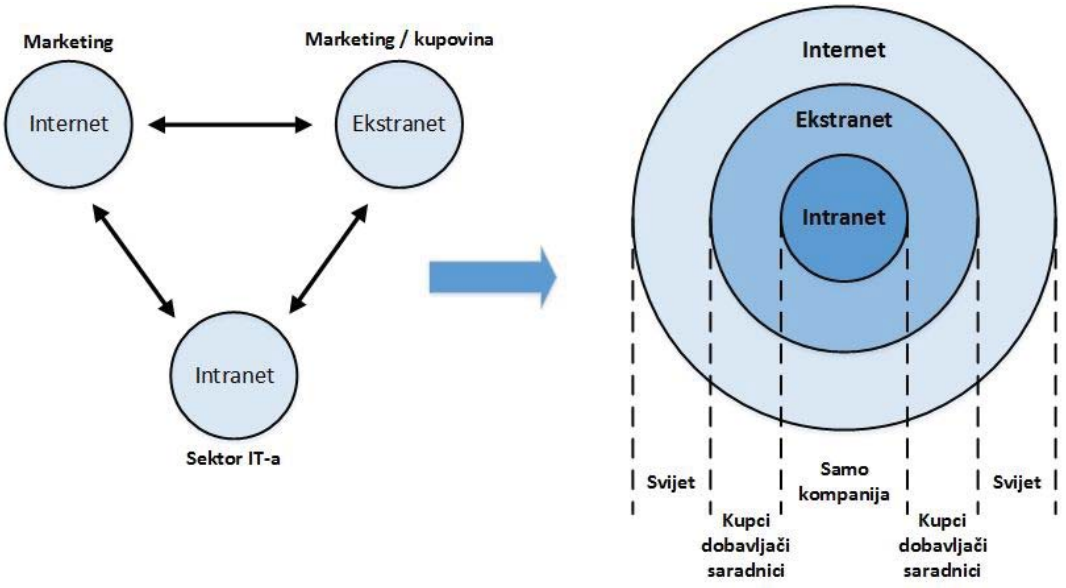
- dva krajnja korisnika najprije se međusobno autorizuju: VPN server može da odredi kojim uslugama radna stanica ima dozvolu da pristupi i može u saglasnosti sa tim da upravlja saobraćajem koji slijedi; ovaj korak se zove autorizacija;
- jednom kada je tunel stvoren, njegove krajnje tačke dodaju posebna zaglavlja paketima koji su adresirani za suprotnu stranu tunela, šifruju originalni paket i zaglavlje i enkapsuliraju sve te informacije u nove IP pakete; interna zaglavlja obezbeđuju informacije o autorizaciji na nivou paketa i obezbeđuju da se otkrije svako falsifikovanje podataka.



Slika 7.27*: Uspostava VPN tunela*

7.9.3. Odnos Interneta, intraneta i ekstraneta

Šematski se veza između Interneta, intraneta i ekstraneta može prikazati kao na Sl.7.28.



Slika 7.28: *Veza između Interneta, intraneta i ekstraneta*

POGLAVLJE 8

Približavanje svijeta mobilnih komunikacija Internetu

Krajem 2012 godine prema procjenama međunarodne unije za telekomunikacije broj mobilnih pretplatnika na svijetu je iznosio oko 6,8 milijardi što je tada predstavljalo blizu 96 % ukupne svjetske populacije. Postoje predviđanja da će u razvijenim zemljama svijeta sa velikim brojem Internet pretplatnika kakve su SAD broj pretplatnika koji pristupaju vebu putem mobilnih uređaja veoma brzo premašiti broj pretplatnika koji pristupaju vebu putem personalnih računara. U ovom poglavlju su objašnjene ključne komponente danas najprisutnijih mobilnih mrežnih tehnologija, putem kojih korisnici u BiH i zemljama okruženja najčešće ostvaruju pristup Internetu.

8.1. Pregled najzastupljenijih mobilnih mrežnih tehnologija

Prvo ćemo definisati samo značenje mobilne mreže.

Def.: *Termin mobilna mreža se definiše kao telekomunikaciona mreža koja je konstruisana za mobilne telekomunikacije. Mobilna mreža podržava mobilnost preko handovera, roaming-a ili nekih sličnih tehnologija.*

Izbor tehnologije se zasniva na nekoliko faktora. Karakteristike koje imaju uticaj na korisnika:

- pokrivenost mrežom;
- brzina mreže;
- stepen mobilnosti.

Sa tačke gledišta mrežnog operatera postoje i dodatni faktori kao što su:

- regulatorni problemi, posebno dodjela radio frekvencija,
- autentifikacija korisnika (u svrhu naplate korisnik se mora identifikovati).

Trenutne mobilne mreže koriste nekoliko tehnologija: WiMAX, WLAN (WiFi), Bluetooth, bežična telefonija, satelitski radio, celularna (ćelijska) telefonija,

Bežična telefonija se može smatrati samo kao proširenje fiksne telefonije i nećemo je posebno razmatrati, kao ni satelitski radio koji se rijetko koristi. U ovom poglavlju ćemo dati kratak pregled mobilnih tehnologija koje se kod nas najviše koriste i sa kojima se susrećemo u svakodnevnom životu.

8.1.1. WLAN

Porast broja elektronskih uređaja, kako kod kućnih, tako i kod poslovnih korisnika, za koje je potrebno obezbijediti međusobnu komunikaciju, doveo je do porasta potrebnog broja kablova, što u velikom broju slučajeva može predstavljati problem. Da bi se riješio ovaj problem, ali i povećala udobnost pri korištenju koju donosi mobilnost uređaja, uvedene su tehnike poput WLAN-a i Bluetooth-a, [79].

Bežična lokalna mreža (Wireless Access Network-WLAN) je mreža namijenjena za prenos velikih količina podataka na kratkim udaljenostima od 50-tak metara pa do oko

150 metara od pristupne tačke (access point) sa osobinama uporedivim sa onim kod žičnih LAN mreža, pa se može smatrati proširenjem ili čak zamjenom za žične LAN mreže.

WLAN je definisan serijom 802.11x standarda. Pregled njihovih uporednih karakteristika je dat u Tabeli 8.1.

Tabela 8.1: *Uporedni pregled karakteristika 802.11x standarda*

Standard	Godina	Protok	Frekvencijski opseg
IEEE 802.11	1997	1-2 Mbit/s	ISM[1] opseg od 2,4 GHz
IEEE 802.11b (WiFi)[2]	1999	1-11 Mbit/s	ISM opseg od 2,4 GHz
IEEE 802.1a	1999	Do 54 Mbit/s	5 GHz opseg
IEEE 802.1g (WiFi5)[3]	2002	Do 54 Mbit/s	ISM opseg od 2,4 GHz.

1: ISM: Industrial, Scientific Medical

2: WiFI: Wireless Fidelity

3: WiFi5: Wireless Fidelity 5x

Tip WLAN-a koji koristi 802.11 specifikaciju se naziva WiFI (Wireless Fidelity). Svi 802.11 standardi obuhvataju specifikacije sloja linka za podatke (DLL) i njegovih podlsojeva za kontrolu pristupa medijumu (MAC) i podsloja za kontrolu logičkog linka (LLC) kao i fizičkog sloja, [65], [73], [79], [82].

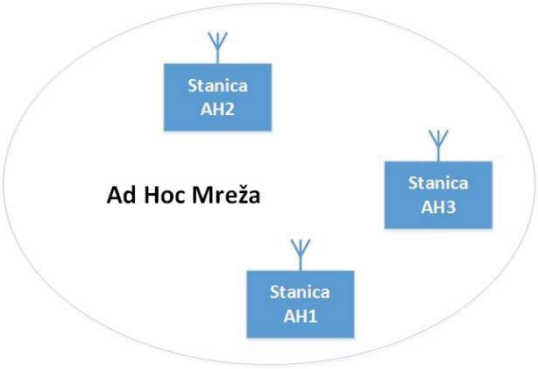
WLAN radi u tzv. industrijsko-naučno-medicinskom ISM (Industrial Scientific-Medicine) opsegu. Ovaj opseg je svima dostupan, pa se radio sistemi koji rade u ovom opsegu projektuju tako da se mogu izboriti sa interferencijom i fedingom, primjenom tehnika proširenog spektra FHSS (Frequency Hopping Spread Spectrum) i DSSS (Direct Sequence Spread Spectrum), [27].

Standardom 802.11, kako se vidi na Sl.8.1, su definisane tri tehnike za fizički pristup:

- tehnika proširenog spektra, FHSS;
- tehnika proširenog spektra, DSSS;
- infracrveni tehnologija (IR-InfraRed).

Slika 8.1: *Sloj linka za podatke i fizički sloj kod 802.11*

Najjednostavnija topologija WLAN mreže je *ad-hoc* način rada u kojem se dva ili više čvorova, tj stanice (Sl.8.2), recimo laptopova povezuje na efikasan način i moguće je na nekoj privremenoj osnovi (npr u nekoj konferencijskoj sali).



Slika 8.2: *Ad-hoc način rada*

Zbog svojih dobrih osobina kao što su automatski bežični pristup, pokretljivost korisnika, jednostavna konfiguracija bez potrebe za kablovima, veliki protoci (od standarda 802.11g čak 54 Mbit/s), WLAN mreže su našle široku poslovnu primjenu u medicini, hotelima, aerodromima, kampusima, uspostavljanje privremene mreže radi recimo potrebe neke konferencije, u poslovnim zgradama, na prodajnim mjestima u tržnim centrima, u kafeima i sl.

Razvoj WiFi-a pospješuje pojava, svakim danom sve više mobilne terminalne opreme koja posjeduje WiFi funkcionalnost, kao što su laptopovi, PDA uređaji, mobilni telefoni novije generacije koji mogu da se povezuju na WiFi hot-spotove. Naime od UMTS Rel 6 predviđen je međurad UMTS tehnologije i WiFi tehnologije, što bi se moglo smatrati začetkom 4G mreže, [29].

8.1.2. Bluetooth

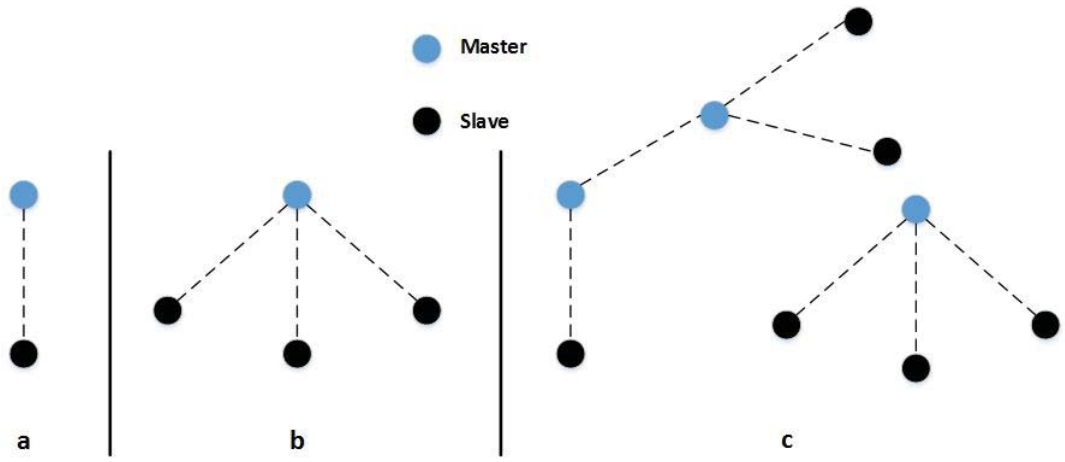
Bluetooth bežična tehnologija omogućava povezivanje prenosnih i stonih (desktop) računara, računarske opreme, mobilnih telefona i sl, na malim udaljenostima koje zavise od okruženja i od izlazne snage uređaja, kako je to prikazano u Tabeli 8.2.

Tabela 8.2: *Klase i dometi Bluetooth uređaja*

Klasa	Max izlazna snaga	Max. izlazna snaga	Očekivani domet	Domet u slobodnom prostoru
Klasa 1	100mW	20dBm	42m	300m
Klasa 2	2.5mW	4dBm	16m	50m
Klasa 3	1mW	0dBm	10m	30m

Bluetooth uređaji rade u frekventnom pojasu 2.4-2.4836 GHz u ISM opsegu. Raspoloživi opseg od 83.5 MHz se dijeli na 79 kanala širine 1MHz. Bluetooth koristi FHSS tehnologiju proširenog spektra. Kanal se dijeli na vremenske odsječke trajanja od 625 ms, a za svaki vremenski odsječak se koristi druga frekvencija skakanja, što rezultira frekvencijom od 1600 skokova u sekundi, [28], [30],[42], [79].

Bluetooth obezbjeđuje veze tačka-tački i tačka-više tačaka. Nekoliko Bluetooth uređaja koji koriste isti kanal (sekvencu skakanja) formiraju *picenot* mrežu. U toj mreži, kako je to prikazano na Sl.8.3 jedna jedinica se ponaša kao nadređena (master), a druga kao podređena (slave).



Slika 8.3: *Mrežna topologija Bluetooth-a*

U svakom je vremenskom odsječku moguća razmjena paketa između nadređene i podređene jedinice. Format paketa je prikazan na Sl.8.4.

Slika 8.4: *Format paketa kod Bluetooth-a*

Pristupni kod (72 bita) služi za identifikaciju i sinhronizaciju uređaja, zaglavlje (54 bita) nosi upravljačke informacije, dok je korisnički dio promjenjive dužine (0-2745 bita).

Definisane su dvije vrste fizičkih veza koje podržavaju prenos govora i podataka:

- sinhrona veza orijentisana na spajanje (SCO-Synchronous Connection Oriented) koja se koristi za prenos govora,
- asinhrona veza bez spajanja (ACL-Asynchronous Connectionless Link), koja se koristi za prenos podataka, sa protocima predstavljenim u Tabeli 8.3.

Tabela 8.3: *Moguće brzine podataka kod ACL veze*

Simetrično (kbit/s)	Asimetrično (kbit/s)	
108.8	108.8	108.8
172.8	172.8	172.8
256.8	384.0	54.4
384.0	576.0	86.4
286.7	477.8	36.3
432.6	721.0	57.6

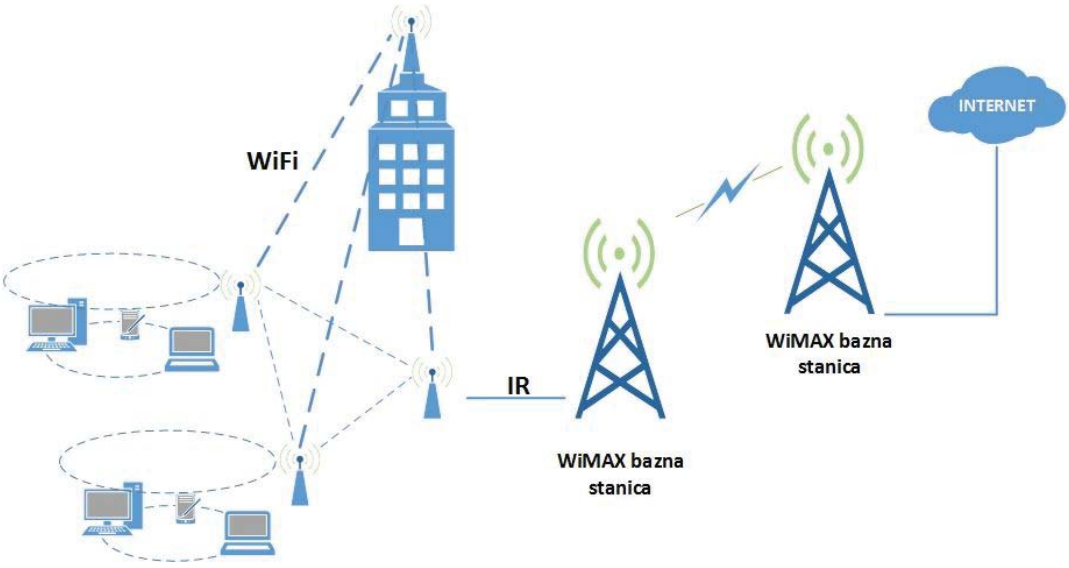
Bluetooth tehnologija je našla široku primjenu na svim mjestima gdje je potrebno da služi kao zamjena za kablovsko ožičenje i gdje je potrebno povezati korisnički terminal na postojeće mreže za prenos govora i podataka.

8.1.3. WiMAX

WiMAX (Worldwide Interoperability for Microwave Access) je baziran na standardu IEEE 802.16. WiMAX mreža može da omogući vezu između bazne stanice i korisnika na mnogo većim udaljenostima od WiFI-a, čak i do 50 km, ali su te udaljenosti u praksi dosta kraće i većinom su od 3-10 km, [79].

WiMAX omogućava velike protoke, čak i do 100 Mbit/s (u praksi znatno manje), tako da se može koristiti za širokopojasni pristup Internetu na mjestima gdje bi izgradnja žične infrastrukture bila skupa i neisplativa.

Može se koristiti u kombinaciji sa WiFi-em, pri čemu se WiMAX koristi za prenos podataka na većim udaljenostima, a WiFi za omogućavanje pristupa kućnim korisnicima, kako je to prikazano na Sl.8.5.



Slika 8.5: *Tipična primjena WiMAX mreže*

8.1.4. Karakteristike ćelijskih sistema mobilne telefonije

Da bi uvidjeli prednost ćelijskog sistema mobilne telefonije ukratko ćemo objasniti kako je radio klasični, [27], [75], [90].

Klasični mobilni telefonski sistem je funkcionisao na sledeći način: biranjem broja i uspostavljanjem veze korisnik zauzima jedan dupleksni radio-kanal tj. određeni frekvencijski opseg, koji se koristi u određenoj geografskoj zoni koja bi trebalo da bude što veća. To znači da emitovana snaga treba da ima maksimalnu moguću vrijednost koja je određena saveznim zakonom. Korisnik koji je započeo razgovor u jednoj zoni mora da ga obnovi kada ulazi u drugu zonu, jer će prethodni biti odbačen.

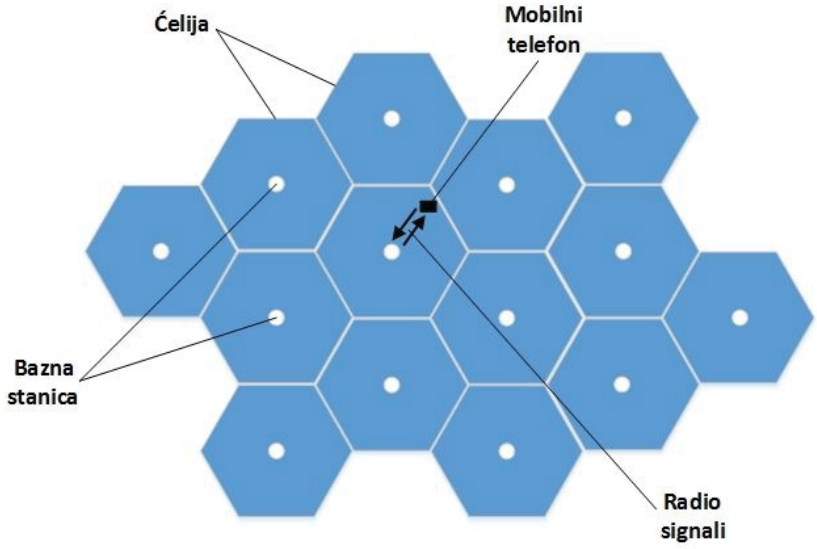
Centralni radio predajnik u baznoj stanici emituje signal velikom snagom obezbjeđujući veze sa mobilnim korisnicima i do 100 km od bazne stanice. Mobilni telefoni su bili veliki i sa velikom potrošnjom snage.

Kapacitet sistema je bio mali a postojala je velika mogućnost interferencije od drugih mreža i drugih izvora zračenja. Potrebno je oko 120 KHz za prenos jednog govornog kanala. Sa razvojem tehnologija frekventne modulacije, radio kanali su postajali uži i njihova širina je od 10-30 KHz. Kapacitet sistema je i dalje bio nedovoljan.

Još jedan nedostatak klasičnog sistema jeste da je broj aktivnih korisnika ograničen brojem kanala dodijeljenih datoj frekvencijskoj zoni. Što je veći broj korisnika, veća je i vjerovatnoća blokiranja.

Zagušenja u sistemu su i dalje česta, sa vjerovatnoćom blokade od 20%, a čak i znatno veća za vrijeme glavnog saobraćajnog časa.

Tako ostvarena usluga prenosa govora je bila veoma skupa.



Slika 8.6: *Teorijska ćelijska mrežna struktura*

Ćelijski sistem koristi princip *handoff*-a, (preuzmanja), koji predstavlja proces automatske promjene frekvencije ili kanala, kada se korisnik kreće iz jedne frekvencijske zone u drugu, tako da razgovor može da bude nastavljen bez ponovnog biranja.

Osnovni razlog uvođenja ćelijskog sistema mobilne telefonije je mogućnost višestruke upotrebe jednog kanala ili frekvencijskog opsega u okviru sistema i podjela geografske zone od interesa na autonomne oblasti, tj ćelije.

Ćelijske mreže koriste princip višestruke upotrebe radio frekvencija. Čitava oblast je podijeljena u regionalne ćelije (Sl.8.6) od kojih svaka ima baznu stanicu blizu centra ćelije kako bi se brinula o komunikaciji sa mobilnim stanicama (mobilnim telefonima). Baznim stanicama u susjednim ćelijama se dodjeljuju različiti frekvencijski opsezi kako bi se izbjegla interferencija signala.

Prethodna slika prikazuje kako se region oblasti pokrivanja dijeli u heksogonalne ćelije upotrebom uzorka u obliku saća i sedam različitih frekvencija. U realnom svijetu, oblik ćelije i njena veličina nisu regularni i zavise od osobina terena, karakteristika antena i gustine pretplatnika.

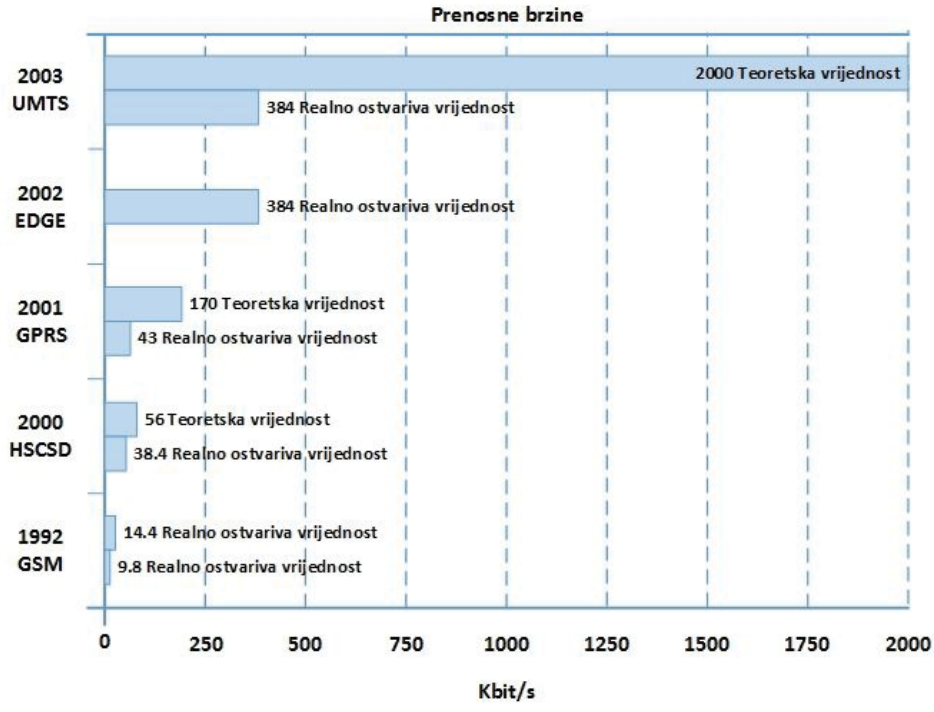
Na Sl.8.7 je prikazana evolucija ćelijskih mreža sa aspekta protoka koje su one omogućavale, [75].

GSM (Global System for Mobile Communications) je bio prvi pravi globalni sistem mobilnih komunikacija, ali kako se vidi sa Sl.8.7 omogućavao je jako male protoke, [24].

Poboljšanje je donijela HSCSD (High Speed Circuit Switched Data) tehnika koja je omogućavala korištenje više od jednog vremenskog slota za jednu konekciji (1-8). Novo kanalsko kodovanje povećava bitsku brzinu u jednom vremenskom slotu od 9,6 kb/s na 14,4 kb/s. HSCSD takođe obezbjeđuje mogućnost kombinovanja ovih vremenskih slotova tako da postoje raznovrsne bitske brzine u opsegu od 14,4 kb/s do 57,6 kb/s. Veće bitske brzine se mogu postići rezervisanjem više vremenskih slotova za jednog korisnika, [24].

Ali, kao i GSM i HSCSD je zasnovan i dalje na tehnici komutacije kola, pa su pristupna vremena paketskim mrežama (npr Internetu) i dalje velika (>30s), što predstavlja istu situaciju, kao kada pristupamo sa fiksne mreže upotrebom modema.

GPRS tehnologija (General Packet Radio Service) uvodi dva nova mrežna čvora u jezgro mreže (u odnosu na GSM i HSCSD) koja omogućavaju paketsku komutaciju i međurad sa vanjskim paketskim mrežama.



Slika 8.7: *Protok mobilnih ćelijskih mreža*

Dodavanjem nove modulacije i kodovanja GPRS-u nastaje EDGE (Enhanced GPRS) koji nudi značajno veću propusnu moć i kapacitet i često se u literaturi označava kao jedna od 2G+ tehnologija jer predstavlja prelaz ka UMTS-u (Universal Mobile Telecommunication System), kao 3G tehnologiji.

Dalji razvojni korak jeste spajanje mobilnih mreža i Interneta. IMS (IP Multimedi Subsystem predstavlja ključni elemenat 3G arhitekture, koji treba da omogući mobilni pristup svim iInternet servisima, [3].

U nastavku ćemo uraditi sledeće: prvo će se detaljno objasniti svi elementi GSM mreže koji su ujedno i elementi GPRS/EDGE mreže, da bi nakon toga pri objašnjavanju ovih tehnologija objašnjavali samo elemente u kojima se one razlikuju.

8.1.4.1. GSM

Postojeći mobilni GSM sistemi ne mogu komunicirati na udaljenostima većim od 35 km zbog toga što kašnjenje na većim udaljenostima prijemnog signala postaje suviše veliko. Slabljenje snage emitovanog signala ograničava ovu udaljenost na 10 km. Da bi se obezbijedila zadovoljavajuće pokrivenost mobilnim signalom neke oblasti potreban je veći broj ćelija, [70], [90].

Svaka ćelija ima jednu baznu stanicu, obično u centru ćelije, kako je to prikazano na Sl.8.5.

Dvije osnovne osobine ćelijske strukture:

- ponovno iskorištenje frekvencija (frequency reuse): bez ponovnog iskorištenja frekvencija ne bi bilo dovoljno prostora u spektru frekvencija za veoma veliki broj korisnika sistema,
- preusmjeravanje signala (handover, handoff): odnosi se na prebacivanje tekućeg poziva u druge kanale ili iz jedne ćelije u drugu; bez handovera pozivi bi bili ograničeni samo na jednu ćeliju.

Ponavljanje frekvencija je moguće na udaljenostima na kojima je nivo interferencije toliki da nije štetan po sistem. Stoga je potrebno ustanoviti grupe ćelija, tako da se u svakoj od njih koristi različit skup frekvencija. Ovakva grupa ćelija se naziva klaster.

Smanjenjem veličine klastera smanjuje se broj potrebnih frekvencija u mreži. Sa druge strane treba voditi računa da se smanjenjem veličine klastera smanjuje rastojanje između ćelija koje koriste isti skup frekvencija, pa se samim tim povećava mogućnost nastanka interferencije.

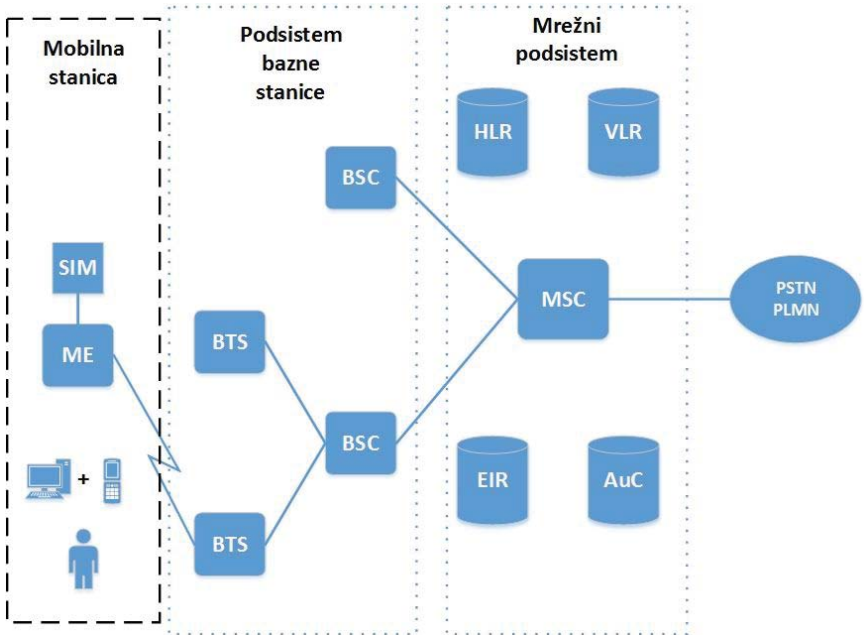
Prednosti celularnog koncepta:

- veliki kapacitet sistema,
- efikasno iskorištenje frekvencijskog spektra,

- veliko pokrivanje,
- prilagodljivost na različite gustine saobraćaja,
- pružanje niza kvalitetnih servisa korisnicima.

Arhitektura GSM mreže (Sl.8.8) je sastavljena od nekoliko funkcionalnih cjelina, čije su funkcije i interfejsi specificirani (naredna slika):

- mobilna stanica, MS (mobile station),
- podsistem bazne stanice (BSS Base Station Subsystem), koji uključuje dva elementa: baznu primopredajnu stanicu (BTS-Base Transceiver Station) i baznu kontrolersku stanicu (BSC-Base Station Controller),
- mrežni podsistem, čiji je glavni dio mobilni komutacioni centar (MSC-Mobile Switching Centre), koji obezbjeđuje komutaciju poziva između mobilnih korisnika i između korisnika mobilne i fiksne mreže.



Slika 8.8: *Arhitektura GSM sistema*

Mobilna stanica (MS) se može podijeliti u dva dijela; mobilnu opremu (ME), koja se ponekad naziva i terminalnom opremom i „pametnu karticu" (smart card) koja se naziva identifikacionim modulom pretplatnika (SIM-Subscriber Identity Module). SIM obezbjeđuje pokretljivost korisnika, tako da korisnik može pristupiti pretplatničkim servisima bez obzira na vrstu terminala.

Podsistem bazne stanice je sastavljen iz dva dijela: bazne primopredajne stanice i bazne kontrolerske stanice.

BTS omogućava slanje i primanje radio signala. Može da sadrži jedan ili više primopredajnika, koristi omnidirekcione ili usmjerene antene i ostvaruje komunikaciju sa mobilnom stanicom preko vazdušnog (Um) interfejsa.

U velikim urbanim oblastima, postojat će vjerovatno veliki broj BTS-ova.

BSC predstavlja mozak baznih primopredajnih stanica. Može da kontroliše više, čak desetine baznih stanica. Bazne stanice su povezane sa BSC-om preko Abis interfejsa.

Osnovne funkcije BSC-a su:

- rezervisanje frekvencija,
- uspostavljanje, održavanje i prekidanje poziva,
- iniciranje preusmjeravanja signala (handover-a),
- prijem mjernih podataka od MS-a (za vrijeme trajanja veze MS mjeri snage od okolnih BTS-ova i šalje informaciju o tome BSC-u) što omogućava kontrolu preusmjeravanja signala,
- kontrola snage zračenja MS-a (minimizacija interferencije, ušteda energije).

MSC je centralna komponenta mrežnog podsistema, centralni element dijela jezgra mobilne mreže koji se odnosi na komutaciju kola. Ona djeluje slično normalnom komutacionom čvoru i dodatno obezbjeđuje svu funkcionalnost koja je potrebna za rukovanje mobilnim pretplatnikom, kao što su:

- komutiranje poziva ka drugim mobilnim mrežama ili prema javnoj telefonskoj mreži,
- upravlja mobilnošću korisnika time što omogućava handover između dva BSC-a ili handover sa drugim MSC-om,
- vrši prikupljanje tarifnih podataka neophodnih za naplatu,
- upravlja mrežnim prolazom (MGW-Media Gateway), jedinicom koja ima ulogu komutacionog čvora i konverzije protokola, odnosno tehnologija (TDM/ATM/IP).

MSC koristi sledeće registre:

- matični registar lokacija (HLR-Home Location Registar): centralna baza podataka za sve korisnike matične mreže; čuva podatke sa SIM kartice:
    - IMSI (International Mobile Subscriber Identity): jedinstveni broj koji se nalazi na SIM kartici; IMSI se memoriše u HLR-u,
    - MSISDN (Mobile Subscriber ISDN Number) broj; MSISDN je broj pretplatnika u mobilnoj mreži; memoriše se u HLR-u; struktura MSISDN-a je slična strukturi E.164 broja,

- ključ za autorizaciju;
- promjenjivi podatci, kao što su podatci o lokaciji korisnika, aktiviranim dodatnim servisima, tip pretplate.

- registar lokacije posjetioca (VLR-Visited Location Registar): dinamička baza podataka koja sadrži informacije o trenutnim korisnicima u geografskoj zoni za koju je VLR zadužen,
- centar za provjeru autentičnosti (AuC-Authentication center) sadrži parametre neophodne za potvrdu poziva, odnosno vrši autentifikaciju podataka sa SIM kartice i većinom je dio HLR-a,
- registar identiteta opreme (EIR-Equimpment Identity Registar), čuva podatke o fizičkoj MS koja se koristi i tu se čuva IMEI broj (International Mobile Equipment Identity) koji predstavlja vrstu serijskog broja koji dodjeljuje proizvođač opreme fizičkom MS-u, odnosno mobilnom telefonu; samo korisnik sa validnim IMSI i IMEI brojem može učlaniti svoju MS u mrežu; EIR sadrži tri liste podataka:
  - bijela lista: lista svih MS-ova sa dobrim IMEI brojem,
  - crna lista: lista neispravnih i ukradenih mobilnih telefona,
  - siva lista: za MS-ove čiji je status neizvjestan.

Kod tradicionalnih bežičnih telefonskih mreža i PSTN-a govor se digitalizuje prije prenosa uz primjenu impulsne kodne modulacije (PCM), tako da se govor prenosi brzinom od 64 kbit/s. GSM koristi *Full Rate* govorni kodek za kompresiju govora u 13 kbit/s, *Enhanced Full Rate* za kompresiju govora u 12,2 kbit/ s i *Half Rate* od 5,6Kbit/s.

GSM je bio prvi pravi personalni mobilni komunikacioni sistem. Podržava međunarodni roaming, telefoniju, prenos podataka, SMS servis koji obezbjeđuje slanje kratkih tekstualnih poruka.

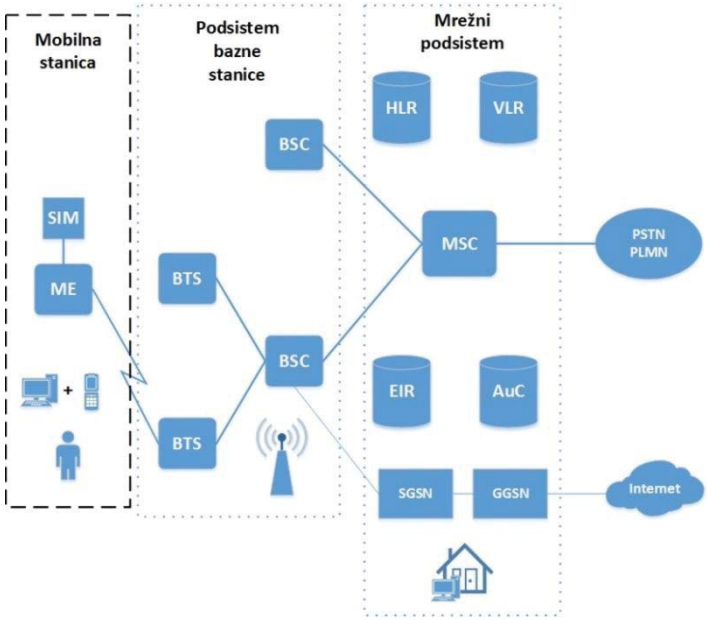
8.1.4.2. GPRS

O komponentama koje se koriste i u GSM-u ovdje nećemo ponovo govoriti, već ćemo se odmah osvrnuti na komponente koje su uvedene kod GPRS-a i nema ih u GSM-u i koje se mogu vidjeti na Sl.8.9.

Da bi se mogao integrisati GPRS u postojeću GSM arhitekturu, dodaju se nove klase mrežnih čvorova:

- SGSN (Serving GPRS Node) koji je odgovoran za raspodjelu paketa podataka od i do mobilnih stanica unutar svoje servisne oblasti; njegovi zadaci su: slanje upita HLR-u radi dobijanja informacija o pretplatniku, upravljanje mobilnošću pri prelazu pretplatnike iz jedne ćelije u drugu, detekcija nove bazne stanice unutar datog servisnog područja, registracija novog korisnika i određivanje njegove lokacije,

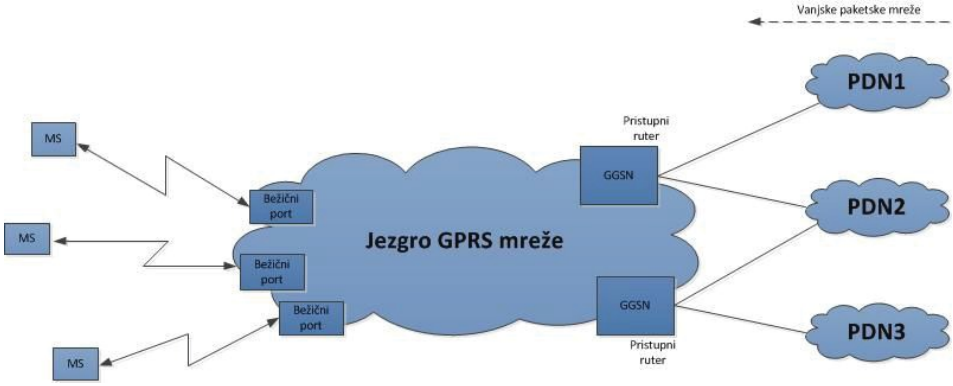
- GGSN (Gateway GPRS Support Node) djeluje kao interfejs između GPRS magistralne mreže i vanjske paketske mreže podataka, kao što je Internet;dakle, on ima zadatak rutiranja dolaznog i odlaznog saobraćaja ka drugim mrežama.



Slika 8.9: *Arhitektura GPRS sistema*

GPRS mreža se može posmatrati kao specijalna IP mreža budući da nudi IP konektivnost IP terminalim, omogućava IP rutiranje i interfejse ka drugim mrežama, [24].

Pristup vanjskim paketskim mrežama (PDN-Packet Data Network) se ostvaruje preko rutera, koji se u GPRS terminologiji označava kao GGSN, [70], [75].



Slika 8.10: *Veza sa vanjskim paketskim mrežama*

Upotreba šeme kodovanja kanala (CS) i broj vremenskih slotova određuju brzinu GPRS servisa.

Pristup korisnika udaljenom PDN-u je sličan ranijem „dial-up“ pristupu, s tim što korisnik može pristupiti bilo kojoj paketskoj mreži sa Sl.8.10 i što se korisniku naplaćuje iznos prenijetih podataka, a ne vrijeme trajanja konekcije.

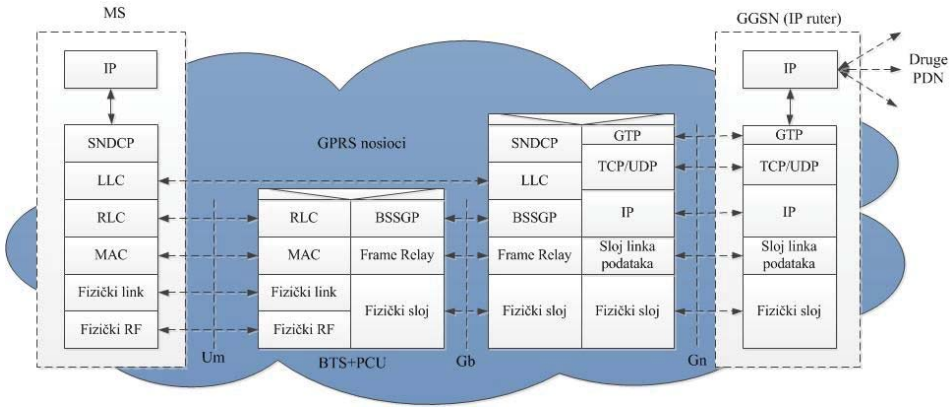
GPRS korisniku može ponuditi transparentan i netransparentan pristup PDN-u.

Kod transparentnog pristupa, ne zahtijeva se autentifikacija od strane udaljenog PDN-a i korisniku se dodjejuje IP adresa iz adresnog prostora GPRS mreže.

Kod netransparentnog pristupa, autentifikacija od strane PDN-a je obavezna i korisniku se dodjeljuje IP adresa od strane vanjske PDN mreže. Netransparentan pristup je pogodan za siguran pristup zaposlenima intranetu neke korporacije ili ISP-u kod koga je korisnik pretplaćen, [24], [70].

Važno je napomenuti, da se bez obzira na tip pristupa PDN-u, uvijek vrši autentifikacija od strane GPRS mreže prije nego što korisnik dobije dozvolu pristupa GPRS servisima.

Na Sl.8.11 dat je detaljan prikaz GPRS mreže. Krajnje lijevo se nalazi mobilna stanica (MS), a krajnje desno GGSN. Sa tačke gledišta MS-a, GGSN se može posmatrati kao udaljeni ruter.



Slika 8.11: *Protokoli GPRS-a*

Ovdje ćemo napomenuti da GGSN može predstavljati interfejs ne samo ka IP mrežama već i ka drugim PDN-ovima poput recimo X.25 mreže.

GPRS mreža obezbjeđuje GPRS nosioca, tj komunikacioni kanal sa određenim atributima između MS-a (terminala) i GGSN-a (rutera), putem kojega se vrši slanje IP paketa ka GGSN-u, odnosno prijem IP paketa od GGSN-a, [24], [70].

MS komunicira sa BTS-om preko Um interfejsa, koji obezbjeđuje uglavnom fizički nivo funkcionalnosti. Kod GPRS-a, BTS rukuje predajom i prijemom paketa podataka na

GPRS fizičkim kanalima. Podaci primljeni od BTS-a se obrađuju (npr. dekoduju) i usmjeravaju ka sledećem čvoru u GPRS arhitekturi, tj ka PCU-u (Packet Control Unit).

Zadatak PCU-a jeste da upravlja radio resursima i on je odgovoran za dodjelu resursa u u smijeru od korisnika ka mreži (uplink) i od mreže ka korisniku (downlink) na zahtjev MS-a. PCU komunicira sa SGSN-om preko Gb interfejsa. Kako je već rečeno GGSN obezbjeđuje funkciju upravljanja mobilnošću, upravljanja sesijom, rasporedom paketa u *downlink* smijeru i rutiranjem/tunelovanjem paketa. Interfejs između SGSN-a i GGSN-a se ostvaruje putem Gn interfejsa i on se zasniva na IPv4 protokolu.

GGSN uglavnom obezbjeđuje funkcije rutiranja i može se posmatrati kao interfejs ka vanjskim PDN-ovima, [24].

Ukratko ćemo objasniti uloge pojedinih protokola sa Sl.8.11.

SNDCP (Subnetwork Dependent Convergence Protocol) se pokreće između MS-a i SGSN-a. Prima IP datagrame za dalji prenos. Njegove osnovne namjene su:

- transportni servisi: sa potvrdom (acknowledged), povećana segurnost u odnosu na transportni servis bez potvrde (*nonacknowledledged*),
- kompresija TCP/IP zaglavlja,
- kompresija korisničkih podataka (prema V.42bis ili V.44),
- segmentacija/ponovno sastavljanje datagrama,
- multipleksiranje PDP koneksta.

Funkcija segmentacije/ponovnog sastavljanja, osigurava da dužina jedinice podataka koje se šalju ka LLC nivou ne prelazi maksimalnu dogovorenu vrijednost.

LLC (Logical Link Control) protokol se pokreće između MS-a i SGSN-a i obezbjeđuje servise linka podataka. U suštini LLC obezbjeđuje više logičkih linkova (Logical Links) između MS-a i SGSN-a i to:

- korisnički logički linkovi (User LL) za prenos korisničkih podataka između MS-a i SGSN-a; mogu raditi i u modu sa potvrdom i bez potvrde,
- kontrolni logički linkovi (Control LL) za prenos signalizacije, rade isključivo u modu bez potvrde.

RLC (Radio Link Control) i MAC (Medium Access Control) djeluju između MS-a i PCU-a. RLC podržava rad i u modu sa potvrdom i bez potvrde preko radio interfejsa. Omogućava segmentaciju i ponovno sastavljanje LLC jedinica podataka u fiksne RLC/MAC blokove. U modu sa potvrdom RLC omogućava pokretanje procedure za korigovanje greške, tokom koje je moguća selektivna retransmisija neuspješno isporučenih RLC/MAC blokova. Moglo bi se reći, da dok LLC obezbjeđuje transportne servise između MS-a i SGSN-a, RLC obezbjeđuje transportne servise između MS-a i PCU-a, [24], [70].

MAC sloj obezbjeđuje procedure koje omogućavaju da više radio stanica dijele zajedničke radio resurse koji se sastoje od više fizičkih kanala. U smijeru od MS-a do mreže (uplink), MAC sloj omogućava arbitražu između više mobilnih stanica koje istovremeno pokušavaju da pristupe prenosnom medijumu. U smijeru od mreže ka MS-u (downlink), MAC obezbjeđuje procedure za upravljanje redovima i opsluživanje paketa (queuing and scheduling) pristupa. Glavna funkcija MAC sloja u mreži jeste implementiranje funkcije opsluživanja paketima (u uplink smijeru), kojom se dodjeljuju resursi aktivnoj MS na način koji garantuje kvalitet servisa (QoS) za svaku MS, [24], [70].

BSSGP (Base Station Susystem GPRS Protocol) se pokreće preko Gb interfejsa. Osnovna namjena BSSGP-a jeste da obezbijedi nepouzdan transport LLC jedinice podataka između PCU-a i SGSN-a i kontrolu toka u *downlink* smijeru. Kontrola toka ima za cilj da spriječi prepunjavanje bafera u PCU-u da usaglasi prenosnu brzinu na Gb interfejsu (od SGSN-a do PCU-a) sa prenosnom brzinom na radio interfejsu (od PCU-a do MS-a). Nije obezbjeđena kontrola toka u uplink smijeru, jer se pretpostavlja da su uplink resursi na Gb-u optimalno dimenzionisani i da su značajno veći od uplnik resursa na radio interfejsu. BSSGP ne pruža pouzdan prenos, jer se pretpostavlja da je pouzdanost *frame relay* mreže dovoljno velika za zahtijevani nivo pouzdanosti na Gb interfejsu, [70].

GTP (GPRS Tunneling Protocol) djeluje između SGSN-a i GGSN-a, ali i između dva SGSN-a. GTP pruža nepouzdanu transportnu funkciju (obično djeluje iznad UDP-a) i obično se koristi za signalizacione funkcije koje se primarno koriste za upravljanje tunelovanjem i upravljanjem mobilnošću. GTP-ov transportni servis se koristi za prenos korisničkih IP datagrama kroz GTP tunele. GTP tuneli između SGSN-a i GGSN-a su neophodni za rutiranje.

GPRS može ponuditi i druge nestandardizovane servise, kao što je pristup bazama podataka, servisi slanja poruka, provjera kreditne kartice, elektronsko nadgledanje, sistemi prismotre i sl.

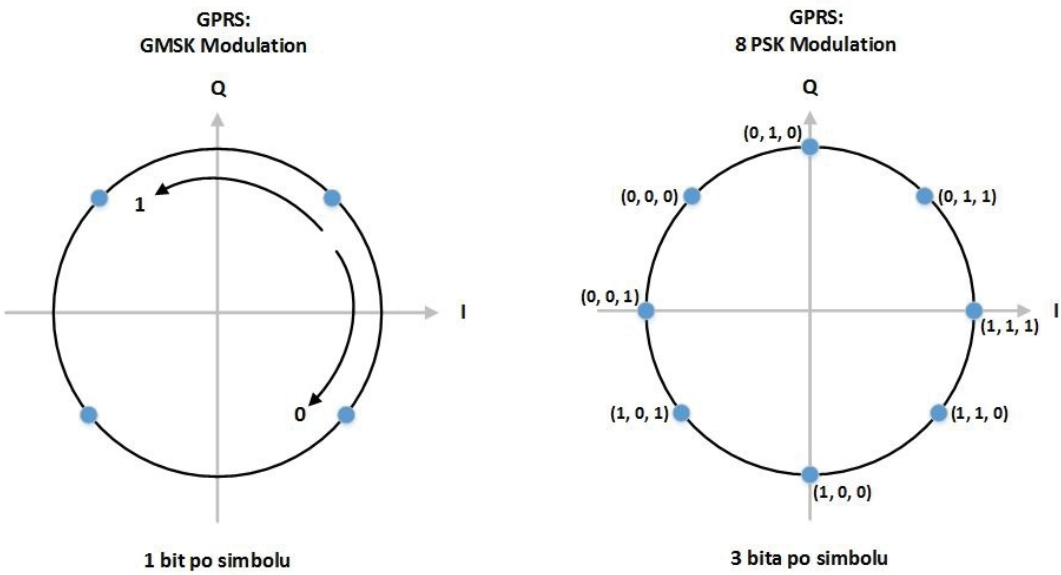
8.1.4.3. EDGE

EDGE (Enhanced GPRS) igra važnu ulogu u razvoju prema UMTS-u. Povećanje bitske brzine urađeno je promjenom kanalne kodne šeme i promjenom tehnike modulacije.

Modulaciona tehnika koja se koriste kod GSM-a je GMSK (Gaussian Minimum Shift Keying), koja predstavlja vrstu fazne modulacije. Ovo se može predstaviti I/Q dijagramom koji pokazuje realne (I) i imaginarne (Q) komponente prenošenog signala, kako je prikazano na Sl.8.12, dok se kod EDGE-a koristi 8PSK (8-*phase shift keying*).

8PSK modulacioni metod je linearni metod u kojem se tri uzastopna bita preslikavaju u jedan simbol u I/Q planu. Brzina simbola, ili broj poslatih simbola u određenom periodu

vremena ostaje isti kao za GMSK, ali sada svaki simbol predstavljaju tri bita umjesto jednog. Ukupna brzina podataka se stoga povećava sa faktorom tri, [13],[75], [90].



Slika 8.12: *GMSK i 8PSK modulacija*

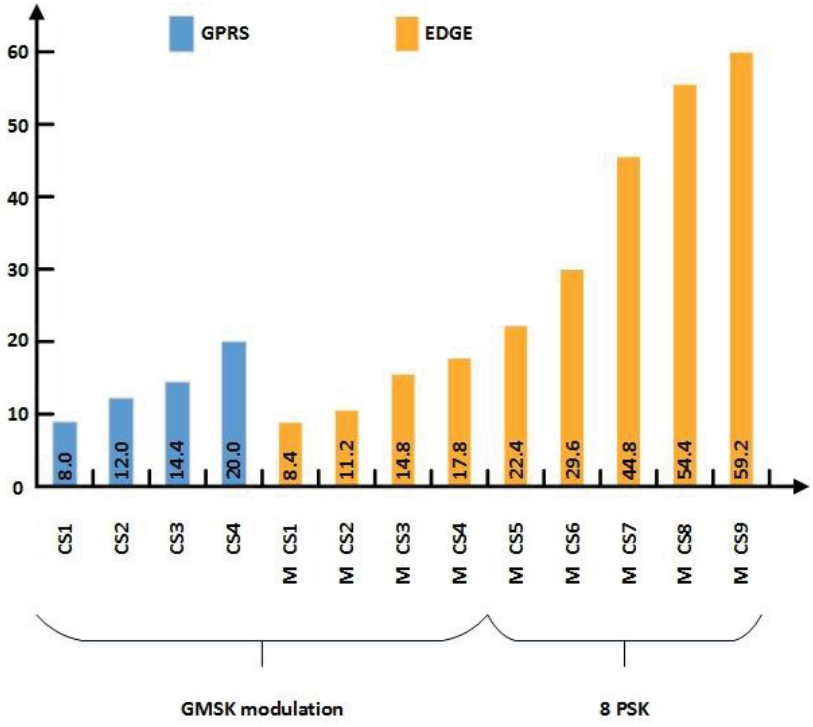
Razlika između različitih simbola je kraća upotrebom 8PSK modulacije u odnosu na onu kad se koristi GMSK. Kraća udaljenost povećava rizik od pogrešnog shvatanja simbola zbog toga što je mnogo teže za radio prijemnik da detektuje koji je simbol primljen. Pod dobrim radio uslovima, to nema značaja, međutim u lošim radio uslovima ima jer se dodaju ekstra biti radi kodovanja sa korekcijom greške. Samo u veoma lošem radio okruženju GMSK će biti efikasnija. Stoga su EDGE kodne šeme mješavina GMSK i 8PSK, [90].

Kodovanje kanala znači dodavanje detekcije greške i korekcije informacija podacima koji se prenose preko radio interfejsa.

Kod GPRS-a se koriste različite kodne šeme (Sl.8.13), koje se označavaju sa CS1 do CS4. Svaka ima različit iznos kodovanja za korekciju greške koja su optimizirana za odgovarajuća radio okruženja. Maksimalna brzina jednog vremenskog slota kad se ne koristi korekcija greške je 21.4 kbit/s (CS-4). Jedna mobilna stanica može koristiti do osam vremenskih slotova i maksimalna ukupna bitska brzina je 171.2 kbit/s. U stvarnosti brzina jednog vremenskog slota je 13.4 kbit/s i mobilne stanice koriste tri ili četiri vremenska slota.

Za EGPRS se uvodi devet modulacionih kodnih šema, koje se označavaju sa MCS1 do MCS9. One ispunjavaju isti zadatak kao GPRS kodne šeme. Četiri najniže kodne šeme

(MCS1 do MCS4) koriste GMSK, dok pet najviših koriste (MCS5-MCS9) 8PSK modulaciju.



Slika 8.13: *Modulacione kodne šeme kod GPRS-a i EDGE-a*

I GPRS CS1 do CS4 i EGPRS MCS1 do MCS4 koriste GMSK modulaciju sa neznatno različitim performansma propusne moći. Ovo je usljed razlika u veličini zaglavlja (i veličini *payload*, odnosno korisnog dijela) EGPRS paketa. Ovo čini mogućim resegmentiranje EGPRS paketa. Paketi koji su poslani sa višom kodnom šemom (manjom korekcijom greške) u slučaju da se ne prime ispravno se ponovo šalju sa nižom kodnom šemom (većom korekcijom greške) ako to zahtijeva novo radio okruženje, [90].

8.1.4.4. UMTS

Motivisanost provajdera servisa za uvođenje nove generacije tehnologije zavisi od očekivanih prihoda i od toga koliki je iznos očekivanih početnih ulaganja.

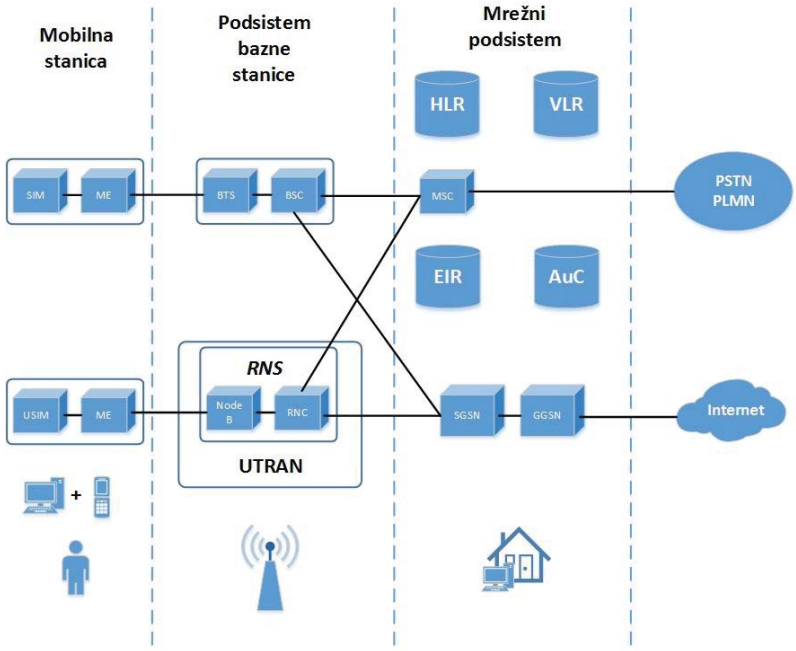
Prema Nokinim procjenama troškovi nadgradnje postojeće GSM/GPRS mreže ka UMTS-u će biti između 10% i 40% više u odnosu na početna ulaganja pri izgradnji GSM mreže sa približno istom pokrivenošću kao kod UMTS mreže.

Dilema: da li ostati na EDGE-u ili investirati u UMTS?

EDGE obezbjeđuje tri do četiri puta veću brzinu podataka od GPRS-a, koja je dovoljna da se osiguraju širokopojasni servisi podataka, [13], [66], [75], [90].

Prva faza UMTS-a jeste R99.Najznačajnija promjena koju je R99 ponudio je nova radio pristupna mreža, UTRAN (UMTS Radio Access Network), [13].

UTRAN koristi WCDMA (Wideband Code Division Multiple Access) i TD/CDMA (Time Division/CDMA) tehnologije radio pristupa. WCDMA se koristi za primjenu u širokim područjima sa velikom mobilnošću, dok se TD/CDMA koristi u područjima sa malom mobilnošću (unutrašnjosti zgrada), [66], [90].



Slika 8.14: *Arhitektura UMTS mreže*

Pojednostavljena arhitektura UMTS sistema je data na Sl.8.14.

UTRAN je podijeljen na individualne radio mrežne podsisteme (Radio Network Subystem-RNS) koji se vezuju na jezgro mreže preko Iu interfejsa.

Uvedena su i dva nova mrežna elementa : RNC i čvor B.

Radio mrežni kontroler (RNC-Radio Network Controller) omogućava autonomno upravljanje radio resursima UTRAN-a. On obezbjeđuje iste funkcije kao GSM BSC i odgovoran je za centalizovan rad i održavanje (O&M) čitavog RNS-a sa pristupom OSS-u (Operation Support System) koji se sastoji od centra za rad i održavanje i ima zadatak daljinskog i centralizovanog rada, administracije i održavanja.

Čvor B je fizička jedinica za radio prenos/prijem sa ćelija. Čvor B mjeri kvalitet i snagu konekcije i o tome obavještava RNC. Čvor B učestvuje takođe u kontroli snage tako što omogućava podešavanje snage UE-a.

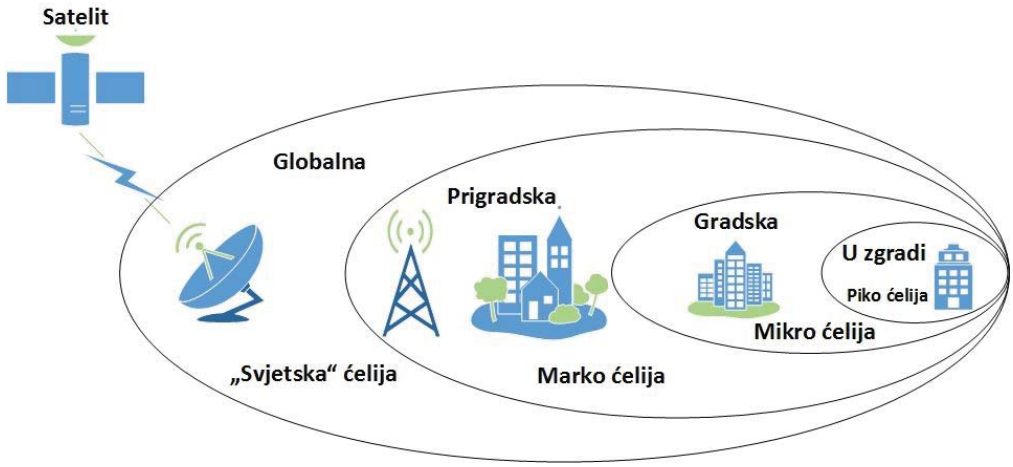
USIM (Universal SIM) jeste identifikacioni modul pretplatnika koji se koristi kod 3G mreža umjesto SIM-a (mada može i obični SIM), jer su primjenom USIM-a dostupne neke nove mogućnosti, poput ostvarivanja video poziva (naravno za oblasti pokrivene signalom 3G mreže), bolji sigurnosni algoritmi, veći telefonski imenik i sl.

UMTS koristi visoke frekvencije od 2000 MHz što će još više doprinijeti smanjivanju ćelija. Suštinska razlika u odnosu na GSM je u tome što kod UMTS-a sve susjedne ćelije koriste iste frekventne kanale za komunikaciju. Pošto UMTS koristi WCDMA neće doći do uzajamnog uticaja susjednih ćelija.

Kod WCDMA maksimalni protok zavisi od prenošene snage a time znači i od udaljenosti pretplatničke opreme od zemaljske stanice. Što je veća ćelija to je manji protok koja dolazi na kraj ćelije.

Zavisno od oblasti koja se želi pokriti signalom, kao i od protoka koji se želi pružiti, razlikujemo sledeće vrste UMTS ćelija:

- za ruralne oblasti i velike oblasti pokrivanja koriste se makro ćelije i maksimalni protoci kod tih ćelija su 144 kbit/s,
- mikro ćelije za oblasti prečnika od 100 do 250 metara i sa maksimalnim protocima od 384 kbit/s,
- piko ćelije su prečnika do 50 m i sa protocima od 2 Mbit/s.



Slika 8.15: *Hijerarhijska ćelijska struktura uz upotrebu piko, mikro, makro i svjetskih ćelija*

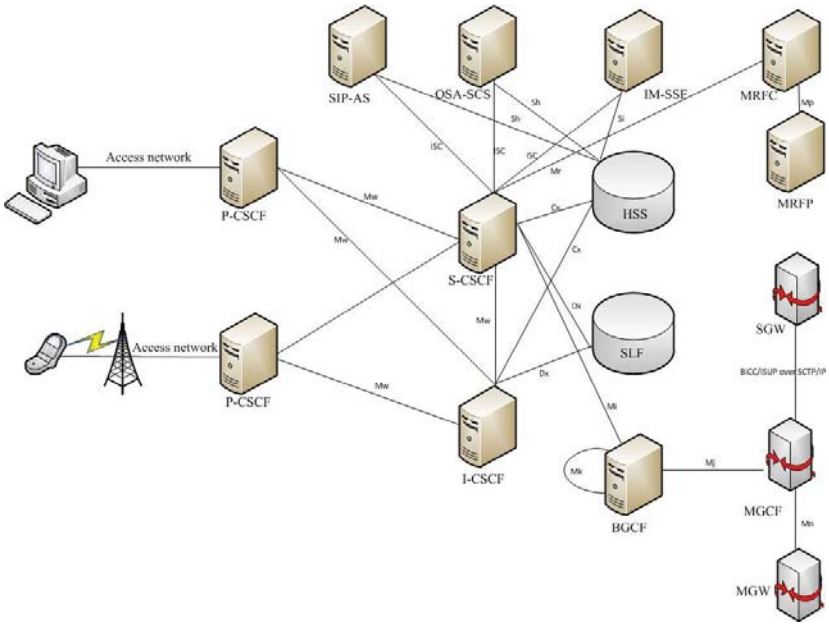
5.1.2.3.2. IMS

IMS je prvobitno bio namijenjen samo za mobilne mreže. Osnove IMS-a su date od strane 3GPP (Third Generation Partnership Project) organizacije u SW Release 5. Od SW Release 6 i 7, omogućen je pristup IMS-u i sa drugih bežičnih mreža kao što su WLAN (Wireless LAN) i WiMAX (Worldwide Interoperability for Microwave Access), ali i pristup IMS-u sa fiksne mreže, što je praktično dovelo do integracije fiksnih i mobilnih mreža i Interneta. Budući da se IMS bazira na IP protokolu, koncept „all-IP mreže“ postaje moguć i praktično ostvariv, [13].

Putem IMS-a, pretplatnik ima mogućnost pristupa svim registrovanim servisima i aplikacijama, bez obzira na pristupnu tehnologiju jer IMS omogućava jedinstven mehanizam identifikacije pretplatnika i njihov pristup registrovanim servisima bez obzira na tip pristupne mreže. Uz to, moraju biti ispunjeni zahtjevi u pogledu odgovarajućeg kvaliteta servisa (QoS) i mogućnosti ostvarivanja *roaming*-a. IMS omogućava i brzo kreiranje servisa bez potrebe za dodatnom standardizacijom, [3], [91].

Posebna pažnja se mora obratiti na sigurnost jer IMS-u se može pristupiti sa različitih pristupnih mreže koje mogu imati različite stepene sigurnosti (access security). Uvođenjem zaštite koja se ostvaruje na nivou samog IMS-a (network security), nadoknađuje se nedovoljan stepen sigurnosti kod pojedinih pristupnih mreža, [11].

Sa Sl.8.16 se vidi da pretplatnik pristupa paketskoj GPRS mreži preko radio pristupne mreže (RAN-Radio Access Network), ali je prikazano i to da korisnik može pristupiti IMS-u i sa drugih (ranije nabrojanih) pristupnih mreža, što je omogućeno od SW Release 6 i 7, [3].



Slika 8.16: *IMS Release 5*

8.2. WAP protokol stek

Uvođenjem 3G mreža, brzina prenosa podataka se značajno povećala i to predstavlja dobru osnovu za mnogo savršeniji mobilni Internet nego što je to bilo moguće putem GPRS-a i donekle EDGE-a. Mobilni Internet ne znači samo pristup Internetu putem mobilnog uređaja, nego i personalizovanim uslugama sa bilo kog mjesta i u bilo koje vrijeme, [19], [75], [80], [81], [83].

Pristup Internetu omogućava WAP (Wireless Aplication Protocol). WAP predstavlja skup protokola (protokol stek kako smo ga ranije definisali u Poglavlju 2) koji omogućava pristup Internet servisima i pretraživanje veba putem mobilnog uređaja, prvenstveno mobilnih telefona. Nedostaci koji su bili prisutni kod mobilnih uređaja druge generacije:

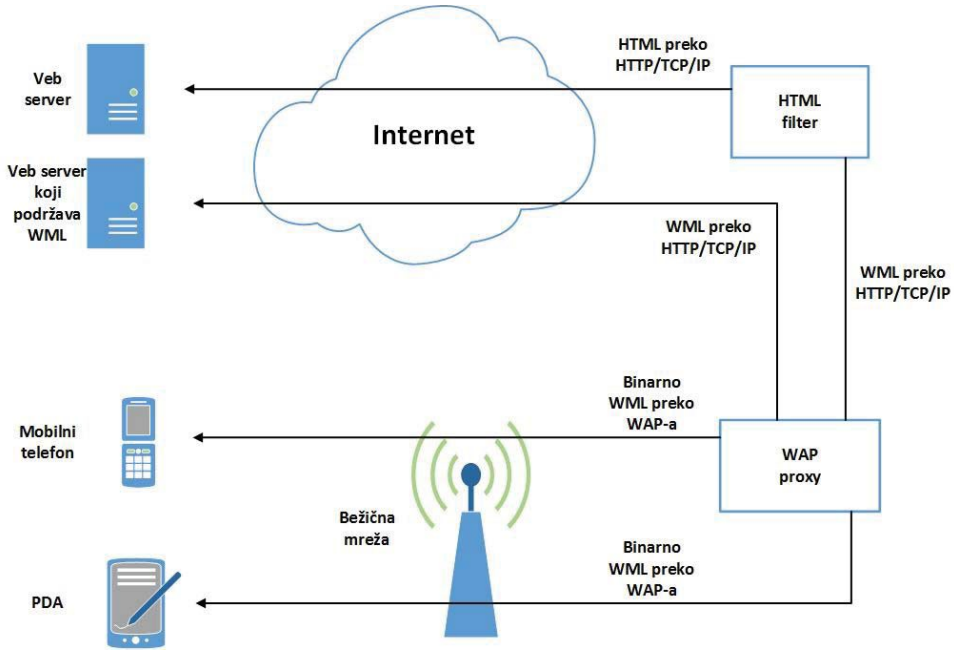
- mala brzina prenosa podataka,
- ograničena snagu baterije,
- nizak kvalitet servisa (QoS) preko bežičnih linkova,
- ograničena snagu procesiranja i ograničeni memorijski resursi,
- mala veličina ekrana mobilnog telefona.

većim dijelom su otklonjeni, ali ne i u potpunosti. Tu se ogleda značaj WAP-a tako da bismo mogli reći:

Def.: *WAP je konstruisan kako bi odgovorio zahtjevima i ograničenjima mobilnih mreža i uređaja druge generacije.*

Def.: *WAP predstavlja skup standarda koje bežičnim aplikacijama osiguravaju standardno Internet okruženje. WAP ima zadatak da prilagodi Internet sadržaj tako da se on ne može predstaviti na mobilnom uređaju.*

Na samom početku razvoja WAP-a postojala je ideja da se obezbijedi filtriranje u realnom vremenu HTML dokumenata i njihovo prevođenje u WML, tako da su postojala dva načina dobijanja WAP sadržaja: ili direktno preko servera ili preko filtra (Sl.8.16).



Slika 8.17: *Dobijanje sadržaja preko WAP-a*

Budući da se takvo prevođenje pokazalo neefikasnim ideja se napustila. Ta ideja je postojala još kod 1.1 verzije WAP-a, potom je slijedila 1.2 a danas je u upotrebi 2.0.

WAP aplikacije koriste klijent-server model koji je gotovo identičan klijent-server modelu Interneta koji smo objasnili u Poglavlju 2. Klijent kod WAP-a nije personalni računar nego mobilni uređaj koji koristi WAP. WAP uređaji imaju mikro-čitač (micro-browser) pomoću koga se mogu pregledati aplikacije i sadržaji koji se nalaze na udaljenom serveru. Način dobijanja sadržaja preko WAP protokol steka je prikazan na Sl.8.16.

8.2.1. WAP 2.0

WAP forum je razvio WAP 2.0 kako bi približio svijet bežičnih komunikacija Internetu. Sa realizacijom WAP 2.0, WAP forum je uspješno ispunio nekoliko zadataka:

- dao je podršku standardnim Internet komunikacionim protokolima; WAP 2.0 obezbjeđuje podršku za protokole kao što su: IP, TCP i HTTP; ovim je omogućeno bežičnim uređajima da iskoriste postojeće Internet tehnologije,
- nastavlja rad WAP 1.0 protokola dozvoljavajući aplikacijama i servisima da rade preko svih postojećih vazdušnih interfejsnih tehnologija i njihovih nosioca (Slika 8.18); ovo uključuje nove tehnologije velikih brzina kao što su GPRS i UMTS,

- obezbjeđuje bogato aplikaciono okruženje, koje omogućava raspodjelu informacija i interaktivnih servisa digitalnim mobilnim telefonima, pejdžerima, ličnim digitalnim asistentima (PDA–Personal Digital Assistant) i drugim bežičnim uređajima;

- mnoge osobine koje predstavljaju ograničavajući faktor kod upotrebe bežičnih uređaja, kao što su mali ekran, ograničeno vrijeme trajanja baterije, ograničeni RAM i ROM (neki od hardverskih nedostataka) kao i interfejsi (poput „one-finger“ navigacije) su poboljšane,

- minimizira se upotreba snage procesiranja uređaja i optimiziraju se mrežni resursi, kako bi se minimizirali troškovi i poboljšale performanse.

WAP forum je tijesno sarađivao sa organizacijama kao što su W3C (World Wide Web Consortium) i IETF (Internet Engineering Task Force) kako bi razvio specifikacije koje će odgovoriti gornjim zahtjevima. WAP 2.0 predstavlja pokušaj WAP foruma da primijeni poslednje Internet standarde i protokole.

8.2.1.1. Struktura WAP 2.0. protokol steka

Zbog ograničene širine propusnog opsega WAP sadržaj se koduje prije slanja bežičnom vezom, , [52],[90].

Kada klijent pokuša pristupiti određenom veb sajtu unošenjem odgovarajuće URL adrese, WAP vrši kriptovanje zahtjeva i bežičnom vezom ga šalje WAP mrežnom prolazu.

WAP-ov mrežni prolaz pretvara sadržaj u uobičajeni HTTP zahtjev koji se prosleđuje URL serveru preko Internet mreže. Server vraća WML/WMLScript ili XHTML dokument mrežnom prolazu koji ga kriptuje i prosleđuje mobilnom uređaju (postupak sličan onom na Sl.7.2).

Na Sl.8.18 je dat WAP protokol stek, dok je na Sl.8.19. dato poređenje Internet i WAP arhitekture, radi lakšeg razumijevanja pojedinih protokola iz WAP protokol steka.

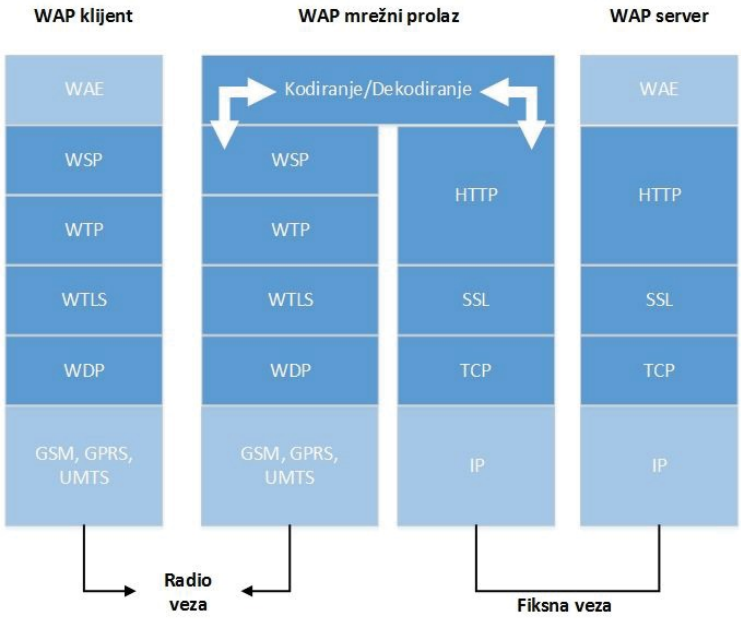
WAP protokol stek se može posmatrati kao zajednička platforma, način za implementiranje bilo kog servisa preko „browser-style“ interfejsa koji se zasnivaju na WML-u (Wireless Markup Language) koji se koristi za izradu WAP stranica. Uloga WML-a u mobilnim internet aplikacijama je ista kao uloga HTML-a u veb aplikacijama, naime WAP sajtovi se pišu u WML-u. WML predstavlja jezik za obilježavanje koji se počeo koristiti u WAP 1.x specifikaciji. WML jezik ima zadatak da implementira klijentski interfejs na bežični uređaj i optimiziran je za izradu veb sadržaja koji je kompatibilan WAP-u. WML jezik se zasniva na XML jeziku (Extensible Markup Language).

XML omogućava prilagođenje istog sadržaja ekranima različitih mobilnih uređaja, bez obzira na njihovu veličinu, font i mogućnosti prikaza boja, što pruža prednost veb dizajnerima jer njegovom primjenom se ne moraju praviti različite verzije programa za svaki model bežičnog uređaja.

Danas je aktuelna verzija WAP 2.0 sa jezikom XHTML. Taj jezik predstavlja kombinaciju HTML i XML jezika i čini prelaz između sada već tradicionalnog HTML jezika koji se koristi na vebu i jednostavnijeg i pristupačnijeg XML jezika

Zašto se HTML koji se koristi kod veba ne koristi kod WAP-a? HTML ne razlikuje sadržaj od prezentacije i zbog toga nije koristan u WAP aplikacijama.

WMLScript jezik omogućava dizajnerima da se informacije koje unosi klijent obrađuju na klijentskoj strani, radije nego da se te informacije šalju WAP mrežnom prolazu na obradu.



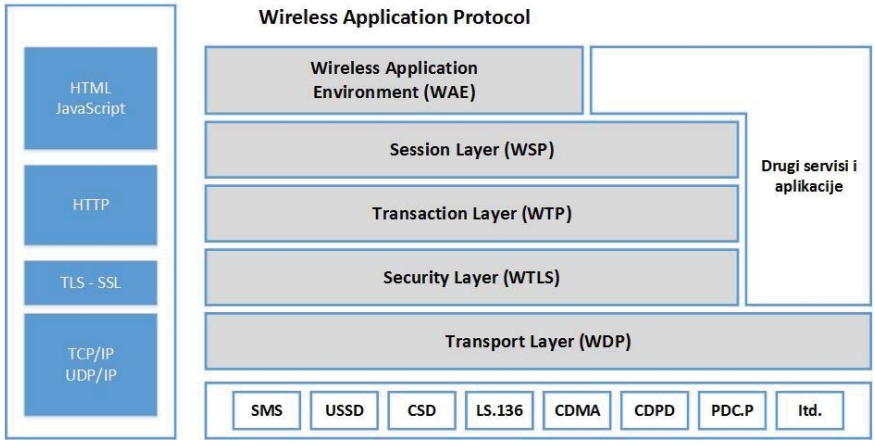
Slika 8.18: *Protokol stek WAP 2.0*

Funkcije pojedinih protokole iz steka (Sl.8.18) su:

- Wireless Application Environment (WAE) obezbjeđuje međusobni rad između WAP/Web aplikacija i bežičnih uređaja koji sadrže WAP-ov mikro-čitač, dakle WAE uključuje mikro-čitač, WML i WML Script jezike,
- Wireless Session Protocol (WSP) osigurava okruženje spremno za transakciju; to uključuje proces pregovaranja klijentske i serverske strane o zajedničkom nivou funkcionalnosti protokola i kodiranja; WSP omogućava ponovno uspostavljanje veze u istom kontekstu u kojem je bila u trenutku kad je veza obustavljena;

omogućava i višestruku vezu, odnosno prebacivanje sa GPRS veze (čitanje pošte) na UMTS vezu (video konferencija) i ponovno vraćanje na GPRS vezu,

- Wireless Transaction Protocol (WTP) je dizajniran kao transakciono orijentisani protokol za mobilne uređaje s malom memorijom i procesorskom snagom; optimizovan je za rad preko bežične veze; to uključuje upravljanje potvrdama i retransmisijom izgubljene informacije; neke korist od upotrebe WTP-a su:
  - poboljšanje pouzdanosti datagramskih servisa; WTP olakšava višem nivou retransmisiju i potvrdu koja je neophodna kad se koristi datagramski servis,
  - poboljšana efikasnost preko spojno orijentisanih servisa; WTP nema eksplicitnu fazu uspostave ili raskidanja veze,
  - prednost upotrebe protokola orjentisanog na slanje poruka, koji je konstruisan za servise orjentisane prema transakcijama kao što je „prelistavanje“.
- Wireless Transport Layer Security (WTLS) je konstruisan da obezbijedi privatnost, integritet podataka i autentifikaciju između dvije komunikacione aplikacije; WTLS obezbjeđuje interfejs za održavanje (kreiranje i završavanje) sigurnih veza; on obezbjeđuje funkcionalnost sličnu TLS 1.0 (protokolu koji se obično koristi na Internetu) i inkorporira dodatne osobine kao što su podrška prenosu datagrama i optimizirano rukovanje;
- Wireless Datagram Protocol (WDP) je servis za prenos datagrama, koji nudi konzistentan servis gornjim nivoima protokola i komunicira transparentno preko jednog od raspoloživih nosećih servisa, datih na Sl.8.18 (SMS, USSD,...).



Slika 8.19: *Poređenje Internet i WAP arhitekture*

POGLAVLJE 9

Sigurnost Interneta

Internet je, kako smo vidjeli u ranijim poglavljima, evoluirao tako da bismo mogli reći da on danas predstavlja najveću informaciono-telekomunikikaciono-poslonu platformu. U prethodnim poglavljima smo se bavili najviše sa prva dva aspekta. Međutim, kako danas Internet predstavlja osnovu e-poslovanja, pa se broj transakcija putem Interneta ali i vrijednost transakcija sve više povećava, to bi u ovom poglavlju morali nešto reći o bezbjednosti Interneta. Reći ćemo prvo nešto o osnovnim postulatima infomacione sigurnosni, a zatim ćemo ukratko predstaviti neke od sigurnosnih protokola koji djeluju na različitim nivoima TCP/IP protokol steka.

9.1. Osnovni ciljevi mjera bezbjednosti u informacionim sistemima

Internet je otvorena mreža, čija struktura i protokoli ne pružaju dovoljno bezbjednosti i sajber kriminal postaje sve značajniji problem, kako za organizacije, tako i za pojedince. Nije svaki oblik sajber kriminala direktno vezan za novac, u nekim slučajevima cilj je samo da se naruši ili blokira veb sajt a ne direktna krađa novca, robe i usluga.

Pored implementacije kvalitetne računarske mreže, mora se voditi računa i o obezbjeđenju sigurnosti mreže od raznih oblika napada i ometanja koje mogu poteći iz okruženja našeg informacionog sistema, [54].

Osnovni ciljevi mjera bezbjednosti u informacionim sistemima su:

- povjerljivost: obezbjeđuje se nedostupnost informacija neovlaštenim licima,
- integritet: obezbjeđuje se konzistentnost podataka, sprečava neovlašteno generisanje, promjena i uništenje podataka,
- dostupnost: obezbjeđuje se da ovlašteni korisnici uvijek mogu da koriste servise i da pristupe informacijama,
- upotreba sistema isključivo od strane ovlaštenih korisnika: resursi sistema se ne mogu koristiti od strane neovlaštenih osoba niti na neovlašten način.

9.1.1. Metode i nivoi zaštite

Zaštita sistema i održavanje sigurnosti sistema zahtjeva velika ulaganja, te je stoga uvijek potrebno težiti kompromisu između potrebnih ulaganja i smanjenja mogućnosti štete koja može nastati. Potrebno je odrediti tačku u kojoj se postiže ravnoteža ulaganja i efekata. Takođe je potrebno imati u vidu da sigurnosni mehanizmi ili procedure vrlo često negativno utiču na performanse sistema.

Postoji nekoliko pristupa i podjela kada je riječ o metodama zaštite, ali ćemo izdvojiti sledeću podjelu:

- fizička i organizaciona zaštita i sigurnost: predstavlja klasični sistem zaštite i to je prvi korak koga treba primijeniti u programu zaštite i odnosi se na metode koje se primjenjuju na zaštitu objekta i njegove okoline kao i pravila ponašanja svih onih koji dolaze u dodir sa objektom koji se čuva,
- hardversko-softverka zaštita i sigurnost: odnosi se na korištenje standardnih hardversko-softverskih mogućnosti sistema i pratećih uređaja razvijenih i

ugrađenih od strane proizvođača opreme koje može dopuniti i modifikovati sam korisnik; hardverska zaštita se koristi kod zaštite memorije i telekomunikacija; softverska metoda zaštite se koristi kod zaštite programskih paketa, datoteka, U/I operacija i eventualno prenosa podataka,

- administrativna kontrola zaštite i sigurnosti: predstavlja nadogradnju fizičkih mjera zaštite; pod administrativnom kontrolom podrazumijevamo kontrolu i organizaciju baze podataka, kontrolu i evidenciju broja izvještaja i njihovih korisnika, kontrolu izlaznog materijala, kontrolu i evidenciju pristupa podacima unutar sistema, kontrolu pristupa putem lozinki i šifri koje treba pravilno upotrebljavati i periodično mijenjati, te kontrolu dokumentacije o sistemu, programima, načinu djelovanja i sl,

- komunikaciona zaštita (kriptozaštita) i sigurnost: koristi se za zaštitu podataka koji se prenose komunikacionim linijama unutar umreženih sistema; najčešće metode zaštite su: kriptografska zaštita, korištenje specijalnih uređaja za promjenu signala (skremblovanje), korištenje „smart“ kartica i sl.

Kada je riječ o nivoima zaštite, oni se definišu u odnosu na pozicioniranje mehanizama zaštite u računarskom ili informacionom sistemu ili računarskoj mreži. Stoga imamo sledeće nivoe:

- zaštita na nivou aplikacije: softverska zaštita aplikacije (na primer, zaštita od prekoračenja bafera), izolovanje kritičnih aplikacija na namjenskim *host*-ovima, primjena specifičnih protokola,

- zaštita na nivou operativnog sistema: minimalna zaštita obuhvata: blokiranje nepotrebnih servisa (npr. ftp), obezbeđivanje sveobuhvatne i obavezne kontrole pristupa na nivou korisnika, obezbjeđivanje integriteta softvera koji čine operativni sistem (većina sigurnosnih napada usmjerena je na operativne sisteme bez primjenjenih zakrpa, pa je zato potrebno redovno ažurirati sve elemente sistema njihovim zakrpama),

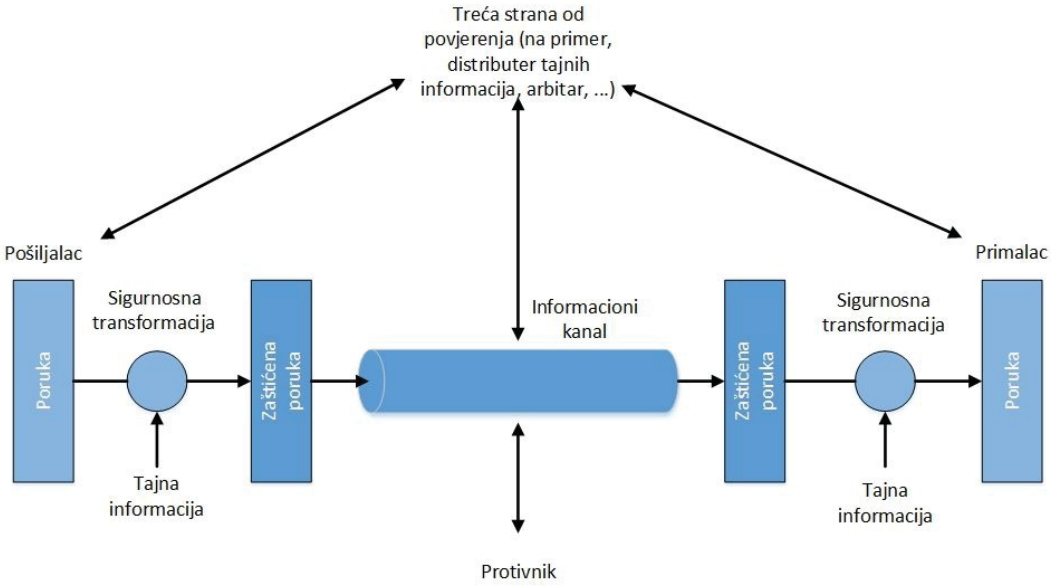
- zaštita na nivou mrežne infrastrukture: primjena mrežnih barijera (firewall-ova), blokiranje nepotrebnih portova, šifrovanje putanje, izolovanje putanje pomoću rutera i komutatora ili pomoću posebne infrastrukture,

- proceduralna i operativna zaštita: zaštitne polise, detekcije napada, upravljanje konfiguracijom sistema i obrazovanje korisnika.

9.1.2. Modeli mrežne sigurnosti

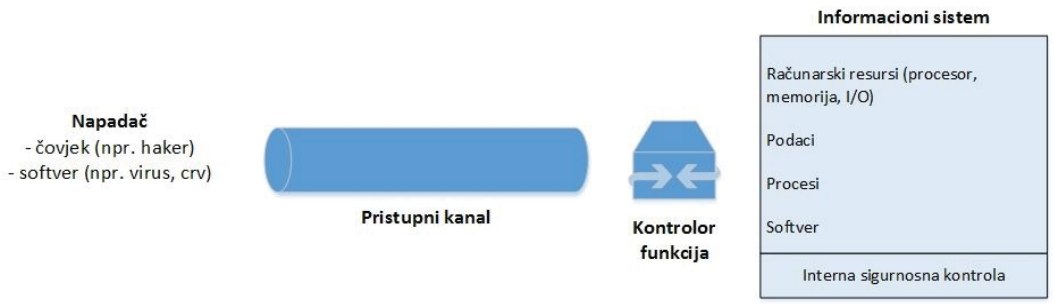
Izdvajaju se dva modela mrežne sigurnosti i to model sa nesigurnim komunikacionim kanalom i model sigurnog pristupa mrežnim resursima, [90].

Prvi model (Sl.9.1) predstavlja razmjenu informacija između dva učesnika preko nesigurnog komunikacionog kanala formiranog kroz Internet kao globalnu mrežu. Uvijek postoji mogućnost potencijalnog napada na ovaj komunikacioni kanal Oba učesnika primjenjuju sigurnosnu transformaciju sa odgovarajućim tajnim informacijama, koje obezbjeđuje treća strana kojoj vjeruju oba učesnika u komunikaciji čime se komunikacioni kanal štiti od napadača, jer napadač ne zna i ne može da dobije skrivenu informaciju. Sigurnosna transformacija može biti šifrovanje sa javnim ključem, a lice od povjerenja neka ustanova koja će učesnicima u komunikaciji distribuirati javne ključeve i obezbjeđivati potvrdu između identiteta učesnika i ključa (pomoću sertifikata);



Slika 9.1: *Model sa nesigurnim komunikacionim kanalom*

Drugi model (Sl.9.2) se odnosi na kontrolisanje pristupa podacima ili resursima računarskog sistema, u prisustvu potencijalnih napadača; ovaj model je zasnovan na odgovarajućoj kontroli pristupa unutar samog sistema (na primjer, liste za kontrolu pristupa datotekama na disku, prava dodijeljena korisnicima nad nekom bazom podataka) i takozvanom „kontroloru“ (gatekeeper), tj. zaštitnom mehanizmu koji kontroliše pristup sistemu spolja (na primjer, mrežna barijera koja obezbjeđuje pristup samo određenim mrežnim servisima) kako bi se obezbijedila adekvatna sigurnost;u ovom modelu se, takođe, mogu koristiti neke od kriptografskih tehnika zaštite.



Slika 9.2: *Model sigurnog pristupa mrežnim resursima*

9.2. Prijetnje sigurnosti sistema

Postoji mnogo načina na koje se može ugroziti sigurnost računarskog sistema, ali se generalno napadi mogu svrstati u dvije osnovne kategorije, a to su aktivni (active attack) i pasivni (passive attack) napadi.

Aktivnim napadom se pokušavaju izvršiti određene promjene nad izvorom informacija ili uticati na izvršenje određenih operacija. Pasivnim napadom, napadač pokušava da dođe do nekih važnih informacija, pri čemu ne utiče na izvor informacija, ne vrši nikakve destruktivne radnje, [54].

Osnovne vrste aktivnih napada su:

- virusi: predstavljaju kodove koji se dodaju normalnom programu čijim izvršavanjem se inficiraju i drugi programi; lako se šire i mogu dovesti do brisanja dijela datoteka; oporavak od virusne infekcije može biti i veoma težak zadatak i zahtijeva djelimično ili potpuno obustavljanje rada računara na duži period vremena; antivirusni progami pomažu u slučaju poznatih virusa,
- crvi: predstavljaju programe koji se šire mrežom od jednog programa ka drugom; koriste načine na koje se mrežni resursi dijele a ponekad koriste i greške u standardnoj programskoj podršci koja je instalirana na mrežnom sistemu; ako i nisu destruktivni oni mogu mrežu onesposobiti, dovesti je do zagušenja, uzurpirajući resurse mreže koristeći ih za svoje potrebe; da bi se eliminisao crv potrebno je najčešće ugasiti sve računare koji se nalaze na mreži.

Osnovne vrste pasivnih napada su:

- pregledavanje (browsing): počinioci nastoje da čitaju pohranjene podatke, memoriju drugih procesa i sl; zaštita se sastoji u ograničenju pristupa (podaci i memorija), odnosno šifrovanju poruka,

- curenje (leaking): kod ove vrste krađe informacija, počinioc mora imati saučesnika koji ima pristup sistemu,
- zaključavanje (inferencing): na osnovu posmatranja aktivnosti sistema, uljez pokušava donijeti neke zaključke koji bi mu pomogli pri ulazu u sistem; npr. ako su informacije kriptovane, uljez pokušava na osnovu analize nekoliko kriptovanih datoteka da izvede ključ; ovo bi mogao uraditi i prisluškivanjem protoka informacija u komunikacionoj mreži,
- maskiranje: počinioc se želi predstaviti kao ovlašteni korisnik kako bi se infiltrirao u sistem; neovlaštena osoba je tada u stanju da modifikuje datoteke, otkriva povjerljive informacije i koristi resurse sistema na neligitiman način; informaciju neophodnu za infiltraciju napadač dobija pretražujući korpu za otpatke svoje žrtve ili primoravajući na neki način žrtvu da mu je da.

9.3. Kriptografija

***Def.*:** *Kriptografija je naučna disciplina koja se bavi proučavanjem metoda za slanje poruka u takvom obliku da ih samo onaj kome su namijenjene može pročitati. Uopšteno rečeno, kriptografija se bavi problemom šifrovanja i dešifrovanja podataka.*

Osnovna namjena kriptografije [64], [90], jeste da:

- da zaštiti memorisanu informaciju bez obzira da li je neko i pristupio podacima,
- da zaštiti prenošenu informaciju bez obzira da li se prenos posmatra.

Osnovni ciljevi kriptografije su:

- tajnost: prevencija od neautorizovanog pristupa informacijama,
- integritet (cjelovitost) odnosno autentičnost (vjerodostojnost): prevencija od neautorizovanog mijenjanja informacija (poruka na odredište treba da stigne nepromijenjena),
- autentičnost njihovog porijekla: prevencija od lažnog poricanja slanja date poruke/dokumenta (može se dokazati da poruka/dokument dolazi od datog entiteta iako taj entitet to poriče).

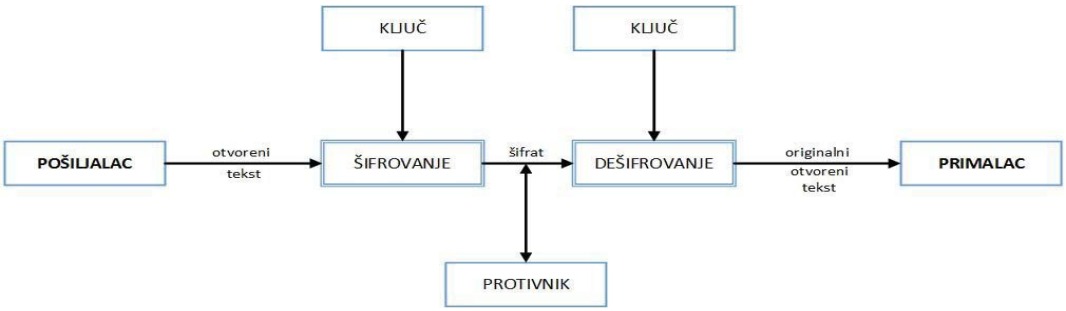
Ovdje ćemo definisati još jedan pojam.

Def.: *Pojmom uljez (intruder) ili napadačem (attacer) definišemo osobu ili program koj(a)i nastoje dobiti neovlašteni pristup podacima ili resursima računarskog sistema.*

Sada bismo mogli reći da je osnovni zadatak kriptografije omogućavanje dvjema osobama (pošiljaocu i primaocu) da komuniciraju preko nesigurnog komunikacionog kanala (telefonska linija, računarska mreža, ...) na način da treća osoba (uljez ili napadač) ne može razumjeti njihove poruke, [64], [90].

Def.: *Poruku koju pošiljalac želi poslati primaocu zovemo otvoreni tekst (plaintext). To može biti tekst, numerički podaci ili bilo šta drugo. Pošiljalac transformiše otvoreni tekst koristeći unaprijed dogovoreni ključ. Taj postupak se zove šifrovanje, a dobijeni rezultat šifrat (ciphertext) ili kriptogram.*

Nakon toga pošiljalac pošalje šifrat preko nekog komunikacionog kanala. Protivnik prisluškujući dozna sadržaj šifrata, ali ne može odrediti otvoreni tekst. Za razliku od njega, primalac koji zna ključ kojim je šifrovana poruka može dešifrovati šifrat i odrediti dobijeni tekst.



Slika 9.3: *Postupak slanja i primanja poruka*

***Def.*:** *Kriptoanaliza ili dekriptovanje je naučna disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa.*

***Def.*:** *Kriptosistem se sastoji od kriptografskog algoritma, te svih mogućih otvorenih tekstova, šifrata i ključeva.*

***Def.*:** *Kriptologija je grana nauke koja obuhvata kriptografiju i kriptoanalizu.*

***Def.*:** *Kriptografski algoritam ili šifra je matematička funkcija koja se koristi za šifrovanje i dešifrovanje (uopšte, radi se o dvije funkcije, jednoj za šifrovanje, a drugoj za dešifrovanje). Njeni argumenti su ključ i otvorene tekst, odnosno ključ i šifrat. Skup svih mogućih vrijednosti ključeva zovemo prostor ključeva.*

9.3.1. Osnovne vrste kriptografskih algoritama

Osnovne vrste kriptografskih algoritama su:

- simetrični kriptografski algoritmi;
- asimetrični kriptografski algoritmi;

- algoritmi izvoda poruke.

9.3.1.1. Simetrična kriptografija

Kod simetričnih ili konvencionalnih kriptosistema, ključ za dešifrovanje se može izračunati poznavajući ključ za šifrovanje i obrnuto. U stvari, najčešće su ovi ključevi identični. Sigurnost ovih kriptosistema leži u tajnosti ključa, pa se zato oni zovu i kriptosistemi sa tajnim ključem. Ključ treba da bude što duži, jer od dužine ključa zavisi koliko je potrebno vremena da se pregledaju svi mogući ključevi, [34], [54], [64].

Simetrični algoritmi se dalje mogu podijeliti na:

- algoritmi za šifrovanje nizova bita (protočni): vrše šifrovanje jednog po jednog bita podataka i jednostavni su za implementaciju u elektronskim sklopovima; nisu tako sigurni kao blokovski algoritmi ali je zato vjerovatnoća širenja greške kod njih manja (npr u slučaju da se bit šifrovanog teksta ne može pročitati algoritmi za šifrovanje nizova bita će pogriješiti u samo jednom bitu, dok bi se u slučaju algoritma za šifrovanje bloka podataka greška prenijela na cio blok),
- algoritmi za šifrovanje blokova podataka su u praksi lakši za programsku implementaciju jer šifruju podatke po blokovima obično veličine 64 bita.

Najpoznatiji simetrični enkripcioni algoritmi su:

- DES (Data Encryption Standard): ključ dužine 56 bitova,
- Triple DES, DESX, GDES, RDES: ključ dužine 168 bitova,
- (*Rivest*) RC2, RC4, RC5, RC6: promenljva dužina ključa do 2048 bitova,
- IDEA (International Data Encryption Algorithm): osnovni algoritam za PGP (Pretty Good Privacy), ključ dužine 128 bitova,
- Blowfish: promenljiva dužina ključa do 448 bitova,
- AES (Advanced Encryption Standard): radi sa blokovima od po 128 bitova i koristi ključeve dužine 128, 192 i 256 bita.

9.3.1.2. Asimetrična kriptografija

Kod kriptosistema sa javnim ključem ili asimetričnih kriptosistema, ključ za dešifrovanje se ne može (barem ne u nekom razumnom vremenu) izračunati iz ključa za šifrovanje. Ovdje je ključ za šifrovanje javni ključ, naime, bilo ko može šifrovati poruku pomoću njega, ali samo osoba koja ima odgovarajući ključ za dešifrovanje (privatni ili tajni ključ) može dešifrovati tu poruku, [64], [67].

Ideja asistemtrične kriptografije počiva na takozvanim jednosmijernim funkcijama. Treba pronaći funkciju koja se lako računa, ali čiju je inverznu funkciju (gotovo) nemoguće izračunati bez dodatnih argumenata, privatnog ključa.

Najveća prednost simetrične kriptografije je njena brzina, tj. u odnosu na asimetričnu kriptografiju zahtijeva manje računanja, tako da se veće količine podataka brže šifruju i dešifruju. Najveća mana ovog sistema je činjenica da se mora pronaći bezbjedan način za razmjenu ključa, tj. mora se osigurati siguran kanal za distribuciju ključeva između zainteresovanih strana. S druge strane, postavlja se sledeće pitanje: ako imamo siguran kanal, zašto se njime ne razmijene i svi podaci, a ne samo ključ? Odnosno, da li je šifrovanje uopšte potrebno? Osim toga, danas se ogroman broj podataka razmjenjuje Internetom, pa bi bilo potrebno generisati veliki broj ključeva.

Dakle, kod kriptografije javnim ključem, javni ključ je poznat svima, pa svako može šifrovati i poslati poruku. Dešifrovanje može obaviti isključivo vlasnik privatnog ključa. I upravo zbog činjenice da je svako može šifrovati, primalac ne može biti siguran ko mu je poslao poruku. Međutim, kriptografija javnim ključem u stanju je da prevaziđe i ovaj problem, [64], [90].

Šifrovanje podataka asimetričnom kriptografijom se može obaviti na dva načina:

- šifrovanje originalne poruke javnim ključem: samo vlasnik privatnog ključa može dešifrovati poruku, ali ne može biti siguran ko je poruku poslao, jer je javni ključ dostupan svima,
- šifrovanje originalne poruke privatnim ključem: porijeklo poruke je nedvosmisleno, kao i nemogućnost poricanja vlasnika javnog ključa da je poruku poslao; međutim, ovu poruku svako može dešifrovati, pa ona ne može biti tajna; ipak, kako samo pošiljalac ima taj privatni ključ, očigledno je da je on poslao poruku, pa se ovaj pristup može iskoristiti za digitalno potpisivanje, o čemu će više riječi biti u nastavku.

Prema tome, treba kombinovati ova dva pristupa: pošiljalac šifruje poruku javnim ključem primaoca, a zatim svojim privatnim ključem šifruje čitavu poruku ili neki njen dio (digitalno je potpisuje). U procesu dešifrovanja primalac zna javni ključ pošiljaoca, čime je potvrđena autentičnost poruke, a zatim je dešifruje svojim privatnim ključem.

Glavna prednost korišćenja asimetrične kriptografije jeste da strane koje nikada do tog momenta nisu komunicirale i koje nemaju siguran kanal za bezbjednu komunikaciju, mogu tajno komunicirati. Takođe, potrebno je samo dva ključa za komunikaciju-jedan koji se slobodno prenosi i drugi koji se čuva. Sa druge strane, šifrovanje korišćenjem asimetričnih postupaka je mnogo sporije nego zaštita korišćenjem simetričnog kriptografskog postupka za oko hiljadu puta, u zavisnosti od konkretnih algoritama. Iz tog razloga se ovakav vid šifrovanja ne primjenjuje kod razmjene većeg broja podataka.

Najčešće korišćeni algoritmi za asimetrično šifrovanje su RSA algoritam i Diffie-Hellman algoritam. Njihov rad se zasniva na činjenici da je teško razbiti na činioce velike brojeve koji su proizvod dva prosta broja.

9.3.1.3. Algoritmi izvoda poruke

Algoritmi izvoda poruke (message digest) služe za digitalno potpisivanje dokumenta. Digitalni potpis predstavlja osnovnu metodu za provjeru porijekla informacija u globalnom elektronskom sistemu komunikacije, [64].

Izvod poruke je niz fiksne dužine koji se dobija od ulaza promjenjive dužine. Matematička funkcija koja to obavlja naziva se heš (hash) funkcija. Gotovo je nemoguće proizvesti dokument koji ima istu heš vrijednost kao neki drugi dokument, tako da je ova tehnika provjere integriteta podataka veoma pouzdana.

Najpopularniji algoritmi za izračunavanje izvoda poruke su: MD2, MD4 i MD5.

9.4. Sigurnosni protokoli na pojedinim nivoima TCP/IP protokol steka

9.4.1 Sigurnosni protokoli na mrežnom nivou TCP/IP protokol steka

Implementacijom IPv6 protokola se probao riješiti ne samo problem nedostatka adresnog prostora kod IPv4 protokola, nego i problem sigurnosti, budući da IPv4 nije pružao adekvatan odgovor na ovaj zahtjev. Rješenje je u implementaciji IP Security (IPSec) protokola, koji se može implementirati i kod IPv4 i kod IPv6.

9.4.1.1. IPSec

IPSec djeluje na mrežnom, IP nivou TCP/IP protokol steka. Standardi koji definišu IPSec su RFC 2401, RFC 2402, RFC 2403, RFC 2404, RFC 2406, RFC 2408, RFC 2409 i RFC 2412.

IPSec nije jedan protokol, već bi ispravnije bilo reći da je to skup servisa i protokola koji treba da obezbijede sugurnost IP mreži, [16],[34],[54],[55]. Ovi servisi i protokoli se kombinuju da obezbijede različite tipove zašite kao što su:

- šifrovanje korisničkih podataka radi obezbjeđenja privatnosti,

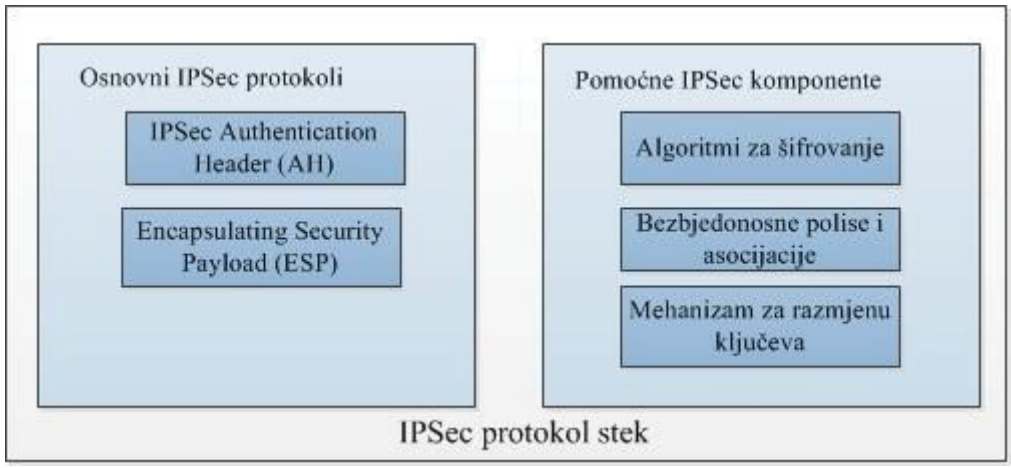
- provjera integriteta poruke, kako bi se utvrdilo da ona nije mijenjana na svom putu,
- zaštita od određenih vrsta napada, kao što je napad ponavljanjem,
- ugovaranje različitih sigurnosnih protokola i ključeva između uređaja u saglasnosti sa njihovim sigurnosnim potrebama,
- dva sigurnosna moda, transportni i tunelski u zavisnosti od mrežne sigurnosti.

IPSec obuhvata i specifikaciju osnovnih funkcija *firewall*-a, o čemu će u ovom poglavlju još biti riječi.

Da bi dva uređaja (dva hosta ili dva posrednička uređaja, dva rutera ili *firewall*-a) uspostavila bezbjednu komunikaciju, moraju se sprovesti (najmanje) sledeći koraci:

- uređaji se moraju dogovoriti oko sigurnosnih protokola koje će koristiti kako bi svako mogao poslati podatke u formatu koji će drugi moći da razumije,
- moraju da odluče koji će algoritam šifrovnja da koriste,
- moraju da razmijene ključeve koji će se koristiti za dešifrovanje kodiranih podataka,
- po završetku ovog pozadinskog procesa, svaki uređaj može da koristi prethodno dogovorene metode, protokole i ključeve za šifrovanje podataka i njihovo slanje kroz mrežu.

Da bi se podržale ove aktivnosti razvijen je IPSec protokol stek koga čine dva osnovna protokola i tri pomoćne IPSec komponente, kako je to prikazano na Sl.9.4, [16], [55].



Slika 9.4: *Pregled IPSec protokola i komponenti*

Kako se vidi sa slike 9.4 dva osnovna IPSec protokola su AH i ESP.

AH (IPSec Authentication Header) protokol pruža servis autentifikacije za IPSec. Omogućava primaocu poruke da provjeri identitet pošiljaoca poruke, kao i da provjeri da li se na bilo kojem od posredničkih uređaja promijenio bilo kakav podatak u datagramu. AH omogućava zaštitu i od tzv. „napada ponavljanjem“ kada neautorizovani korisnik može da presretne poruku. AH osigurava integritet podataka u datagramu, ali ne i njihovu privatnost.

ESP (Encapsulating Security Payload) protokol se koristi za zaštitu privatnosti podataka, šifrovanjem cjelokupnog sadržaja (payload) IP datagrama.

AH i ESP smo ovdje nazvali protokolima, mada se oni u praksi implementiraju kao zaglavlja koja se dodaju na IP datagram. Oni se mogu, mada istina rijetko, upotrebljavati istovremeno za osiguravanje autentifikacije i privatnosti, [34], [54].

Da bi oni ispravno funkcionisali potrebna je podrška nekih drugih protokola i servisa prikazanih na Sl.9.4.

AH i ESP ne koriste neke konkretne mehanizme za šifrovanje, ali se najčešće koriste heš algoritmi MD5 i SHA-1 (Secure Hash Algorithm 1) koji služe za verifikaciju podataka.

Bezbjedonosne polise i asocijacije služe za praćenje bezbjedonosnih relacija između uređaja.

Kod IPSec kao protokol koji omogućava razmjenu ključeva za šifrovanje i dešifrovanje, koristi se IKE protokol (Internet Key Exchange), [34], [54], [55].

Postavlja se pitanje gdje implementirati IPSec. Postoje dva pristupa:

- implementacija IPSec u hostovima (end-host implementation): kod ove implementacije IPSec se implementira u sve host uređaje u mreži čime se postiže sigurnost sa kraja na kraj (end-to-end) između bilo koja dva uređaja u mreži, ali zahtijeva i najviše posla pri implementaciji,

- implementacija u ruterima (router implementation): zahtijeva mnogo manje posla pri implementaciji jer su potrebne promjene u samo nekoliko rutera a ne na stotinama i hiljadama klijenata čime se postiže zašita između para rutera kod kojih je implementiran IPSEc što je u većini slučajeva dovoljno (primjer VPN mreže); štite se datagrami na dijelu puta van organizacije, dok se saobraćaj između rutera i hostova unutar organizacije ostavlja neobezbjeđen ili štiti na drugi način, što će biti objašnjeno u nastavku.

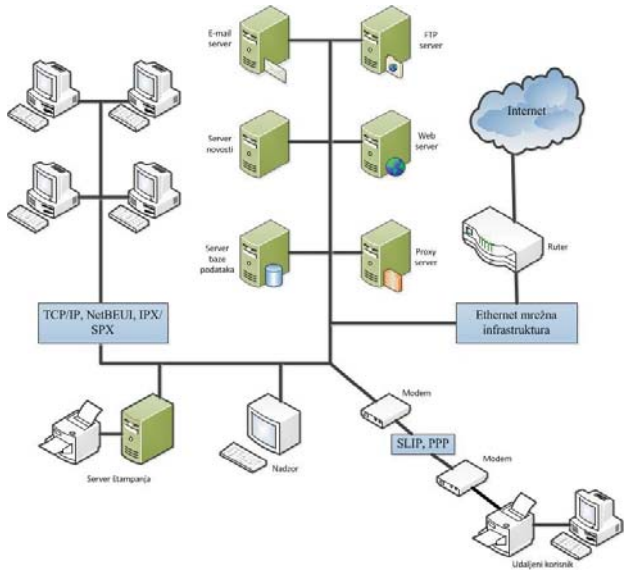
9.4.1.1.1. Zaštita lokalnih mreže uz pomoć *firewall*-a

Na Sl.9.5 je data ilustracija protoka podataka u jednoj LAN mreži, a ne fizička infrastruktura mreže.

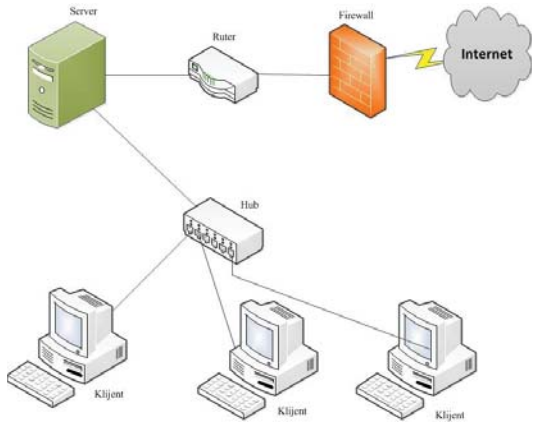
Veza sa vanjskim svijetom se obavlja preko rutera i to je mjesto gdje treba postaviti *firewall* radi zaštite od vanjskog svijeta, [54], [90].

Firewall predstavlja računar ili skup komunikacionih uređaja koji fizički razdvajaju vanjsku (javnu) mrežu od unutrašnje (privatne) mreže. S obzirom da *firewall* povezuje dvije različite mreže (javnu i privatnu) i prosleđuje pakete iz jedne u drugu, to ga možemo smatrati i ruterom, međutim njegova osnovna namjena nije prosleđivanje paketa već sprečavanje da neki sadržaji budu prosleđeni u, ili iz lokalne mreže koju *firewall* štiti.

Firewall možemo posmatrati kao filtar koji odbacuje sve one pakete koji su naslovljene na neku IP adresu lokalne mreže i/ili neki TCP port. *Firewall* može odbacivati IP pakete na osnovu IP adrese pošiljaoca čime je spriječeno da neko spolja uspostavi komunikaciju sa nekom osobom unutar lokalne mreže koju taj *firewall* štiti. Filtriranje komunikacije između domaćina iz lokalne mreže i ostatka mreže se sprovodi sa ciljem kontrole pristupa računarima i sadržajima lokalne mreže, kao i sa ciljem sprečavanja da se iz lokalne mreže šalju neki sadržaji. Uloga *firewall*-a jeste da se zaposlenim u preduzeću eventualno ograniči pristup Internetu, kao i da se dolazeći zahtjevi sa Interneta usmjere na one sadržaje intraneta koji ne sadrže nikakvu poslovnu tajnu. *Firewall* dakle rješava problem sigurnosti na taj način što sprečava svaku komunikaciju sa lokalnom mrežom za koju smatra da bi mogla biti štetna.



Slika 9.5: *Protok podataka u LAN mreži*



Slika 9.6: *Zaštita LAN mreže uz pomoć firewall-a*

Firewall-i se dijele na dvije osnovne klase:

- *firewall*-i koji se koriste kao filtri,
- *firewall*-i zasnovani na primjeni proxy-a.

Firewall-i koji se koriste kao filtri (filter-based) sadrže tabelu adresa i portova na osnovu koje se utvrđuje koji će se paketi proslijediti a koji odbaciti. Svaki red tabele sadrži četiri osnovna parametra: IP adresu izvora i TCP (ili UDP) port izvora i IP adresu odredišta i TCP (ili UDP) port odredišta.

Takvi zapisi se mogu koristiti da se eksplicitno spriječi komunikacija za navedene adresa i portove u tabeli ili da se eksplicitno dozvoli komunikacija samo za one adrese koje su navedene u tabeli.

Proxy se nalazi između klijenta i servera i gledano sa strane klijenta on poprima ulogu servera, dok gledajući sa strane servera poprima ulogu klijenta. *Proxy* u svojoj memoriji pohranjuje razne sadržaje (podatke, upit i odgovore) koji se često razmjenjuju u okviru komunikacije između klijenta i servera.

Obzirom da se ti upiti često ponavljaju (od strane istog klijenta ili drugih), pohranjeni sadržaji ranijih upita i odgovora omogućavaju *proxy*-u da sam odgovara na upite klijenata.

9.4.1.1.2. Režimi rada IPSec

IPSec može da radi u dva režima rada: transportnom i tunelskom. Izborom režima rada određujemo koji dio datagrama želimo da štitimo. Donekle se razlikuje primjena kod IPv4 i IPv6, [16], [55].

U transportnom modu, IPSec štiti sadržaj koji na IP stiže sa transportnog sloja. Sadržaj se potom obrađuje od strane AH i ESP-a i njihova zaglavlja se dodaju ispred zaglavlja transportnog nivoa (TCP/UDP). IP zglavlje se dodaje ispred IPSec zaglavlja (Sl.9.7).

Slika 9.7: *Transportni mod IPv4*

U tunel modu (Sl.9.8), IPSec zaštita se primjenjuje na kompletan datagram. IPSec se postavlja ispred originalnog IPSec zaglavlja, čime se postiže zaštita originalnog IP datagrama koji se pakuje u novi IP datagram.

Slika 9.8: *Tunel mod IPv4*

Kod IPv6 se primjenjuje i zaglavlja za proširenje (extension headers) koja se prilikom upotrebe IPSec moraju postaviti u određeni raspored. Prvo idu zaglavlja koja se mijenjaju prilikom rutiranja paketa (mutable headers), a potom zaglavlja koja se ne mijenjaju (fixed headers).

Slika 9.9: *Transportni mod IPv6*

Slika 9.10: *Tunel mod IPv6*

9.4.2. Sigurnosni protokoli na transportnom nivou TCP/IP protokol steka

9.4.2.1. SSL protokol

SSL (Secure Sockets Layer) je protokol namijenjen za sigurnu razmjenu podataka. Danas je to najčešće korišćeni protokol u aplikacijama e-trgovine. Razvila ga je Netscape korporacija i 1994. ugrađen je u Netscape navigator. Prva publikovana verzija SSL–a je 2.0, jer je verzija 1.0 korišćena samo kao testna verzija unutar Netscape-a. Danas je aktuelna verzija 3.0 u kojoj su korigovani neki nedostaci uočeni u verziji 2.0. Verzija 3.0

poslužila je kao osnova za TLS (Transport Layer Security). Kasnije je TLS modifikovan, za potrebe bežičnih komunikacija u WTLS (Wireless TLS), [34].

SSL predstavlja sloj smješten između transportnog i aplikcionog sloja TCP/IP prtokol steka (Sl.9.11). SSL obezbjeđuje identifikaciju klijenta i servera i šifrovanu razmjenu podataka između njih. Da bi se ostvario zaštićeni prenos SSL protokol moraju podržavati i klijent i server.

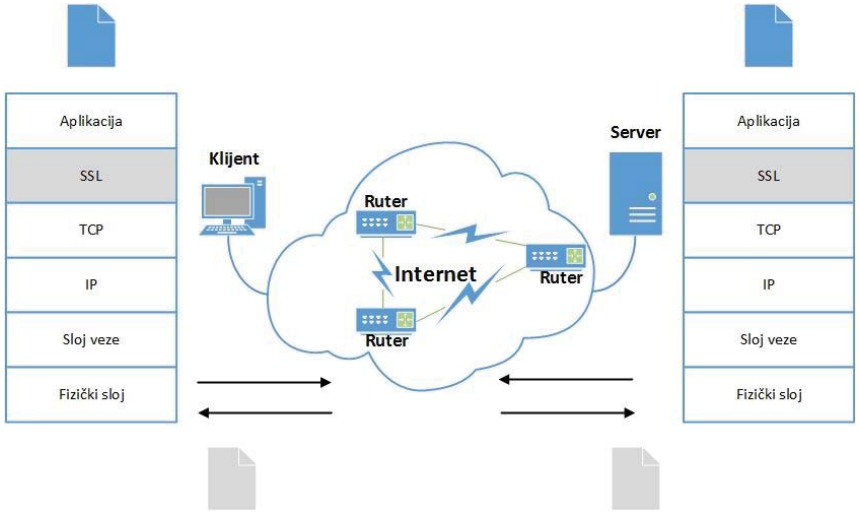
SSL protokol, kao protokol sigurne razmjene podataka putem Interneta mora da zadovolji tri uslova:

- privatnost: konekcija mora biti zaštićena enkripcijom; koriste se najčešće protočni (RC4) algoritam i blokovski (DES, 3DES, IDEA) algoritmi,
- autentifikacija: identifikacija preko sertifikata,
- integritet podataka: upotrebom recimo MD5 algoritma izvoda poruke.

SSL obezbjeđuje dakle privatnost, integritet podataka i autentičnost pošiljaoca korišćenjem kombinacije šifrovanja javnim ključem, simetričnog šifrovanja i digitalnih sertifikata.

SSL protokol se sastoji od 4 potprotokola:

- *Handshake:* protokol za „rukovanje“, odnosno za uspostavljanje sesije,
- *Record:* protokol za zapise,
- *ChangeCipherSpec (CCS):* protokol za slanje informacije o sigurnosnim parametrima,
- *Alert:* protokol za upozorenja.

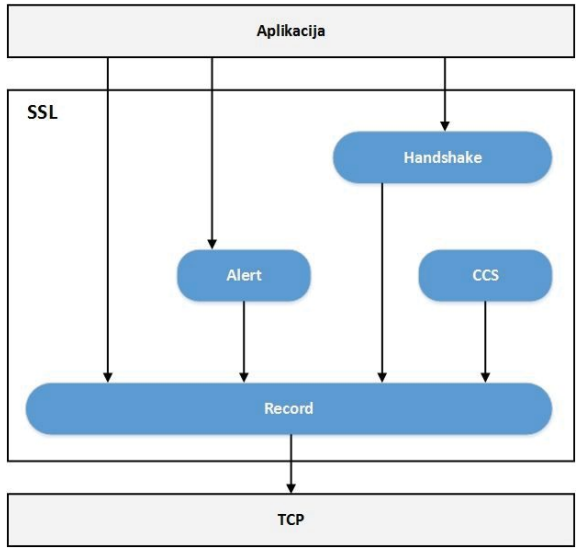


Slika 9.11: *Način funkcionisanja SSL-a*

Handshake („rukovanje“) protokol je odgovoran za autentifikaciju komunikacionih strana gdje se obje strane „dogovaraju“ oko enkripcijskih i heš algoritama i gdje se vrši razmjena ključeva. Funkcija CCS protokola je da signalizira *Record* protokolu bilo kakvu promjenu u sigurnosnim parametrima (Sl.9.12). *Alert* protokol pokazuje greške na koje se naišlo tokom verifikacije poruke. *Record* protocol primjenjuje sve dogovorene parametre da se zaštite podaci u razmjeni. Ovi nivoi se nalaze iznad sloja za prenos podataka, koji je obično TCP sloj.

Transakcija korišćenjem SSL protokola obavlja se u nekoliko koraka, kao što je prikazano na Sl.9.10:

- server šalje svoj digitalni sertifikat klijentu,
- klijent provjerava da li je sertifikat izdat od strane CA,
- klijent i server razmjenjuju javne ključeve,
- klijent generiše tajni ključ koji se koristi samo u započetoj transakciji,
- klijent šifruje generisani tajni ključ, korišćenjem serverovog javnog ključa i šalje ga serveru.



Slika 9.12: *Protokol stek za SSL potprotokole*

U daljem toku transakcije server i klijent koriste isti tajni ključ metodom simetričnog kriptovanja.

9.4.3. Sigurnosni protokoli na aplikacionom novou TCP/IP protokol steka

9.4.3.1. SET protokol

SET (Secure Electronic Transaction) protokol je dizajniran da omogući bezbjedne transakcije izvršene bankovnim karticama preko otvorenih mreža, poput Interneta. Ovaj protokol je zajednički razvijan od strane Visa i MasterCard, u saradnji sa vodećim firmama iz svijeta informatike, kao što su IBM, GTE (nekadašnji General Telephone & Electronics Corporation), Microsoft, SAIC (Science Applications International Corporation), Terisa Systems i VeriSign. Zajednički cilj je bio da se podstakne korišćenje kreditnih kartica za *on-line* plaćanja i da se izbjegne fragmentacija tržišta na mnoštvo nekompatibilnih protokola, [90].

SET radi na aplikativnom sloju, nezavisno od transportnog sloja i ovo ga svojstvo razlikuje od SSL-a. U praksi se, međutim, SET obično uzima za obezbjeđivanje transporta putem TCP protokola. SET se fokusira isključivo na plaćanje i isključuje pretraživanje i biranje robe. U SET transakciji, plaćanje se vrši bez umetanja kartice u čitač. Transakcija se ovjerava prethodno postavljenim sertifikatom dodijeljenim od CA. Ova potvrda se čuva na hard disku računara (ili na disketi, CD-u ili nekom drugom mediju) i omogućava provjeru identiteta vlasnika kartice kriptografijom sa javnim ključem.

Osnovni princip kojim su se rukovodili kreatori SET protokola je bio da se obezbijede transakcije bankovnim karticama preko Interneta, a da se ne mijenjaju postojeći bankarski kanali za autorizaciju i plaćanja.

Mreža bankovnih kartica ima ovlašćene servere koji filtriraju transakcije od zloupotreba u skladu sa preciznim kriterijumima, na primjer ako je trošak premašio zadati limit ili ako je izvršen veliki broj transakcija u zadatom intervalu. Dakle, prije autorizacije transakcije, trgovac mora da da upit ovlašćenim serverima u sistemu kartica. Kasnije u fazi poravnanja, trgovcu se isplaćuje iznos koji odgovara vrijednosti robe ili usluga. Međutim, pojedini sistemi bankovnih kartica zahtijevaju da se finansijsko poravnanje obavi tek nakon isporuke robe. To je tek onda kada trgovac pošalje banci klirinški zahtjev za namirenje neizmirenih dugova; ovaj zahtjev je onda proslijeđen putem bankarske mreže banci izdavaocu. Primijetimo da u nekim sistemima bankovnih kartica, autorizacioni zahtjev i zahtjev za poravnanje, mogu biti kombinovani u istu operaciju za svaku transakciju. Drugi sistemi omogućavaju grupisanje transakcija, tako da se više autorizacionih zahtjeva i zahtjeva za poravnanjem mogu poslati u isto vrijeme, na primjer na kraju radnog dana. Ukoliko trgovac treba da nadoknadi kupcu određeni novac, bilo zbog toga što je proizvod vraćen ili zato što je neispravan, trgovac daje instrukcije banci za prebacivanje novca na račun klijenta.

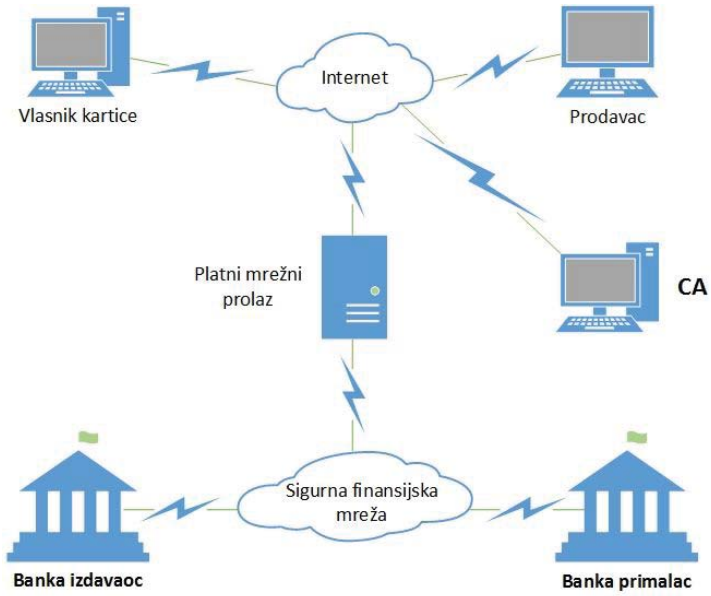
Da bi omogućili rad sistema na svjetskom nivou, SET je predstavio dva nova entiteta:

- sertifikaciono tijelo (CA) koje ovjerava učesnike,
- platni mrežni prolaz (payment gateway) koji povezuje Internet i mrežu bankovnih kartica.

Dakle, postoji šest učesnika u SET-u:

- korisnik, čija kartica mora biti u skladu sa SET specifikacijom i koju izdaje odgovarajuća institucija, obično banka povezana sa Visa ili MasterCard,
- server trgovca,
- platni mrežni prolaz,
- CA,
- institucija izdavalac(banka) koja je izdala bankovnu karticu,
- banka kod koje trgovac ima račun.

Naredna slika prikazuje funkcionalnu arhitekturu SET-a. Kartice, trgovac, CA i platni mrežni prolaz su povezani preko Interneta. Klijent ne uspostavlja direktnu vezu sa platnim mrežnim prolazom, ali koristi tunel koji prolazi kroz server trgovca. Svaki od učesnika prvo mora da dobije sertifikat od sertifikacionog tijela koji je u skladu sa SET specifikacijom. Ovi sertifikati se priloženi u svakoj od poruka koje se razmjenjuju između korisnika, trgovca i platnog mrežnog prolaza, [90].



Slika 9.13: *Učesnici u SET protokolu*

Institucije izdavaoca i primaoca povezane su zatvorenom i sigurnom bankarskom mrežom. Platni mrežni prolaz je most između otvorene i zatvorene mreže koji štiti pristup bankarskoj mreži. Mrežni prolaz ima dva interfejsa, jedan u skladu sa SET specifikacijom, na Internet strani, a drugi na sigurnoj strani finansijske mreže.

SET obezbjeđuje razmjenu između klijenta i trgovaca i istovremeno razmjenu između trgovca i platnog mrežnog prolaza. Platni mrežni prolaz, upravlja uplatama u ime banke koja je izdala karticu i u ime banke trgovca. Kao posledica toga, mrežni prolaz mora biti odobren od strane bankarskih vlasti, a u suprotnom je za obavljanje ove funkcije odgovorna finansijska institucija.

9.4.3.2. PGP

PGP (Pretty Good Privacy) predstavlja softver koji koristi kriptografiju radi obezbjeđenja sigurnosti za elektronske poruke (mail-ove) kao i druge aplikacija na Internetu. PGP se sve više koristi zbog toga što se on može koristiti na različitim platformama i zbog toga što je njegov izvorni kod slobodan, [68].

Komponente PGP-a:

- autentifikacija (digitalni potpis),
- privatnost (enkripcija),
- kompresija: PGP izvršava kompresiju svake poruke, poslije potpisivanja a prije šifrovanja koristeći ZIP algoritam,
- kompatibilnost sa elektronskom poštom,
- segmentiranje: često je najveća dužina poruke ograničena na 50 000 okteta; PGP automatski dijeli poruku koja je previše duga; na prijemnoj strani se vrši obrnut proces radi dobijanja originalne poruke.

9.5. Sigurnost mobilnih mreža

Uzimajući u obzir da je sve popularniji pristup Internetu preko mobilnih uređaja, javljaju se i opasnosti koje uvijek vrebaju kada se korisnici povezuju na Internet. Uvijek postoje sigurnosni rizici i prijetnje od zlonamjernih napadača. Zato je potrebno pravilno zaštititi sve komunikacione kanale. Uz to, treba napomenuti da su prevare preko telefona i zloupotreba prenosa govora vrlo česte, [50], [90].

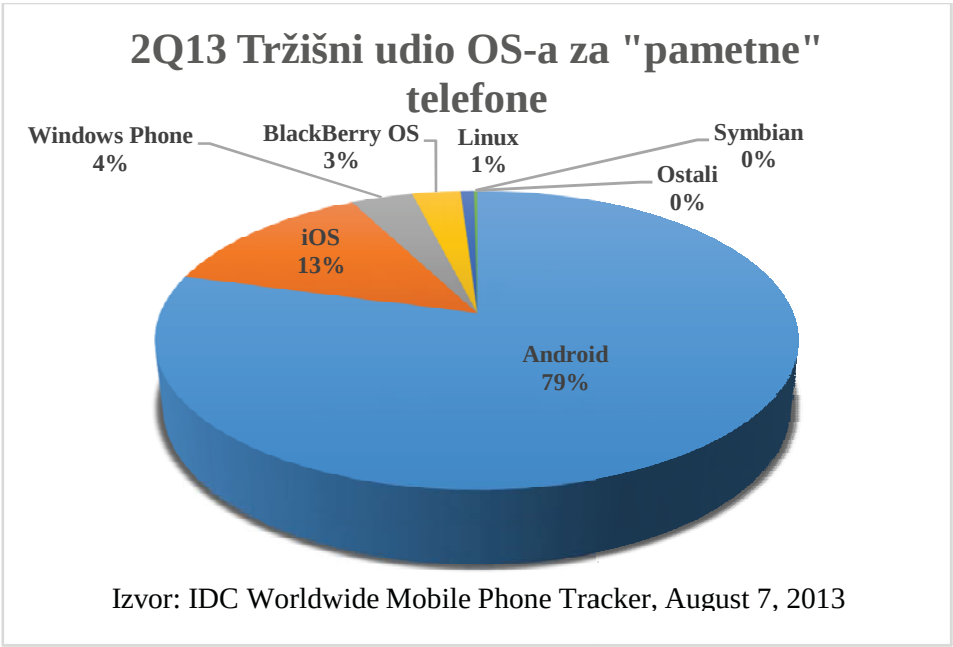
U mobilnim mrežama sigurnosni problemi su vezani za zaštitu razgovora, podataka o pozivima i sprečavanju prevara putem mobilnih telefona. U slučaju starijih analognih sistema bilo je jednostavno presresti i prisluškivati telefonske razgovore samo uz pomoć policijskog skenera.

Takođe, poznati su i problemi tzv. „kloniranja mobilnih uređaja“, odnosno krađa identiteta i lažno predstavljanje. Postupak kojim mobilni uređaj registruje svoju poziciju u mobilnoj mreži je ranjiv na presretanje. U slučaju da napadač presretne i sazna poziciju mobilnog telefona, saznao je i korisnikovu poziciju čiju promjenu može iskoristiti kada mobilni telefon nije u upotrebi, [54].

Sa razvojem tehnologije, javljaju se i moderniji (kompleksniji) mobilni uređaji koji omogućavaju korisniku da sa sobom nosi pravi lični računar. Iako je korisniku vrlo koristan takav uređaj, uz njega se javljaju isti sigurnosni problemi kao i kod ličnih računara (npr. krađa identiteta, uskraćivanje usluga, neovlaštena upotreba, podmetanje zlođudnih programa i drugo). Jedan takav uređaj je „smart phone“ ili u dvosmislenom prevodu pametni telefon. Takvi telefoni, ali i malo slabiji modeli, posjeduju kameru, omogućavaju pristup Internetu, koriste virtualne tastature, sadrže module za reprodukciju multimedijalnih sadržaja i ostale tipične funkcionalnosti koje imaju lični računari. Međutim, kao što su lični računari ranjivi na sigurnosne propuste, tako su i mobilni telefoni, [90].

Neki od najpoznatijih i najkorišćenijih operativnih sistema za „pametne telefone“ su:

- Android: operativni sistem namijenjen za mobilne uređaje, kao što su mobilni telefoni, „tablet“ računari i „netbooks“; Android je razvijen u kompaniji Google, i baziran je na Linux kernelu i GNU softveru; u početku, ovaj OS je razvila firma Android Inc., koju je kasnije kupila firma Google i proširila na Open Hadnset Alliance,
- iOS: je operativni sistem kompanije Apple; prvobitno je razvijen za iPhone, a kasnije i iPod Touch, iPad i AppleTV; Apple ne dozvoljava pokretanje iOS sistema na hardveru drugih proizvođača,
- Windows Phone: je mobilni operativni sistem firme Microsoft i nasljednik je Windows Mobile operativnog sistema; za razliku od prethodnika, primarno ciljno tržište Windows Phone-a su potrošači, dok su kod Windows Mobile sistema ciljno tržište bili poslovni korisnici.



Izvor: IDC Worldwide Mobile Phone Tracker, August 7, 2013

Slika 9.14: *Tržišni udio OS-a za "pametne" telefone*

Na Sl.9.14 je prikazan tržišni udio OS-a za „pametne“ telefone za period drugog kvartala u 2013. godini.

Nabrojani operativni sistemi korisniku koji zna iskoristiti njihove prednosti olakšavaju rad i nude mnoge dodatne funkcionalnosti, ali postoji i druga strana, a to je da iste prednosti koje omogućavaju prilagodljivost operativnih sistema napadači mogu iskoristiti za zloupotrebu i ugroziti sigurnost podataka na mobilnim telefonima korisnika. Korisnici mobilnih telefona čuvaju mnogo privatnih informacija u svojim uređajima. Ukoliko napadač neovlašteno pristupi uređaju i ukrade podatke, može ih iskoristiti za lažno predstavljanje, a ako se među ukradenim podacima nađu i oni o kreditnim karticama, napadač može nanijeti i finansijsku štetu korisniku. Razvoj programa za operativne sistema na mobilnim uređajima vrlo je sličan razvoju programskih paketa za operativne sisteme namijenjene ličnim računarima, što napadačima olakšava pisanje zlonamjerne programa za mobilne uređaje, [90].

9.5.1.1. Sigurnosne prijetnje kod mobilnih uređaja

Najopasnije sigurnosne prijetnje za mobilne uređaje nalaze se u sledećih sedam područja:

- tekstualne poruke,
- kontakti i adresar,

- video,
- snimci telefonskih razgovora,
- istorija poziva,
- dokumentacija,
- upotreba *clipboard*-a.

9.5.1.1.1. Tekstualne poruke

Gotovo svi mobilni uređaji korisniku pružaju mogućnost slanja i blokiranja poruka. Napadači mogu korisniku poslati posebno oblikovane poruke sa zlonamjernim programskim kodom koji mogu iskoristiti za krađu ličnih podataka i ostalih podataka koji se nalaze na mobilnom telefonu. Osim opisanih poruka, napadač može korisniku poslati poruku u kojoj ga navodi na otkrivanje osjetljivih podataka. Takav oblik napada se naziva *SMS phishing*, prema već poznatom obliku napada na ličnim računarima *phishing*-u.

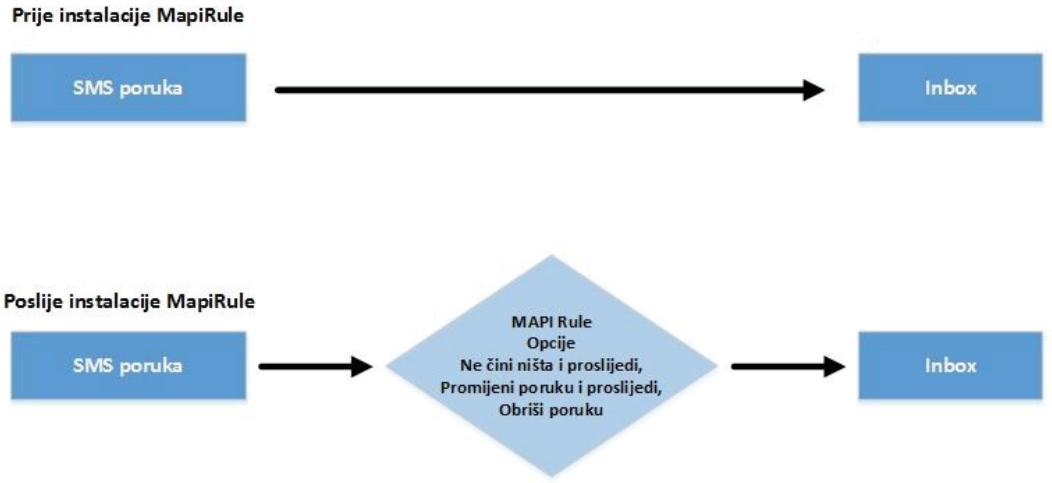
Primjer zlonamjernog programa kojeg napadač može podmetnuti korisniku je tekstualna poruka koja koristi funkcije za upravljanje SMS porukama za slanje lažnih poruka ljudima koji se nalaze u imeniku. Ova metoda napada je slična napadu korištenjem poruka elektronske pošte na ličnim računarima, ali napadi upotrebom SMS poruka imaju veću mogućnost uspjeha jer žrtva obično nije svjesna da postoji takva sigurnosna prijetnja. Korisnici uglavnom vjeruju u autentičnost dolaznih SMS poruka na temelju broja s kojeg su poslane. Ali ako je napadač ukrao identitet osobe koju spomenuti korisnik ima u svom imeniku, može se lažno predstavljati kao korisnikov prijatelj, pa mu može također slati lažne SMS poruke. Običan će korisnik vrlo teško otkriti jesu li dobijene SMS poruke zlonamjerne, [90].

Zlonamjerni programi koje podmetnu napadači mogu koristiti funkcije za upravljanje SMS porukama za naplaćivanje usluga mobilnih telefona preko SMS poruka.

Primjer:*"U mobilnim telefonima koji koriste programski jezik Javu otkriveni su napadi ovog tipa. Ukoliko napadač uspješno podmetne trojanskog konja koji šalje posebne tekstualne poruke provajderu, napadač može otkriti koliko korisnik plaća usluge korištenja mobilne mreže provajdera te zloupotrijebiti te podatke za svoju finansijsku korist."*

Na primjer, upotrebom programskog paketa Windows Mobile Software Development Kit, alata za razvoj aplikacija namijenjenih operativnom sistemu Windows Mobile, napadač može stvoriti posebno oblikovani programski kod samo upotrebom primjera programskog koda naziva MAPI Rule. MAPI Rule klijent je COM (Component Object Model) objekat koji implementira ImailRuleClient interfejs. MAPI Rule klijenta pokreće aplikacija koja prima elektronsku poštu i tekstualne poruke u dolazni sandučić. Dolazne SMS poruke se

predaju MAPI Rule klijentu kako bi on odlučio koje će akcije biti obavljenje nakon prijema poruke. Stvaranje zlonamjernog koda je vrlo jednostavno. Nakon što je napadač podmetnuo programski kod, on postaje filtar između kratkih poruka i programa za elektronsku poštu *tmail.exe.* Napadač može ometati upotrebu slanja tekstualnih poruka brisanjem, izmjenom i/ili prosleđivanjem poruka. Osim toga, napadač može podmetnuti zlonamjerni program kao dodatak porukama koje prosleđuje. Ukoliko korisnik koristi svoj mobilni telefon za komunikaciju u svojoj firmi ili za razmjenu službenih podataka, napadač može opisanim načinom efikasno presretati korporacijski tok podataka. Na Sl.9.15 je dat primjer toka poruka sa postavljenim MAPI Rule klijentom i bez njega.



Slika 9.15: *Tok poruka sa i bez MAPI Rule klijenta*

Iako ovakav napad predstavlja opasnosti korisnicima, nema potrebe za panikom. MAPI Rule tehnologija za blokiranje SMS poruka koristi tačno određeni port koji je predodredio proizvođač. Prema tome, korisnici lako mogu utvrditi imaju li na svojim telefonim program kome tu nije mjesto. Za instalaciju na predviđeni port zlonamjerni program se mora registrovati kao DLL (Dynamic Link Library) modul za filtriranje i imati dodatni CLSID ključ. CLSID ključ je jedinstvena oznaka koja identifikuje objekat COM klase. On izgleda na primjer ovako:

„{3AB4C10E-673C-494c-98A2-CC2E91A481115}“ = dword:1

CLSID ključ se treba dodati u direktorijum:

[HKEY_LOCAL_MACHINE\Software\Microsoft\Inbox\Svc\SMS\Rules]

Međutim, nije svaki program koji je identifikovan na opisani način na mobilnom uređaju zlonamjeran. Ukoliko korisnik ukloni pogrešan ključ, neki važni programi mogu prestati raditi. Kada korisnik otkrije sličan ključ koji je dat u primjeru prilikom donošenja odluke treba se pouzdati u antivirusni program, [90].

9.5.1.1.2. Imenik

U korporativnom okruženju imenik je jedna od najvažnijih aplikacija na mobilnom uređaju. Krađa kontaktnih podataka može imati kobne posljedice za zaposlene i firmu. Napadač može, ukoliko uspješno podmetne zlonamjerni program, ukrasti podatke sa mobilnog uređaja, među njima i kontakte osoba u imeniku. Napadač tada može osobama čije je kontakte ukrao slati poruke sa zlonamjernim programima u dodatku, poruke koje sadrže linkove na veb stranicu koja sadrži zlonamjerne programe i/ili poslati poruku u kojoj navodi korisnika na otkrivanje povjerljivih podataka. Napadač može iskoristiti ugrađene alate za stvaranje sigurnosne kopije (backup) imenika, kao što su IPOutlok, ItemCollection, te izmijeniti podatke u imeniku i poslati takve podatke nekom drugom.

9.5.1.1.3. Video

Većina mobilnih telefona u današnje vrijeme ima kameru kojom se mogu snimati fotografije i video sadržaj. Napadač može podmetnuti posebno oblikovani programski kod kojim preuzima upravljanje kamerom na mobilnom uređaju. Ali, kako korisnici uglavnom čuvaju svoje mobilne uređaje u džepu ili torbici, mjestima s kojih nije korisno slikati ili snimati video sadržaj, vjerovatnoća zloupotrebe je vrlo mala. Veći sigurnosni problem je ukoliko napadač preuzme upravljanje nad mobilnim telefonom i sadržajem koji je sačuvan u direktorijumu kamere. Na mobilnim telefonima je uobičajeno da postoji poseban direktorijum za smještanje multimedijalnog sadržaja kojem se može pristupiti putem kamere. U slučaju uspješnog napada, napadač može ugroziti sigurnost fotografija i video snimaka koje se nalaze na telefonu. Napadač može postaviti posebno oblikovani program da pošalje sve fotografije na neku adresu elektronske pošte, [90].

9.5.1.1.4. Snimci telefonskih razgovora

Mnogi mobilni telefoni imaju aplikacije koje mogu snimati telefonske razgovore. Na primjer, na operativnom sistemu Windows Mobile moguće je instalirati aplikaciju „Waveform Audio Functions“ za snimanje i reprodukciju audio datoteka. Aplikacija je vrlo slična i temelji se na onima koje se koriste na ličnim računarima, tako da napadač može iskoristiti sigurnosne propuste tih aplikacija i prilagoditi ih programima namijenjenim mobilnim uređajima. Audio sadržaj snimljen modernim mobilnim telefonom visokog je kvaliteta, čak i ako je sadržaj snimljen dok se uređaj nalazio u korisnikovom džepu. Mobilni uređaji imaju ograničen prostor za smiještanje podataka i datoteka tako da se sadržaj ne može snimati neograničeno dugo. Ukoliko napadač podmetne posebno oblikovani program i preuzme upravljanje nad snimanjem zvuka, može snimati proizvoljno dugo i poslati datoteku u poruci elektronske pošte ili multimedijalne poruke, [90].

9.5.1.1.5. Istorija poziva

Zapisi o pozivima mogu koristiti napadaču i on može podmetnuti posebno oblikovani program kako bi pročitao podatke o pređašnjim pozivima. Korisnici bi u svrhu zaštite trebali pratiti zapise o pozivima i povremeno ih obrisati, [90].

9.5.1.1.6. Dokumentacija

Mnogi korisnici mobilnih telefona čitaju i spremaju dokumente tipa Word, Excel ili PDF na svoje telefone. Napadač može podmetnuti zloćudni program kojim će ukrasti takve datoteke upotrebom metode opisane u dijelu „Tekstualne poruke“. Datoteke sa ekstenzijama *.doc, *.xls i *.pdf su popularne mete napadača. Preporučuje se da korisnici mobilnih telefona ne čuvaju važne i povjerljive dokumente na svojim uređajima, [90].

9.5.1.1.7. Upotreba clipboard-a

Sigurnosni propusti vezani uz *clipboard* su neki od najčešćih programskih propusta. U slučaju postojanja programskog propusta vezanog za *clipboard*, napadač ga može iskoristiti za prepisivanje istog. Ukoliko se to dogodi, napadač može podmetnuti proizvoljni programski kod. Operativni sistemi mobilnih telefona vrlo su slični operativnim sistemima ličnih računara i upotreba *clipboard-a* je uobičajena, [90].

REGISTAR SLIKA

POGLAVLJE 1

POGLAVLJE 2

POGLAVLJE 3

POGLAVLJE 4

POGLAVLJE 5

POGLAVLJE 6

POGLAVLJE 7

POGLAVLJE 8

POGLAVLJE 9

REGISTAR TABELA

SPISAK SKRAĆENICA

ACL-Asynchronous Connectionless Link
AES-Advanced Encryption Standard
AH-IPSec Authentication Header
APD-Avalanche Photo Diode
API-Application Program Interface
ARPANET-Advanced Research Projects Agency Network
ARP-Address Resolution Protocol
ARPU-verage Revenue Per User
AS-Autonomous Systems
ASCII-American Standard Code for Information Interchange
ATM-Asynchronous Transfer Mode
AuC-Authentication Center
BGP-Border Gateway Protocol
BOOTP-BOOTstrap Protocol
BPON-Broadband Passive Optical Networks
BRAS-Broadband Remote Access Server
BSC-Base Station Controller
BSS-Base Station Subsystem
BSSGP-Base Station Susystem GPRS Protocol
BTS-Base Transceiver Station
CA-Certification Authorities
CAC-Call Admission Control
CAC-Carrier Access Code
CC-Circuit Switched
CC-Country Code
CDMA-Code Division Multiple Access
CGI-Comom Gateway Interface
CO-Central Office
COO-Cell of Origin
CSMA/CD-Carrier Sense Multiple Access with Collision Detection
CWDM-Coarse Wavelength Multiplexing
DES- Data Encryption Standard
DLL-Data Link Layer
DMT-Discrete Multitone
DNS-Domain Name System
DSL-Digital Subscriber Line
DSLAM-Digital Signal Access Multiplexer
DSP-Digital Signal Processor
DSSS-Direct Sequence Spread Spectrum
DV-Distance Vector
DWDM-Danse Wavelength Division Multiplexing
FTP-File Transfer Protocol
EDGE-Enhanced GPRS
EDI-Electronic Data Interchange
ESP-Encapsulating Security Payload

EGP-Exterior Gateway Protocols
EIR-Equipment Identity Registrar
ENUM tElephony Numbering Mapping)
EPON-Ethernet PON
ES-Elementary Stream
ETL- Extract Transform and Load
ETSI-European Telecommunication Standard Institute
FCS-Frame Check Sequence
FEC-Forwarding Equivalence Class
FHSS-Frequency Hopping Spread Spectrum
FTTB-Fiber to the Building
FTTH-Fiber to the Home
FTTN-Fiber to the Node
FTTP-Fiber to the Premises
FQDN-Fully Qualified Domain Name
GGSN-Gateway GPRS Support Node
GMSK-Gaussian Minimum Shift Keying
GNU General Public License
GoP-Group of Pictures
GPON-Gigabit PON
GPRS-General Packet Radio Services
GSM-Global System for Mobile Communications
GSN-Global Subscriber Number
GTP-GPRS Tunneling Protocol
HDLC-High Level Data Link Control
HLR-Home Location Registrar
HSCSD -High Speed Circuit Switched Data
HTML-HyperText Markup Language
HTTP-Hypertext Transfer Protocol
IAB -Internet Architecture Board
ICMP-Internet Control Message Protocol
ICT-Information and Communications Technology
IDEA-International Data Encryption Algorithm
IEEE-Institute of Electrical and Electronic Engineers
IETF-Internet Engineering Task Force
IGMP- IP Group Membership Protocol
IGP-Interior Gateway Protocol
IM-Instant Messaging
IMEI-International Mobile Equipment Identity
IMS-IP Multimed Susystem
IMSI -International Mobile Subscriber Identity
InterNIC-Internet Network Information Center
IP-Internet Protocol
IPTV-Internet Protocol TV
IR-InfraRed
IRC-Internet Relay Chat

IRM-Internet Relationship Management
ISDN-Integrated Digital Suscriber Line
ISP-Internet Service Provider
IS-IS-Intermediate System
ISM -Industrial Scientific-Medicine
IT-Information Technology
ITU- International Telecommunication Union
IVR-Interactive Voice Response
IVVR-Interactive Voice and Video Response
JPEG-Joint Protocol Expert Group
LAI-Location Area Identity
LAN-Local Area Network
LDAP-Lightweight Directory Access Protocol
LDP-Label Distribution Protocol
LER-Label Edge Router
LFA -Label-Swapping Forwarding
LLC-Logical Link Control
LS-Link State
LSP-Label Switched Path
LSR-Label Switching Router
MAC-Medium Access Control
MAP-Mobile Application Part
MAN-Metropoliten Area Network
MAU-Multistation Access Unit
MC -Multipoint Controller
MCU-Multipoint Control Unit
ME-Mobile Equipment
MEGACO-Media Gateway Controller
MGCP-Media Gateway Control Protocol
MGW-Media Gateway
MOS-Mean Opinion Score
MPEG-Moving Picture Expert Group
MPLS-Multiprotocol Label Switching
MPTS-Multi Program Transport Stream
MRP-Material Requirements Planning
MS-Mobile Station
MSB-Most Significant Bits
MSAN-Multi Service Access Node
MSC-Mobile Switching Centre
MSISDN-Mobile Subscriber ISDN Number
MTU-Maximum Transmission Unit
NAPTR-Naming Authority Pointer
NDC-National Destination Code
NGA-Next Generation Access
NIC-Network Interface Card
NNTP-Network News Transport Protocol

NT-Network Termination
ODN-Optical Distribution Network
OLT-Optical Line Terminal
OMS-Operation and Maintenance Subsystem
ONU-Optical Network Unit
ONT-Optical Network Terminal
OS-Operating System
OSI-Open Systems Interconnection
OSPF-Open Shortest Path First
PCM-Pulse Code Modulation
PCR- Program Clock Reference
PCU-Packet Control Unit
PDA–Personal Digital Assistant
PDN-Packet Data Network
PES-Packetized Elementary Stream
PES-Proposed Encryption Standard
PGP-Pretty Good Privacy
PHP-Personal Home Page
PID-Packet Identification Code
PIN-Personal Identification Numbers
PIN-Positive Intrinsic Negative
PKI-Public Key Infrastructure
PLC-Packet Loss Concealment
PMT-Program Map Table
POH-Path Over Head
POP-Point of Presence
PPP-Point-to-Point
PSI-Program Specific Information
PSTN-Public Switched Telephone Network
POTS-Plain Old Telephony System
PUSI-Payload Unit Start Indicator
QAM-Quadrature Amplitude Modulation
QoE-Quality of Experience
QoS-Quality of Service
RAM-Random Access Memory
RIP-Routing Information Protocol
RLC-Radio Link Control
RNC-Radio Network Controller
RNS-Radio Network Subsystem
RTP-Real Time Transport Protocol
RTCP-Real Time Control Protocol
SGSN-Serving GPRS Support Node
SIM-Subscriber Identification Module
SDH-Synchronous Digital Hierarchy
SDP-Session Description Protocol
SET-Secure Electronic Transaction

SHA-Secure Hash Algorithm
SHE-Super Head End
SIP-Session Initiation Protocol
SLA-Service Level Agreement
SMTP-Simple Mail Transfer Protocol
SN-Subscriber Number
SNDCP-Subnetwork Dependent Convergence Protocol
SNMP-Simple Network Management Protocol
SOA-Service-Oriented Architecture
SOF-Start of Frame
SONET-Synchronous Optical Network
SPTS-Single Program Transport Stream
SSL-Secure Socket Layer
STB-Set Top Box
STP-Shielded Twisted Pair
TCP-Transmission Control Protocol
TD-Time Division
TDM-Time Division Multiplexing
3GPP-Third Generation Partnership Project
TLS-Transport Layer Security
TMSI-Temporary Mobile Subscriber Identity
TOA -Time of Arrival
TPON-Telephone Passive Optical Networks
TTL-Time to Live
UAC-User Agent Client
UAS-User Agent Server
UDP-User Datagram Protocol
UMTS-Universal Mobile Telecommunications System
URL-Uniform Resource Locator
USIM-Universal SIM
UTP-Unshielded Twisted Pair
UTRAN-UMTS Radio Access Network
VC-Virtual Channel
VC-Virtual Container
VCI-Virtual Channel Identifier
VDSL-Very High Speed DSL
VHO-Video Hub Offices
VLAN-Virtual Local Area Network
VLR-Visited Location Registrar
VoD-Video on Demand
VoIP-Voice over Internet Protocol
VP-Virtual Path
VPI-Virtual Path Identifier
VPN-Virtual Private Network
VSO-Video Switching Offices
WAE-Wireless Application Environment

WAN-Wide Area Network
WAP-Wireless Application Protocol
W-CDMA-Wideband Code Division Multiple Access
WDM-Wavelength Division Multiplexing
WDP -Wireless Datagram Protocol
WiMAX-Worldwide Interoperability for Microwave Access
WLAN-Wireless Local Area Network
WML-Wireless Markup Language
WSP-Wireless Session Protocol
WTLS-Wireless TLS
WTP-Wireless Transaction Protocol
W3C -World Wide Web Consortium
WWW-World Wide Web
XML-EXtensible Markup Language

LITERATURA

[1] A. Bažant, „Uvod u xDSL i ADSL", Sveučilište u Zagrebu, 2006.

[2] Agilent Technologies, „UnderstandingDSLAM and BRAS Access Device, white paper, 2006.

[3] A.Nešković, I.Janković, „*Integracija Interneta sa javnim mobilnim ćelijskim sistemima*", Akademska misao, Beograd, 2010.

[4] A. Petrović, I. Reljin, „Mogućnost realizacije IPTV servisa", *17. Telekomunikacioni forum TELFOR*, 2009.

[5] Architecture & Transport Working Group, „Triple-play Services Quality of Experience (QoE) Requirements", 2006.

[6] A. Flavia, M-Lima, F.R.Ribeiro „Monitoring based on statistical analysis for evaluating quality of calls in VoIP environment", Department of Engineering of Teleinformatics and Computer Science, Fortaleza, Brazil, 2005.

[7] Broadband Forum, „ADSL2/ADSL2+/ADSL-RE/VDSL2", tehnički izvještaj, 2008.

[8] B. Billali, M.Selimi, „*IPTV over xDSL*", master thesis, Sapienza, Universita di Roma, 2011.

[9] B. Goode, „Voice over Internet Protocol (VoIP)", *Proceedings of the IEEE,* Vol. 90, No 9, 2002., pp. 1495-1517.

[10] B.Odadžić, M.Stanković i M.Janković, „Mreže za pristup sledeće generacije i regulatorni izazovi",*17-ti Telekomunikacioni forum TELFOR*, Beograd, pp 46-49, 2009

[11] B.Radenković, M.Despotović, „Priručnik za pripremu prijemnog ispita za upis na master studije", Beograd, 2012.

[12] B. Furth, „*The VC-1 and H:264 Video Compression Standards for Broadba*" *Ericsson Nikola Tesla REVIJA 17*, pp. 28-43, 2004.

[13] C.Hellberg, D. Green, T.Boyes, „*Broadband Network Architectures"*, Prentice Hall, 2007.

[14] C. Fransoa, „IPTV over XDSL", Sapienza, Universita di Roma.

[15] C.Hoene,B.Rathe,A.Wolisz, „On the Importance of a VoIP Packet", Technical University of Berlin, 2003.

[16] C.Kozierok, „TCP/IP guide", Kozierok, 2005.

[17] D.M.Sultan and M.T Arefin, „GPON, the Ultimate Perteinent of Next Generation Triple-Play Bandwidth Resolution", *Journal of Telecommunications and Information Technology*, pp 53-60, 2009.

[18] D. Pan, „A Tutorial on MPEG/Audio Compression" *Multimedia IEEE*, 1995.

[19] D. Singelee and B. Preneel, „The Wireless Application Protocol" in *International Journal of Network Security*, Vol. 1, No. 3, pp. 161-165, 2005.

[20] DSL forum, „Migration to Ethernet-Based DSL Aggregation",tehnički izvještaj, 2006.

[21] E.Osborne, A.Simha, „*Traffic Engineering with MPLS*“, Cisco Press, jul 2002.

[22] ETSI Specification, TS 102 051 V1.1.1 „ENUM Administration in Europe“, 2002

[23] E. Weinman and Peter Rysavy, „Mobile Commerce: State of the Market“ *InformationWeek reports, Mobile commerce world,* San Francisco, 2013.

[24] G. Heine and H. Sagkob, „*GPRS – Gateway to Third Generation Mobile Networks“*, Boston, Artech House, 2003.

[25] G. Huston, „ENUM-Mapping the E.164 Number Space into the DNS“; Telstra, 2000.

[26] H.Schulzrinw, S.Casner, R.Frederic, V.Jacobson, „RTP: A Transport Protocol for Real-Time Application“, RFC 3550, IETF, 2003.

[27] IBM, „*An introduction to Wireless Technology“*, IBM Corporation, 2005.

[28] H. Wang, „*Overview of Bluetooth Technology“*, Depertment of Electrical Engineering State Collage, 2001.

[29] I. F. Akyildiz, „The evolution to 4G cellular systems: LTE-Advanced“ in Physical Communication 3, *Elseviar* pp. 217-244, 2010.

[30] I. Puy, „Bluetooth“, Hochschule furtwangen univrsity, 2008.

[31] I. Reljin, M.Ivančić, Arhitekture multipleksiranja u multimedijalnim sistemima, *25-ti PosTel*, 2007, Beograd, 2007.

[32] ITU-T Recommendation G.984.1 „Gigabit-capable passive optical network (GPON): General characteristic“, 2008.

[33] ITU-T Recommendation 984.7 „Gigabit capable passive optical network (GPON): long reach“, 2010

[34] Javvin Technologies, „*Network Protocol Handbook“*, secon edition, 2005.

[35] J. Davidson, J. Peters, M. Bhatia, S. Kalidindi, S. Mukherjee, „*Voice over IP Fundamentals“* Cisco Press, second edition, 2006.

[36] J. Peterson, H. Liu, J. Yu, B. Campbell, „Using E.164 numbers with the Session Initiation Protocol (SIP)“, Internet RFC 3824, 2004.

[37] J.Postel, „User Datagram Protocol“, RFC 768, IETF, 1980.

[38] J.Postel, „Transmission Control Protocol-DARPA Internet Program Protocol Specification“, IETF, 1981.

[39] J.Postel, „Domain Name System Structure and Delegation“, RFC 1591, IETF, 1994.

[40] J.Postel, J.Reynoldy, „File Transfer Protocol (FTP)“, RFC 959, IETF, 1985.

[41] J. Peterson, „Enumservice Registration for Session Initiation Protocol (SIP) Addresses-of-Record“, RFC 3764, J. Peterson, april 2004.

[42] J. S. Beasley, „*Networking“*, 2nd ed, Pearson Education, Inc., 2008.

[43] K.Kerpez,D.Waring,G.Lapiotis, „IPTV Service Assurance“, *IEEE Communications Magazine*, pp 166-172, 2006.

[44] K. Wallace, „*Authorized Self-Study Guide, Cisco Voice ove IP (CVOICE")*, 3rd ed, Indianapolis, Cisco Press, 2009.

[45] L.Anderson, T.Madsen, „Provider Provisioned Virtual Private Network (VPN) Terminogy", RFC 4026, IETF, 2005.

[46] L. Harte, „*IPTV Basics"*, Althos Publishing, 2007.

[47] L. Kleinrock, „An Erly History of the Internet", IEEE Communications Magazine, vol. 48, no. 8, , pp 26-36, 2010.

[48] L. Parziale, D.t.Britt, C.Davis, J.Forrester, W.Liu, C.Matthews, N.Rosselot, „*TCP/IP Tutorial and Technical Overview"*, ibm.com/redbooks, decembar, 2006.

[49] L.Sun, „*Speech Quality Prediction for Voice over Internet Protocol Networks"*, Ph.D thesis, 2004.

[50] M. Aksić, „*Bezbednosni problemi i zaštita bežičnih i mobilnih mreža*" Magistarska teza, Univerzitet Singidunum, Beograd, Republika Srbija, 2013.

[51] M. Listanti and V. Eramo, „Architectural and Technological Issues for Future Optical Internet Networks", pp 82-92, Septembar 2000.

[52] M.P.Clark, „*Data networks, IP and the Internet*", Wiley, New York, 2003

[53] M.W.Murhammer, K.K.Lee and P.Motallebi, „*IP Network Design Guide"*, 2nd ed. IBM, 1999.

[54] M. Stamp, „*Information security: principles and practice"*, John Wiley & Sons, 2006.

[55] M.Stojanović, V.A. Raspopović, „*Savremene IP mreže, arhitekture, tehnologije i protokoli*", Akademska misao. Beograd, 2012.

[56] M. Liotine, „*Mission-critical Network Planning*", Artech House, 2003.

[57] M. W. Murhammer, „IP Network Design Guide", in *International Technical Support Organization*, 2nd ed., 1999.

[58] N.Degrande, K.Laevens, D.D. Vleeschauwer, „Increasing the User Perceived Quaility for IPTV Services", *IEEE Communication Magazine*, pp 94-100, Feb 2008.

[59] N. Ghani, S. Dixit and T.-S. Wang, „On IP-over-WDM Integration", *IEEE Communication Magazine*, Mart 2000, pp. 72-84

[60] P. Golden, „*Implementation and Applications of DSL Technology"*, New York, Taylor & Francis Group, 2008.

[61] P. Golden, H.Dedieu, K.Sjacobsen, „*DSL Technology*", CRC press, 2008.

[62] P.E.Eriksson and B. Odenhammar, „VDSL: Next Important Broadband Technology", *Ericsson Rewiew*, No.1, 2006.

[63] P. Kumar, A. Pande, A. Mittal, and A. Mudgal, „Distributed video coding and content analysis for resource constraint multimedia applications" *Ubiquitous Multimedia and Mobile Agents: Models and Implementations*, p. 251, 2011.

[64] P.Oorschot, A.Menezes, *„Handbook of Applied Cryptography"*, CRC Press, 1997.

[65] R. L. Freeman, „*Radio System Design for Telecommunications*“, 3rd ed., New Jersey, John Wiley & Sons, 2007.

[66] R. Kreher, „*UMTS Performance measurements: A Practical Guide to KPIs for the UTRAN Environment*“, John Wiley & Sons, Ltd., 2006.

[67] RSA Data Security, „Understanding Public Key Infrastructure (PKI), 1999.

[68] S.Garnfikel, „*PGP: Pretty Good Privacy*“, O Reilly and Associates, 1995.

[69] S. Alvarez, „*QoS for IP/MPLS Networks*“, Indianapolis, Cisco Press, 2006.

[70] S.Dixit, R.Prasad, „*Wireless IP and Building the Mobile Internet*“, Artech House, 2003.

[71] S.Han, W. Yue and S. Smith, „FTTx and xDSL: A Business Case Study of GPON versus Copper for Broadban Access Networks“, Fujitsu, technical documentations, 2006.

[72] Snell&Wilcox, „MPEG encoding Basics“, tehnički izvještaj, 2002.

[73] Telecom Regulatory Authority, „*WiFi Technology*“, 2003.

[74] Tektronix, „A Guide to IPTV: The Tecnologies, the Challenges and How to Test IPTV“, 2007.

[75] T. Halonen, J.Romero and j:Melero, „*GSM, GPRS and EDGE performanse*“, 2nd ed., England: John Wiley & Sons Ltd, 2003.

[76] T. Lammle, „*CCNA: Cisco Certified Network Associate*“, 5th ed, Indianapolis, Wiley Publishing, 2005.

[77] V. Marijanović, „*Virtuelne privatne mreže*“, magistarski rad, departman za postdiplomske studije, Univerzitet Singidunum, Beograd, Republika Srbija, 2011.

[78] V.A.Raspopović, G.Marković i V.Radonjic, „Pasivne optičke mreže za pristup“, *PosTel*, Beograd, pp 291-302, 2007

[79] Wimax Outlook Series, „A to Z WiMax, Complete Reference“, John Wiley & Sons, 2005

[80] WiMAX FORUM, „*Mobile WiMAX – Part II: A Comparative Analysis*“, 2006.

[81] Wireless Application Protocol Forum Ltd, „WAP Architecture“, 2000-2001.

[82] Wireless Application Protocol Forum Ltd, „Wireless Application Protocol: WAP 2.0“, 2002.

[83] W. Kou and Y. Yesha, „Wireless Application Protocol“, in *Enabling Technologies for Wireless E-Business*, 2006.

[84] W. Simpson and H. Greenfield, „*IPTV and Internet Video: Expanding the Reach of Television Broadcasting*“ , 2nd ed, Focal Press, 2009.

[85] X. Chen, „Transporting Compressed Digital Video“, Kluwer Academic Publishers, 2002.

[86] Z.Stojanović, „Osnovni elementi arhitekture televizije zasnovane na Internet protokolu (IPTV), Tehnika, vol 66, No 3, jun 2012, pp 426-431, Beograd, Srbija.

[87] Z.Stojanović, B.Jokić i S. Jovanović, „Triple Play u mreži M:TEL-a“, *56-ta konferencija za elektroniku, telekomunikacije, računarstvo, automatiku i nuklearnu tehniku, ETRAN*, 2012

[88] Z.Stojanović i S.Jovanović, „IPTV u mreži M:TEL-a“, *19-ti Telekomunikacioni forum, TELFOR*, No 62, Vol 1, pp 250-253, 2011.

[89] Z.Stojanović i B.Jokić, „Arhitektura mreže za realizaciju triple play-a“, *Tehnika* , Beograd, Srbija, pp. 103-110, 2013.

[90] Z.Stojanovic „*Elektronsko poslovanje*“ Slobomir P Univerzitet, Grafom Brčko, 2014.

[91] Z.Stojanović, „Formiranje paketa servisa kao način zadržavanja postojećih korisnika i povećanja ARPU-a na tržištu Bosne i Hercegovine“, *INFOM*, Beograd, Srbija, pp 44-48, decembar 2014.

[92] Ž. Panian, „*Bogatstvo interneta“*, Zagreb, Hrvatska: Strijelac, 2000.

CIP - Каталогизација у публикацији
Народна и универзитетска библиотека
Републике Српске, Бања Лука

004.738.5(075.8)

СТОЈАНОВИЋ, Звездан
Arhitektura, protokoli i servisi Interneta / Zvezdan Stojanović. - Brčko : Evropski univerzitet Brčko distrikta, 2015 (Banja Luka : Markos). - VI, 222 str. : ilustr. ; 25 cm

Tiraž 200. - Bibliografija: str. 218-222.

ISBN 978-99976-605-9-6

COBISS.RS-ID 4757016