UNIVERZITET SINGIDUNUM
FAKULTET ZA POSLOVNU INFORMATIKU

Mladen Veinović
Aleksandar Jevremović

UVOD U RAČUNARSKE MREŽE

Beograd, 2007. godine

Autori:
Prof. dr Mladen Veinović, dipl.inž.
Aleksandar Jevremović, dipl.inž.

Recenzenti:
Prof. dr Milan Milosavljević
Prof. dr Branko Kovačević

Izdavač:
UNIVERZITET SINGIDUNUM
FAKULTET ZA POSLOVNU INFORMATIKU

Za izdavača:
Prof. dr Milovan Stanišić

Dizajn korica:

Godina izdanja:
2007.

Tiraž:
200 primeraka

Štampa:
CICERO-print
Beograd

1.Uvod....12
1.1. Razlozi za umrežavanje....14
1.1.1 Zajedničko korišćenje informacija (podataka)....14
1.1.2 Zajedničko korišćenje hardvera i softvera....15
2.Prenos podataka i osnove komunikacija....17
2.1. Vrste prenosa podataka....19
2.1.1.Prenos podataka sa komutacijom veza (circuit switched)....20
2.1.2.Prenos podataka sa komutacijom paketa (packett switched)....21
2.1.3.Prenos podataka virtuelnom vezom (virtual circuit)....22
3.Osnove umrežavanja, hardver i softver....23
3.1. Pasivna mrežna oprema....24
3.1.1.Koaksijalni kabl....25
3.1.2.Kabl sa upredenim paricama....25
3.1.3.Optički kablovi....28
3.1.4.Kablovi i elektromagnetno zračenje....29
3.1.5.Strukturno kabliranje....30
3.2. Aktivna mrežna oprema....32
3.2.1.Ripiter (Repeater)....32
3.2.2.Hab (Hub)....32
3.2.3.Mrežni most (Bridge)....33
3.2.4.Svič (Switch) – skretnica....33
3.2.5.Usmerivač (Router)....34
3.2.6.Mrežni prolaz (gateway)....36
3.2.7.Bezbednosna barijera (firewall)....36
3.2.8.Proxy....38
3.3. Interfejsi računara....39

3.3.1.Mrežna kartica....39
3.3.2.Modem....39
3.3.3.ISDN Terminal Adapter....39
3.3.4.ADSL/DSL modem....40
3.4. Protokoli....41
3.4.1.Protokoli bez uspostavljanja veze....43
3.4.2.Protokoli sa uspotavljanjem veze....43
3.5. Standardizacija i organizacije....44
3.4.1Organizacije za standardizaciju....44
4.Tipovi mreža (kategorizacija)....46
4.1. Mediji i načini prenosa podataka....48
4.1.1.Kablirane mreže....48
4.1.2.Bežične mreže....52
4.2. Topologije....53
4.3. Veličina....55
4.3.1.Lokalna računarska mreža (Local Area Network, LAN) 55
4.3.2.Regionalna računarska mreža (Wide Area Network, WAN)....56
4.4. Funkcionalni odnos članova (arhitektura aplikacija)....57
4.4.1.Host-based mreže....57
4.4.2.Klijent-server mreže....58
4.4.3.Peer-to-peer (P2P) mreže....64
5.Slojevitost i referentni modeli....68
5.1. OSI model....71
5.2. Internet model (TCP/IP)....73
6.Fizički sloj....74
6.1. RS-232....74

6.2. USB (Universal Serial Bus) ... 74
6.3. FireWire (IEEE1394) ... 75
6.4. IrDA (Infrared Data Association) ... 75
6.5. Bluetooth ... 76
6.5.1. Bluetooth proizvodi ... 76
6.5.2. Princip rada ... 77
6.6. Ethernet ... 79
6.7. 802.11 (WiFi) ... 81
6.8. ISDN (Integrated Services Digital Network) ... 83
6.9. xDSL (Digital Subscriber Line) ... 85
7. Sloj veze ... 87
7.1. Podela sloja veze ... 89
7.1.1. Kontrola pristupa medijimu (Media Access Control, MAC) ... 89
7.1.2. Kontrola pristupa ... 89
7.1.3. Pristup na osnovu sadržaja ... 92
7.1.4. MAC adresa ... 93
7.1.5. Kontrola logičke veze (Logic Link Control, LLC) ... 94
7.2. Kontrola toka ... 96
7.3. Kontrola greške ... 97
7.3.1. Izvori grešaka ... 97
7.3.2. Detekcija greške ... 98
7.3.3. Korekcija greške ... 101
7.4. Protokoli na sloju veze - Data Link Protocols ... 103
7.4.1. Asinhroni prenos ... 103
7.4.1.1. Asinhroni prenos fajlova ... 103
7.4.2. Sinhroni prenos ... 104

7.4.3.Ethernet 106
7.5. Efikasnost prenosa 108
7.6. Ethernet 109
7.6.1.Ethernet (IEEE 802.3) 109
7.6.2.Osnovni principi Ethernet-a 112
7.6.3.Switched Ethernet 112
7.7. Address Resolution Protocol (ARP) 113
7.8. Token Ring 114
7.9. FDDI (Fiber Distributed Data Interface) 114
7.10. 802.11(WiFi) 115
7.10.1.Komponenete WLAN-a 116
7.10.2.Princip rada WLAN-a 117
8.Mrežni sloj 119
8.1. Internet Protocol (IP) 120
8.1.1.Internet Protocol verzije 4 (IPv4) 120
8.1.2.Mreže i klase mreža 121
8.1.3.Specijalni opsezi adresa 123
8.1.4.CIDR (Classless Inter-Domain Routing) 124
8.1.5.Maska pod-mreže 125
8.1.6.Primer podele mreže klase C na podmreže 128
8.2. Internet Protocol verzije 6 (IPv6) 131
8.2.1.Zaglavlje IPv6 paketa 131
8.2.2.IPv6 adresiranje 134
8.2.3.Kompatibilnost sa IPv4 135
8.3. Internet Control Message Protocol (ICMP) 136
8.4. Internet Group Management Protocol (IGMP) 139

8.5. Internetwork Packet Exchange (IPX)....141
8.6. IPsec....142
9.Transportni sloj....144
9.1. Transmission Control Protocol (TCP)....147
9.1.1.TCP segmenti....148
9.1.2.Uspostavljanje i prekid veze....151
9.1.3.Pouzdanost i performanse....152
9.2. User Datagram Protocol (UDP)....154
9.3. Stream Control Transmission Protocol (SCTP)....156
9.4. Sequenced Packet Exchange (SPX) protokol....157
9.5. Internet SCSI (iSCSI)....158
10.Sloj aplikacije....159
10.1. Telnet....160
10.1.1.Secure Shell (SSH)....162
10.1.2.Remote Desktop....163
10.2. Domain Name System (DNS)....164
10.2.1.Istorijat problema i rešenja....165
10.2.2.Hosts fajlovi....166
10.2.3.Teorija rada DNS-a....168
10.2.4.Keširanje kod DNS-a....172
10.3. File Transfer Protocol (FTP)....174
10.3.1.Ciljevi i mane....174
10.3.2.Sigurni FTP....175
10.4. Elektronska pošta (E-mail)....176
10.4.1.Principi rada e-mail servisa....176
10.4.2.Protokoli e-mail servisa....178

10.5. SMB/CIFS....179
10.6. HTTP, WWW i Web 2.0....180
10.6.1. Nastanak i uloga Web servisa....180
10.6.2. Noseće komponente Web servisa....182
10.6.3. HyperText Transfer Protokol (HTTP)....183
10.6.4. Format dokumenata (HTML)....184
10.6.5. Server (Web/HTTP server)....185
10.6.6. Klijent (Web čitač)....186
10.6.7. Adresa dokumenta/resursa (URI/URL)....188
10.6.8. Evolucija Web servisa....189
10.6.9. Razvoj serverskog dela Web-a....190
10.6.10. Razvoj klijentskog dela Web-a....193
10.6.11. Razvoj HTTP protokola....195
10.6.12. XHTML, CSS, XML, XSLT....196
10.6.13. Nastanak i razvoj Web direktorijuma i pretraživača....198
10.6.14. Ostali izvedeni servisi....199
10.6.15. Web 2.0 (Web aplikacije)....200
10.7. Network Time Protocol (NTP)....201
10.8. Simple Network Management Protocol (SNMP)....202
10.9. Voice over IP (Internet telefonija)....203
10.10. Instant Messaging....204
10.11. Video-konferencija....205
11. Bezbednost, dostupnost i performanse....206
11.1. Mogući napadi i zaštite računarskih mreža....208
11.2. Firewall....211
11.3. IDS i IPS sistemi....214

12.Operativni sistemi računara i mrežna podrška.....215
12.1. Realizacije mrežne podrške u operativnim sistemima.....216
12.2. Unix/Linux operativni sistemi.....219
12.2.1.Konfiguracioni fajlovi.....220
12.2.2.Alati za podešavanje mrežnih parametara.....221
12.2.3.Alati za proveru rada mreže i rešavanje problema.....222
12.2.4.Alati vezani za Dial-Up mreže.....223
12.2.5.Mrežni klijenti i servisi.....223
12.2.6.Podešavanje mrežnih interfejsa (ifconfig).....225
12.2.7.Primer mrežne podrške u OS Linux 2.6.15.....227

Predgovor

Knjiga *Uvod u računarske mreže* namenjena je studentima Fakulteta za poslovnu informatiku Univerziteta Singidunum za pripremu ispita iz predmeta Računarske mreže. Rezultat je višegodišnjeg rada autora u oblastima umrežavanja, mrežnog programiranja, komunikacija i zaštite podataka u računarima i mrežama. Pored svoje osnovne namene knjiga može biti od koristi svim inženjerima koji se u praksi susreću sa umrežavanjem, projektovanjem, instalacijom i administriranjem računarskih mreža. Čitaoci će u njoj naći osnovne koncepte i principe umrežavanja, opis slojevite arhitekture i funkcije pojedinih slojeva kao i njihove protokole, ali i detaljne prikaze najvažnijih Internet protokola i savremenih servisa na aplikativnom nivou.

U uvodnom delu predstavljeni su osnovni pojmovi u umrežavanju i analizirane su glavne komunikacione funkcije koje postoje kod svih mreža nezavisno od njihove veličine. Zatim se prikazuje pasivna i aktivna mrežna oprema, objašnjava se svrha i značaj računarskih protokola i predstavljaju se najvažnije organizacije za standardizaciju u ovoj oblasti. Podela računarskih mreža se može izvršiti na više načina, a u ovoj knjizi su razmatrane mreže u odnosu na komunikacione medijume, toplogiju, veličinu i funkcionalni odnos članova u mreži. U nastavku se preko OSI i TCP/IP modela obrađuju fizički sloj, sloj veze podataka mrežni i transportni sloj i sloj aplikacija. Na fizičkom sloju analiziraju se i žične i bežične komunikacije, a u sloju veze podataka osnovne tehnike za pristup komunikacionom medijumu, formiranje okvira podataka i različite tehnike za prevenciju, detekciju i korekciju grešaka u prenosu. U računarskim mrežama poseban značaj imaju sledeća dva sloja: mrežni i transportni. U okviru mrežnog sloja detaljno su prikazane tehnike adresiranja po standardima IPv4 i IPv6, kao i karakteristični protokoli na ovom sloju ICMP, IGMP, IPX i IPsec. U transportnom sloju koji je odgovoran za isporuku paketa sa kraja na kraj mreže, razmatrana su dva osnovna protokola: TCP i UDP, kao i SCTP, SPX i SCSI interfejs. Sloj aplikacije je detaljno objašnjen. Prikazani su servisi na ovom sloju kao što su Telnet, FTP, E-mail, Internet telefonija, video-konferencija i sl. Ukazujemo na detaljno objašnjeno funkcionisanje DNS-a i Web servisa kao danas najšire prihvaćenih servisa na Internetu. Knjiga obuhvata i osnove bezbednosti i dostupnosti resursa u mreži kroz analizu mogućih napada, ulogu firewall-a, IDS-a i IPS-a. Na kraju je dat prikaz mrežne podrške za Unix/Linux operativne sisteme.

U naslovu ove knjige stoji preambula da ona predstavlja "uvod" zbog kompleksnosti i obima materijala koji se predstavlja. Autori su svesni da nisu obrađeni svi aspekti u umrežavanju, ali je osnovna vodilja autora bila da se studentima omogući što brže i kvalitetnije savladavanje predviđenog nastavnog gradiva. Ako su zbog kratkog roka za pisanje trenutno izostavljeni pojedini

klasični delovi, sa druge strane, posebna pažnja je posvećena savremenim principima, standardima i protokolima u aktuelnim računarskim mrežama.

Knjiga predstavlja prvo izdanje i sve primedbe i sugestije čitalaca su dobro došle.

Beograd, 2007. godine.....Autori

1. Uvod

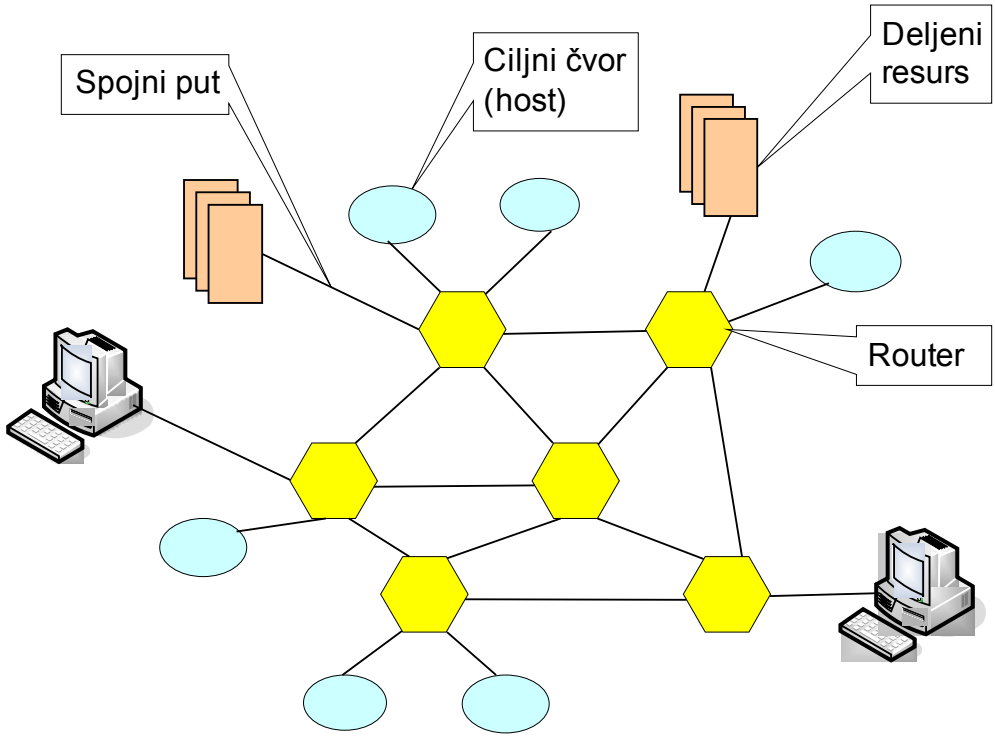
Potreba za informacijama naterala je čoveka da uspostavlja veze sa raznim izvorima informacija i da stvara mreže preko kojih će sebi olakšati prikupljanje, prenos, skladištenje i obradu podataka. Naglim razvojem računarske tehnologije poslednjih godina (povećanje performansi uz pad cena) i sa pravom eksplozijom Interneta, broj korisnika računara i računarskih mreža raste vrtoglavom brzinom. Sa sve moćnijom računarskom opremom svakodnevno se uvode novi servisi, a istovremeno se u umrežavanju postavljaju viši standardi. Vremenom su se mrežni sistemi razvijali da bi danas dostigli nivo praktičnog efikasnog okruženja za razmenu podataka.

Počeci umrežavanja vezuju se za prve telegrafske i telefonske linije kojima su se prenosile informacije do udaljenih lokacija. Dostupnost i fleksibilnost tehnologija današnjih savremenih računarskih mreža omogućava da se sa bilo koje tačke na planeti može povezati na mrežu i doći do željenih informacija. U poređenju sa nekadašnjom cenom korišćenja servisa mreža, cena eksploatisanja današnjih mreža je sve niža. Računarske mreže su danas nezamenjivi deo poslovne infrastrukture, kako velikih, tako i malih organizacija. Poznavanje tehnologije i korišćenje mreža čak izlazi iz okvira primene u poslovanju (koje može da obezbedi poslovnu prednost organizacijama - npr. elektronska trgovina omogućava i malim firmama konkurentnost na tržištu) i zalazi u ostale aspekte života čoveka postajući deo opšte kulture.

Računarska mreža može biti prost skup dva ili više računara, koji su povezani adekvatnim medijumom i koji međusobno mogu da komuniciraju i dele resurse. Koristi se za prenos kako digitalnih tako i analognih podataka, koji moraju biti prilagođeni odgovarajućim sistemima za prenos. Mrežom se prenose računarski podaci, govor, slika, video, a aplikacije na stranama korisnika mogu biti takve da se zahteva prenos podataka u realnom vremenu (govor, video i sl.) ili to ne mora biti uslov (elektronska pošta, prenos datoteka i sl.). Mreža se sastoji od računara, medijuma za prenos (žica, optičko vlakno, vazduh i sl.) i uređaja kao što su čvorišta, svičevi, ruteri itd. koji čine infrastrukturu mreže. Neki od uređaja, kao što su mrežne kartice, omogućavaju vezu između računara i mreže.

Svaka mreža se može svesti na sledeće dve osnovne celine: hardversku i softversku. Hardversku celinu sačinjavaju mrežni čvorovi (*nods*) u kojima se vrši obrada informacija, fizički spojni putevi i deljeni resursi. Čvorovi su delovi mreža u kojima dolazi do obrade podataka. Postoje dve vrste čvorova: čvorovi u kojima se vrši stvarna obrada i oni predstavljaju ciljne čvorove (*hosts*), i čvorovi kojima je uloga da usmeravaju informacije (*routers*). Deljeni resursi su hardverski (štampači, ploteri, faks mašine, diskovi i sl.) ili softverski elementi (datoteke, baze, aplikacije i sl.). Softversku celinu mreže čine protokoli – pravila

po kojima se vrši komuniciranje (razmena podataka) u mreži, operativni sistemi koji su u direktnoj komunikaciji sa hardverom računarskog sistema (i imaju podršku za mrežni hardver i mrežne protokole) i korisnički mrežni softver.



Slika 1.1 Osnovna arhitektura mreže

1.1. Razlozi za umrežavanje

Danas kada su računari relativno dostupni svakom i uz to su izuzetno moćni, umrežavanje povećava efikasnost i smanjuje troškove poslovanja. Osnovni razlozi za umrežavanje su:

- zajedničko korišćenje informacija
- zajedničko korišćenje hardvera i softvera

Konkretnije, računari koji su u mreži mogu zajednički da koriste:

- dokumenta (memorandume, tabelarne proračune, fakture, itd.)
- elektronsku poštu
- softver za obradu teksta
- softver za praćenje projekata
- ilustracije, fotografije, audio i video datoteke
- štampače
- faks mašine
- modeme
- CD-ROM jedinice i druge prenosive jedinice
- ...

1.1.1 Zajedničko korišćenje informacija (podataka)

Mogućnost brzog i jeftinog zajedničkog korišćenja informacija jedna je od najpopularnijih upotreba mrežne tehnologije. Elektronska pošta je ubedljivo najkorišćeniji servis Interneta. Mnoge firme su značajno ulagale u mreže zbog isplativosti elektronske pošte i programa planiranja. Kada postoji zajedničko korišćenje podataka, smanjuje se korišćenje papira, povećava efikasnost, a skoro svaka vrsta podataka je istovremeno na raspolaganju svima kojima je potrebna.

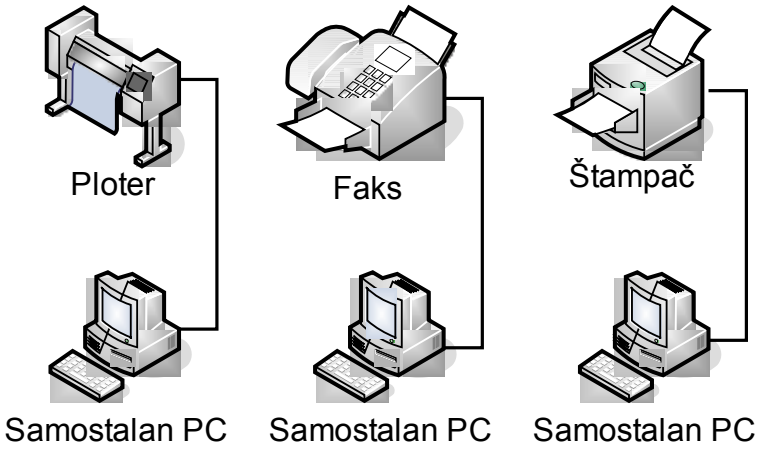
Postoje i situacije vezane za zajedničko korišćenje podataka kod kojih računarske mreže ne samo da smanjuju troškove već su i jedini način na koji je ono izvodljivo. Današnje poslovne sisteme karakteriše što kraće vreme za odgovor na zahteve klijenata kao jedan od glavnih parametara konkurentnosti. Korišćenjem adekvatnih informacionih sistema zasnovanih na računarskim mrežama poslovni sistemi su u mogućnosti da pored toga što informacije pružaju neuporedivo brže u

odnosu na ostale načine informisanja (ličnim kontaktom, telefonom, faksom i sl.) te informacije dostave sa daleko većom tačnošću (manjom verovatnoćom greške).

Kao još jedan reprezentativan primer zajedničkog korišćenja podataka putem računarskih mreža treba navesti i Web servis Internet mreže a pre svega pretraživače Web-a. Korišćenjem pretraživača korisnici imaju besplatan pristup milijardama dokumenata na Web-u čiji izbor mogu odrediti pomoću reči karakterističnih za oblast koja ih interesuje.

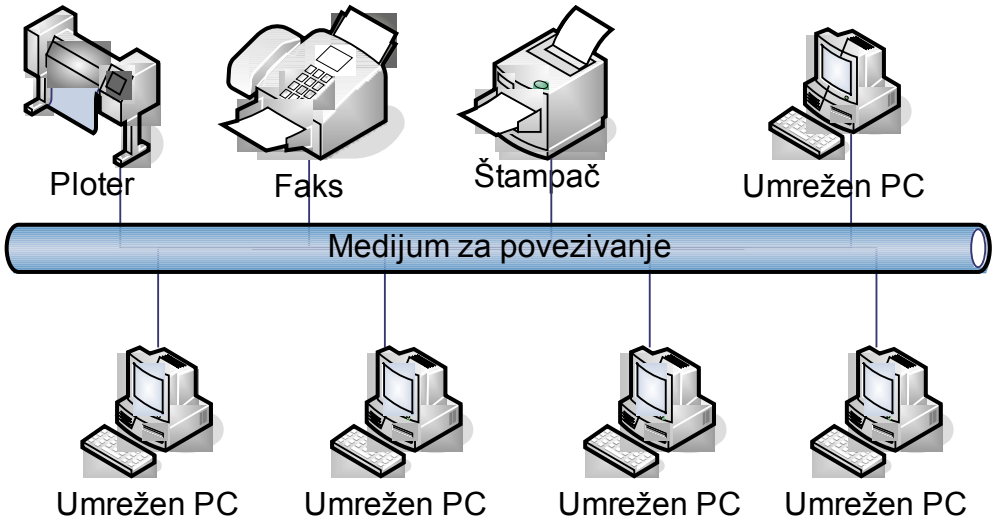
1.1.2 Zajedničko korišćenje hardvera i softvera

Pre pojave računarskih mreža, bilo je neophodno da svaki korisnik ima svoj štampač, ploter, faks ili drugi periferijski uređaj. Jedini način da više korisnika koristi isti uređaj je bio da se naizmenično koristi računar sa kojim je taj uređaj povezan.



Slika 1.2 Samostalne PC konfiguracije

Pojava mreža je otvorila mogućnost da više korisnika istovremeno koristi zajedničke informacije, ali i periferijske uređaje. Ukoliko je štampač neophodan većem broju korisnika koji su u mreži, svi mogu da koriste zajednički mrežni štampač. Mnogo je bolje investirati u jedan kvalitetan uređaj (npr. štampač) nego u desetine slabijih i lošeg kvaliteta.



Slika 1.3 Zajedničko korišćenje hardvera u mrežnom okruženju

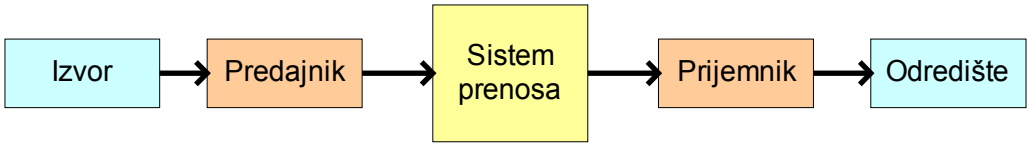
Mreže se mogu upotrebiti i za zajedničko i standardizovano korišćenje aplikacija, kao što su programi za obradu teksta, programi za tabelarne proračune ili baze podataka, u situacijama kada je bitno da svi koriste iste aplikacije i iste verzije tih aplikacija. Na ovaj način se dokumenti jednostavno zajednički koriste, a postoji i dodatna efikasnost u tom smislu da je jednostavnije i bolje da ljudi potpuno savladaju jedan program, nego da moraju da rade sa četiri ili pet različitih programa. Kada su računari umreženi, to značajno pojednostavljuje i njihovu podršku. Za jednu kompaniju je daleko efikasnije kada tehničko osoblje održava jedan operativni sistem i kada su svi računari identično podešeni prema konkretnim potrebama te kompanije.

Veoma često računari u mreži poseduju iste mogućnosti po pitanju procesorske snage i radne memorije što znači da su u stanju da podjednako efikasno obave isti zadatak. Međutim, često jedan od računara ima pristup određenim resursima koji nisu dostupni ostalim računarima. Ovakva kontrola pristupa je najčešće uslovljena bezbednosnim aspektima a može biti i posledica nemogućnosti konkurentnog pristupa resursu. U takvoj situaciji softver privilegovanog računara omogućava indirektan pristup resursu ostalim računarima.

2. Prenos podataka i osnove komunikacija

Računarska mreža se može posmatrati kao komunikacioni sistem, gde se informacija generisana na predajnoj strani (izvorište poruke) dostavlja željenom odredištu. Osnovni elementi komunikacionog sistema su:

- Izvor (*source*) – generiše podatake za prenos.
- Predajnik (*transmitter*) – transformiše generisane podatke u oblik pogodan za prenos (npr. modem digitalne podatke iz PC računara transformiše u analogni signal koji se može preneti preko javne telefonske mreže - PSTN).
- Prenosni sistem (*tramission sistem*) – može biti jednostavna linija ili kompleksna mreža koja spaja izvor i odredište.
- Prijemnik (*receiver*) – prihvata signal iz prenosnog sistema i transformiše ga u oblik pogodan za odredište.
- Odredište (*destination*) – prihvata prenete podatke.



Slika 2.1 Model komunikacionog sistema

Ključni poslovi u komunikacionom sistemu su:

- Povezivanje (*interfacing*) uređaja na komunikacioni sistem;
- Generisanje signala (*signal generation*) – propagacija, regeneracija, domet itd.;
- Sinhronizacija (*synchronization*) predajnika i prijemnika;
- Razmena podataka (*exchange management*) prema odgovarajućem protokolu;
- Otkrivanje i ispravljanje grešaka (*error detection and correction*) npr. kod slanja datoteka;
- Kontrola toka (*flow control*) - usaglašavanje brzine slanja i brzine prijema podataka;
- Adresiranje i usmeravanje (*addressing and routing*) – čim postoji više od dva učesnika;
- Oporavak (*recovery*) – mogućnost da se transfer podataka nastavi od mesta prekida;

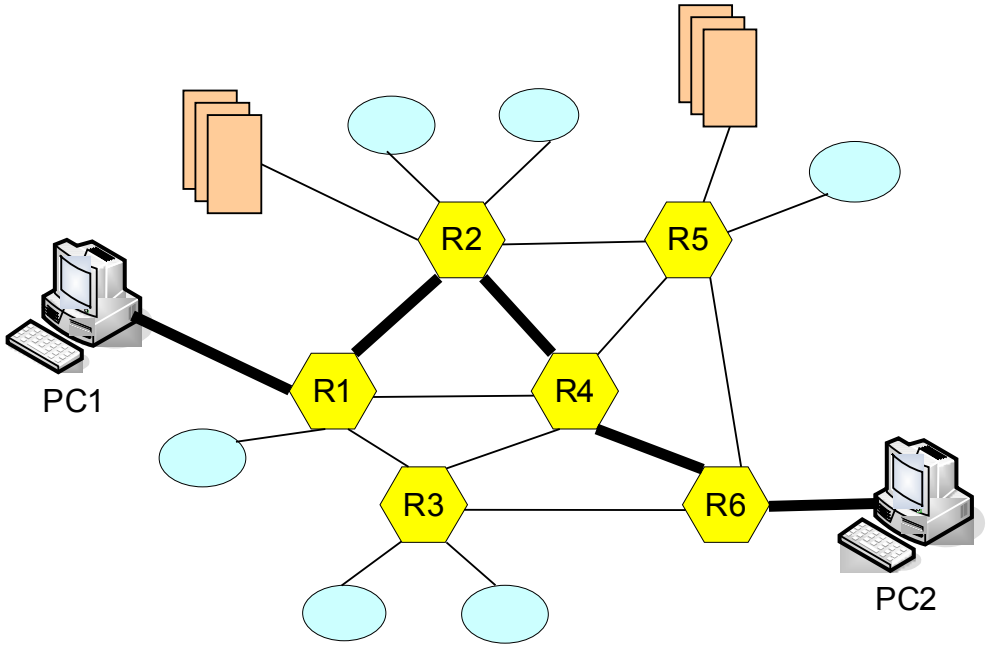
- Formatiranje podataka (*message formatting*) - dogovor učesnika o dužini i strukturi podataka koji se prenose;
- Zaštita (*security*) na prenosnom putu, autentičnost podataka;
- Upravljanje mrežom (*network management*) – mreža je kompleksan sistem, koji ne radi sam po sebi. Neophodno je mrežu konfigurisati, nadgledati (monitorisati), intervenisati i inteligentno planirati za buduću namenu.

2.1. Vrste prenosa podataka

U računarskim mrežama postoje dva osnovna načina prenosa podataka. Kod prvog načina, koji je stariji, veza između izvorišta poruke i odredišta uspostavlja se kroz čvorove mreže, na način da se zauzima kompletan spojni put. Karakterističan primer je javna telefonska komutirana mreža. Drugi tip je paketski način prenosa, gde se poruka deli u manje celine – pakete (okvire), a kroz mrežu se paketi mogu preusmeravati po različitim spojnim putevima. Ovakav način prenosa je karakterističan kod Interneta. Postoji i treći način prenosa podataka, a odnosi se na paketski prenos podataka gde svi paketi prolaze isti spojni put.

2.1.1. Prenos podataka sa komutacijom veza (*circuit switched*)

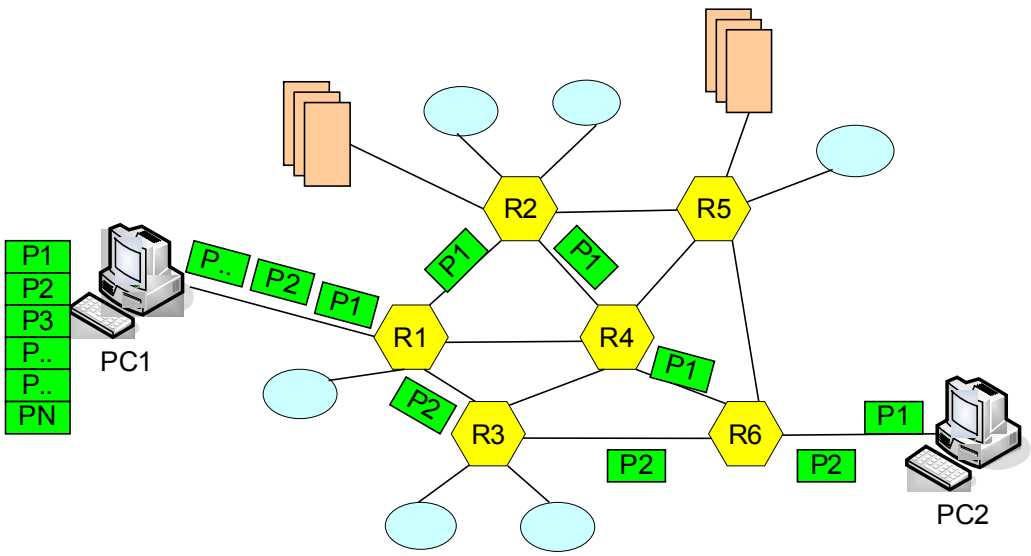
U ovom tipu prenosa podataka između dva učesnika u komunikaciji uspostavlja se čvrsta direktna veza, a ukupna informacija se prenosi putanjom koja je utvrđena u toku uspostave veze. Na primer, ako računar PC1 želi da komunicira sa računarom PC2 prvo se uspostavlja veza između ova dva računara i ta veza postoji samo za dati prenos podataka. Ako neki treći računar poželi da komunicira sa računarom PC2 u tom trenutku, to neće biti moguće po istom spojnom putu. Takođe, komunikacija bilo koja druga dva učesnika ne može da se odvija zauzetim spojnim putem. Osnovna karakteristika ovakvog načina prenosa podataka je da se podaci mogu prenositi uspostavljenom vezom maksimalnom brzinom koja je moguća, tj. u potpunosti se može koristiti kompletan frekvencijski opseg uspostavljenog spojnog puta (komunikacionog kanala) za prenos podataka.



Slika 2.2 Prenos podataka sa komutacijom veza

2.1.2. Prenos podataka sa komutacijom paketa (packett switched)

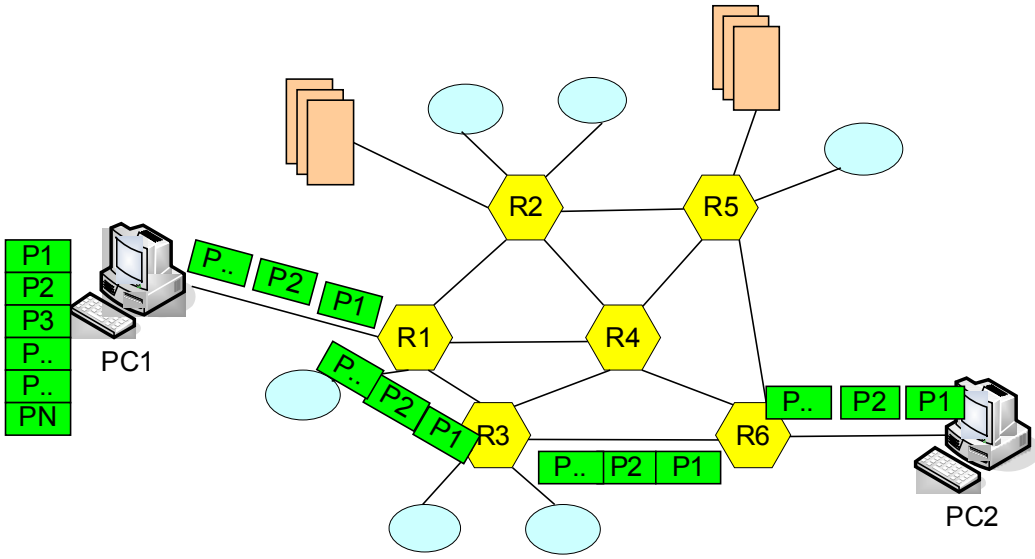
Kod ovog načina prenosa podataka između dva učesnika, prvo se informacija koja se razmenjuje deli u pakete čija struktura (dužina paketa, redni broj, adresa odredišta, prioritet i sl.) odgovara nosećim protokolima. Paketi se upućuju do prvog čvora u mreži (rutera), a u svakom ruteru se vrši nezavisno usmeravanje paketa. Izbor putanje u ruterima se vrši na osnovu više kriterijuma koji važe u datom trenutku. Paketi prolaze različite putanje od izvorišta do odredišta. Na odredištu se vrši slaganje paketa u prvobitan redosled da bi se dobila potpuna informacija. Ovakav način prenosa podataka je karakterističan za računarske mreže gde većinu mrežnog saobraćaja čine kratki naleti podataka sa praznim prostorom između i koji su obično vremenski duži od "popunjenih". Suština ovakvog načina prenosa podataka je da se u praznim prostorima mogu slati paketi koje šalje neki treći učesnik. Dakle, podaci od različitih izvorišta mogu prolaziti istim spojnim putem. Ovo je daleko žilaviji način prenosa, zato što paketi najčešće mogu da nađu bar jedan slobodan spojni put. Mana je što je efektivna brzina slanja podataka na ovaj način manja od maksimalne koju dozvoljava propusni opseg kanala, zato što ga koriste više učesnika u komunikaciji.



Slika 2.3 Prenos podataka sa komutacijom paketa

2.1.3. Prenos podataka virtuelnom vezom (*virtual circuit*)

Ovaj način prenosa podataka se takođe odnosi na paketski prenos. Međutim, paketi se usmeravaju na isti spojni put između dva računara. Virtuelna kola su permanentnog tipa što znači da kada se jednom definišu putanje, retko ili nikada se ne menjaju. Ovo je zapravo softverska zamena za hardverska rešenja ovog tipa. Podaci i dalje putuju kroz mrežu (povezani čvorovi) ali tačno određenom putanjom. Svaki paket, pored karakterističnih polja koje nosi, ima i obeležje koje ukazuje na datu virtuelnu vezu. Skoro sve mreže koje imaju intenzivan saobraćaj na mreži koriste ovu metodu definisanja putanje. Prednost ovakvog načina prenosa paketa je da se krajnjim aplikacijama može obezbediti odgovarajući kvalitet usluge. Na primer, kod interaktivnog prenosa govora kroz mrežu, važno je obezbediti da paketi podataka, kojima je kodovan govor, do prijemnika stižu istom brzinom, tj. da ne postoji varijacija u kašnjenju. U mrežama sa komutacijom paketa, pojedini paketi mogu da pronalaze drastično različite putanje (različito vreme prenosa), što može dovesti do problema na prijemu – nerazumljiv govor. Samo virtuelnim kolima se može obezbediti zahtevani kvalitet usluge. Zbog prenosa kroz mrežu postoji kašnjenje, ali je ono identično za sve pakete i za dati signal nije od interesa.

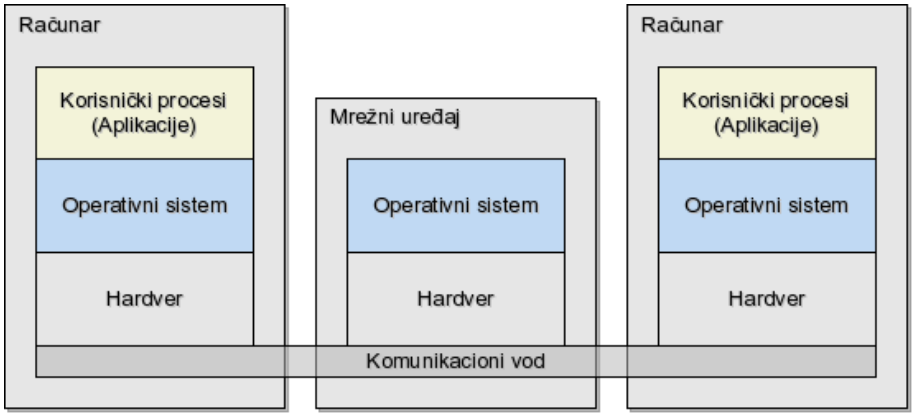


Slika 2.4 Prenos podataka virtuelnim kolima

3. Osnove umrežavanja, hardver i softver

Kao osnovne elemente računarske mrežne komunikacije možemo izdvojiti:

1. komunikacioni kanal (vod)
2. hardver računara
3. operativni sistem
4. korisničke procese (aplikacije)



Slika X - Elementi računarskih mreža

Kod direktne komunikacije dva računara na oba učesnika poseduju sve elemente osim u slučajevima kada se komunikacija inicira/završava na nivou operativnog sistema ili kada je u pitanju kontrolna komunikacija na nivou mrežnog hardvera. Međutim, kod kompleksnijih mreža komunikacija krajnjih čvorova može biti posredna i odvijati se preko jednostavnih mrežnih uređaja koji se sastoje od hardvera sa ugrađenim funkcijama i interfejsima ili preko kompleksnih mrežnih uređaja koji u sebi sadrže specijalizovani mrežni operativni sistem. Komunikacioni kanali i elementi koji ih povezuju sa mrežnim interfejsima računara/uređaja nazivaju se pasivnom mrežnom opremom. Mrežni uređaji koji u sebi sadrže i hardver/firmver/softver sposoban za analizu i modifikaciju nosećih signala nazivaju se aktivnom mrežnom opremom. Pravila po kojima se komunikacija vrši na svim pomenutim nivoima nazivaju se protokolima.

Za uspešnu komunikaciju između krajnjih članova mreže potrebno je obezbediti funkcionalnost na svim nivoima. U slučaju da računari/uređaji nemaju adekvatnu podršku za hardver ili protokole na kojima se bazira računarska mreža, komunikacija neće biti moguća.

3.1. Pasivna mrežna oprema

Pasivna mrežna oprema predstavlja najjednostavniju komponentu računarskih mreža. Atribut "pasivna" potiče od ciljne karakteristike komponenti ove kategorije da nad mrežnim saobraćajem ne izvrše nikakvu izmenu. Pasivne komponente mreže čine:

- utičnice
- kablovi
- paneli za prespajanje i za završavanje kablova (*patch panel*)
- kablovi za prespajanje (*patch cabel*)
- rek ormani
- kanalice za vođenje kabla
- ...

Za prenos signala između računara većina današnjih mreža koristi kablove koji se ponašaju kao mrežni prenosni medijumi. Postoji mnogo različitih tipova kablova koji mogu da se primene u različitim situacijama. Njihov broj je izuzetno veliki i obuhvata više od 2000 različitih tipova. Većina današnjih mreža koristi tri osnovne vrste kablova:

- koaksijalne kablove
- kablove sa upredenim paricama (*twistedpair*)
- optičke kablove

Kroz upredene parice i koaksijalni kabl prenose se električni signali, dok se kroz optička vlakna prenose signali u vidu svetlosnih impulsa. Za ispravan rad mreže potrebno je da se kablovski sistem (kablovi i priključni elementi) formira od komponenti koje zadovoljavaju određene tehničke standarde.

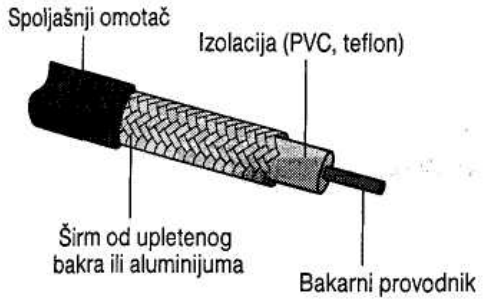
Kablovi koji se koriste u jednoj mreži zavise od više parametara:

- binarni protok
- pouzdanost kabla
- maksimalnu dužinu između čvorova
- zaštitu od električnih smetnji
- podužno slabljenje
- tolerancije u otežanim uslovima rada

- cenu i opštu raspoloživost kabla
- lako povezivanje i održavanje
- ...

3.1.1. Koaksijalni kabl

Koaksijalni kablovi su u jednom periodu bili najrasprostranjeniji mrežni medijum za prenos podataka, i to iz više razloga: relativno su jeftini, laki, fleksibilni i jednostavni za rad. U svom najjednostavnijem obliku, koaksijalni kabl se sastoji od bakarne žice u sredini, oko koje se nalazi najpre izolacija, a zatim sloj od upletenog metala (širm) i, na kraju, spoljašnji zaštitni omotač. Svrha ovog oklopa je da apsorbuje elektromagnetne smetnje ili šum, i time spreči njihovo mešanje sa podacima koji se prenose. Kablovi koji imaju jedan sloj izolacije i jedan sloj od upletenog metala zovu se i kablovi sa dvostrukom zaštitom. Postoje, takođe, i kablovi sa četvorostrukom zaštitom (dva sloja izolacije i dva sloja širma), koji se primenjuju u sredinama sa jakim elektromagnetnim smetnjama.



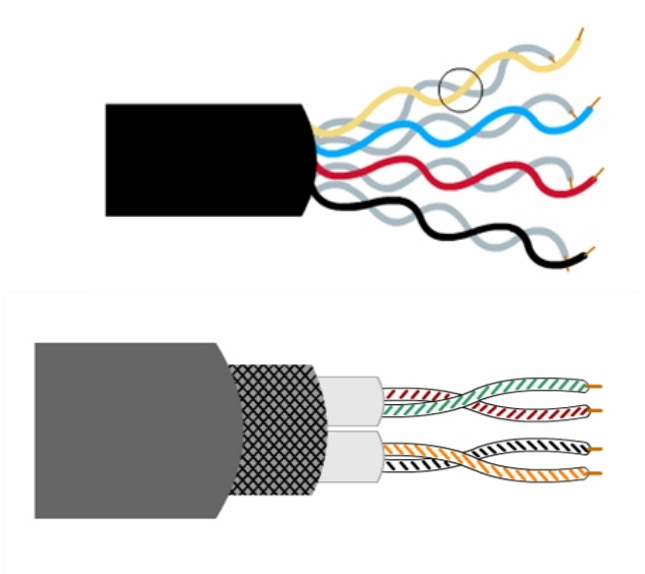
Slika 3.1 Slojevi koaksijalnog kabla

Bakarni provodnik (žica) u sredini kabla prenosi elektromagnetne signale koji predstavljaju kodirane računarske podatke. Ovaj provodnik može biti od punog metala, ili u obliku više upletenih žica. Ukoliko je od punog metala, onda je to obično bakar. Provodnik je obložen dielektričnim izolacionim slojem koji ga odvaja od širma. Širm ima ulogu uzemljenja i štiti provodnik od električnog šuma i preslušavanja.

3.1.2. Kabl sa upredenim paricama

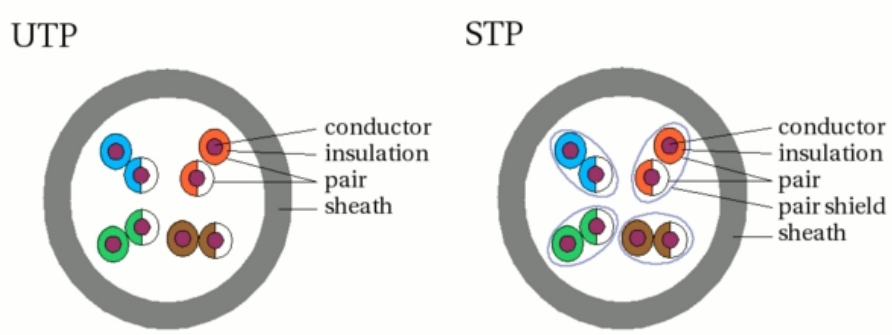
Kabl sa upredenim paricama (*twisted pair cable*) se sastoji od parova izolovanih bakarnih žica koje su obmotane (upredene) jedna oko druge. Upredanje se vrši u cilju otklanjanja elektromagnetnih smetnji. Broj uvrtaja po metru čini deo specifikacije tipa kabla jer što je broj uvrtaja po metru veći, veća je otpornost

kabla na elektromagnetne smetnje. Na slici 3.2 prikazana su dva tipa ovog kabla: kabl sa neoklopljenim (*Unshielded Twisted-Pair, UTP*) i oklopljenim (*Shielded Twisted-Pair, STP*) paricama.



Slika 3.2 Kablovi sa neoklopljenim i oklopljenim paricama

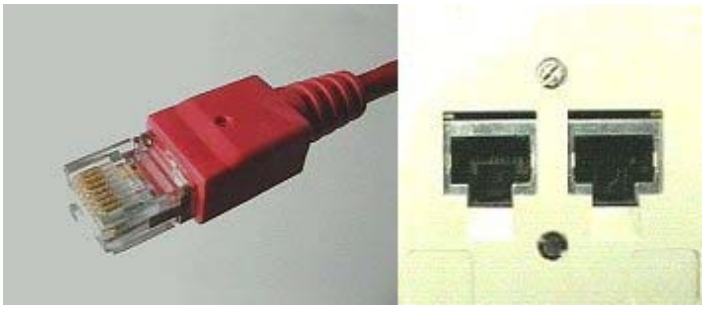
Grupe parica se obično nalaze u zaštitnom omotaču i zajedno sa njim čine kabl. Pravila strukturnog kabliranja, koje se danas skoro isključivo koristi za formiranje računarskih mreža, propisuju da se za povezivanje računara moraju koristiti četvoroparični kablovi. Upredanjem se poništava električni šum od susednih parica, ili ostalih izvora, kao što su motori, releji, transformatori i energetska instalacija. S obzirom da je problem elektromagnetne zaštite veoma ozbiljan, neki proizvođači (IBM, evropske firme) su razvili tzv. oklopljene kablove, koji oko parica imaju određenu električno provodnu strukturu koja pruža znatno veći nivo zaštite. U praksi postoje tri tipa oklopljenih kablova: FTP, S-FTP i STP.



Slika 3.3 Presek: Kablovi sa neoklopljenim i oklopljenim paricama

FTP kabl je napravljen tako da su četiri parice potpuno obavijene tankom metalnom folijom. Ova folija svoju zastitnu funkciju obavlja tako što zahvaljujući visokoj impedansi reflektuje spoljne, ometajuće, elektromagnetne signale na učestanostima većim od 5 MHz i tako im onemogućava prodor do samih parica. Po odnosu cena/performanse u praksi su se najbolje pokazali FTP kablovi, tako da se oni najčešće i koriste.

Bakarne žice kablova sa uvrnutim paricama se sa hardverskim mrežnim interfejsom računara (npr. mrežnom Ethernet karticom) ne povezuju zasebno i direktno već putem odgovarajućih konektora. Najčešće korišćeni tip konektora je RJ (*Registered Jack*) i on se, u više varijanti, koristi kod telefonskih i računarskih mreža.



Slika 3.4 Konektor RJ45 i utičnica

Najčešći RJ konektori su:

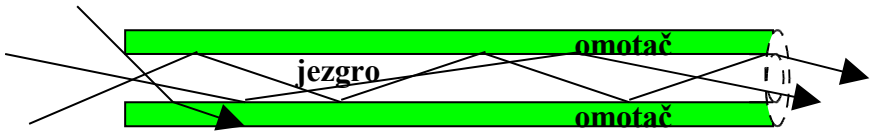
- RJ11 - jedna telefonska linija
- RJ14 - dve telefonske linije
- RJ12 i RJ25 - tri telefonske linije
- RJ45 – Ethernet računarska mreža

Kablovi sa upredenim paricama za povezivanje sa računarima koriste RJ-45 konektore.

Za povezivanje bakarnih žica sa konektorima koristi se poseban tip alata - tzv. klešta za krimpovanje. Ovaj alat najčešće ima mogućnost za rad sa RJ45 i RJ11 konektorima. Raspored žica pri povezivanju je određen standardima 568A i 568B. Ovi standardise koriste kod računarskih mreža (RJ45 konektori). 568A je predloženi standard. Kablovi koji kombinuju 568A i 568B standarde se koriste za direktno povezivanje dva računara.

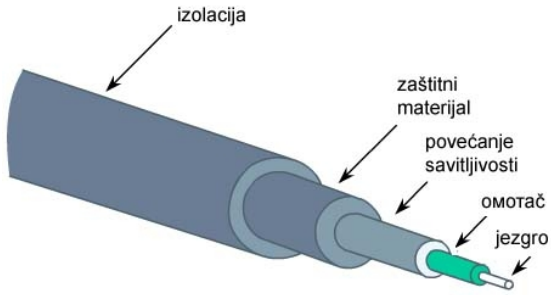
3.1.3. Optički kablovi

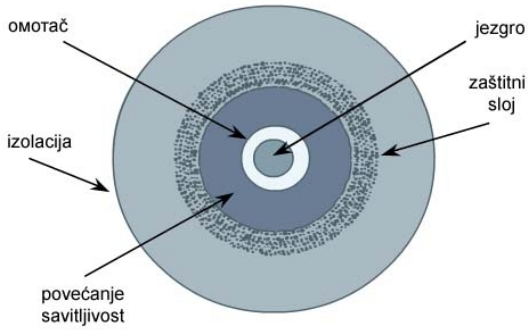
Kod ove vrste kablova, optička vlakna prenose digitalne signale u obliku modulisanih svetlosnih impulsa. Kablovi od optičkih vlakana ne podležu električnim smetnjama, imaju najmanje slabljenje signala duž kabla i podržavaju izuzetno velike brzine prenosa podataka na velikim udaljenostima. Koriste se i u slučajevima kada LAN mreža treba da poveže više objekata, gde se sa bakarnim kablovima mogu očekivati problemi sa uzemljenjem i atmosferskim pražnjenjima. Optičke veze osim velike brzine prenosa obezbeđuju i potrebno galvansko razdvajanje instalacija. Često se postavljaju u objektima, u slučajevima kada se predviđa veliki mrežni saobraćaj između spratnih razvoda u odnosu na centar mreže.



Slika 3.5 Totalna refleksija kod prenosa kroz optičko vlakno

Sistemi prenosa sa optičkim kablovima se sastoje iz tri osnovna funkcionalna dela, a to su predajnik (izvor svetlosti – LED ili laserska dioda), optičko vlakno i prijemnik (foto senzor). Standardni električni signal se dovodi na LED ili lasersku diodu koje vrše konverziju u svetlost, zatim se svetlost "ubacuje" u optičko vlakno na čijem drugom kraju je prijemnik koji vrši opto-električnu konverziju posle koje se dobija standardni električni signal. Princip po kome se informacija prenosi po optičkom vlaknu bazira se na fizičkom fenomenu pod nazivom totalna refleksija. Svako optičko vlakno se sastoji iz jezgra koga čini staklo određenog indeksa prelamanja i omotača presvučenog preko jezgra. Ovaj omotač je takođe od stakla, ali ono ima drugu vrednost indeksa prelamanja. Svetlost se ubacuje u jezgro pod određenim uglom potrebnim da dođe do totalne refleksije, zbog koje se svetlosni zrak neprestalno odbija od granične površine jezgro/omotač putujući tako kroz vlakno do prijemnika.





Slika 3.6 Kabl sa optičkim vlaknom

Optička vlakna se mogu podeliti u dve osnovne grupe: na monomodna (*singlemode*) koja su tanja i omogućavaju prostiranje samo jednog svetlosnog zraka, i multimodna (*multimode*) koja su deblja i omogućavaju istovremeno prostiranje više zraka od više različitih izvora. U tehnološkom procesu je mnogo jednostavnije (a time i jeftinije) proizvesti vlakno većeg prečnika jezgra. To je razlog zbog kog se multimodna vlakna češće koriste. Pored toga, u veće jezgro je mnogo lakše "ubaciti" svetlost iz izvora, pa su i predajnici jeftiniji jer svetlosni snop izvora ne mora biti toliko fokusiran kao u slučaju korišćenja monomodnog vlakna. Dakle, celokupni sistem baziran na multimodnom vlaknu je jeftiniji i takvi sistemi su danas dominantni kod lokalnih računarskih mreža. Sa druge strane, zbog većih rastojanja koja je potrebno premostiti, u telekomunikacijama su dominantna monomodna vlakna. Kod računarskih mreža svaki link (veza) zahteva dva vlakna – jedan za predaju a drugi za prijem.

3.1.4. Kablovi i elektromagnetno zračenje

Elektromagnetno zračenje se nalazi svuda oko nas i praktično je nemoguće naći sredinu u kojoj ga nema pošto izvore predstavljaju radio i TV predajnici, mobilni telefoni, računari, rashladni uređaji i sl. Do nedavno je samo upredanje parica (UTP) predstavljalo dovoljnu zaštitu. Naime, propusni opsezi koje su zahtevale aplikacije u prošlosti su bili daleko ispod 30 MHz, što je gornja granica zaštite upredanjem. Današnje aplikacije koriste propusne opsege reda veličine 100 MHz, što ako se u obzir uzme i činjenica da difuzne radio stanice emituju u opsegu od 88 do 108 MHz, povlači zaključak da je pored upredanja potreban još jedan nivo zaštite. Ovaj nivo zaštite pružaju FTP i STP kablovi. Kod FTP kablova se koristi aluminijumska folija debljine 25 mikrona koja je obmotana oko uporednih parica i koja usled površinskog efekta odvodi indukovano elektromagnetno zračenje na masu. Na ovaj način, današnji kablovi su zaštićeni do 600 MHz. STP kablovi su još otporniji na elektromagnetno zračenje, ali su znatno skuplji. Za potpunu zaštitu od elektromagnetnog zračenja, najpouzdanije ali i najskuplje rešenje

predstavljaju optički kablovi.

3.1.5. Strukturno kabliranje

Za formiranje LAN mreže potrebno je obezbediti niz tehničkih preduslova. Svaki projekat LAN mreže započinje detaljnim snimanjem lokacije sa ciljem da se prikupe potrebni podaci, kao što su postojeće stanje instalacija, građevinske osnove objekta, kao i detalji energetskog uzemljenja. Dalji postupci se sastoje od preliminarnog određivanja horizontalnih i vertikalnih kablovskih trasa i razmeštaja razvodnih ormana.

Savremene računarske mreže se u najvećem broju slučaja realizuju po principu strukturiranog kabliranja, kojim treba da se obezbedi i objedini prenos svih informacija u jednom poslovnom sistemu. Osim kvalitetnog prenosa podataka, ovim sistemom se može obavljati i prenos telefonskih, video, upravljačkih i alarmnih signala. Suštinsku prednost strukturnog kabliranja predstavlja korišćenje jedinstvenog kablovskog sistema za sve instalacije kojima se prenose bilo kakve informacije u propusnom opsegu do 600 MHz. Jedini interfejs ka korisniku je zidna utičnica sa RJ 45 konektorima na koju se može priključiti bilo računar, bilo telefon (ili oba) i koja dalje kablovskim sistemom vodi do odgovarajućih razdelnika i aktivnih uređaja (telefonske centrale ili svičeva). Struktura mreže je takva da se posle instaliranja, bez ikakve intervencije na samim kablovima cela mreža može prekonfigurisati na potpuno drugačiji način, u zavisnosti od potrebe korisnika. To se postiže na samim razdelnicima, koji su posebno konstruisani za lako i jednostavno prespajanje i konfigurisanje mreže po želji. Ova opcija naročito dolazi do izražaja u situacijama kada se vrši menjanje fizičkog rasporeda radnih mesta po zgradi. Odgovorni administrator vrši prespajanje na odgovarajućim razdelnicima i sve što korisnik na novom radnom mestu treba da uradi jeste da priključi svoj telefon i računar u zidnu utičnicu i da radi. Njegov računar je povezan na isti način u računarsku mrežu, njegov telefon je na istom lokalu kao i ranije. Osim velike fleksibilnosti koju pruža, strukturno kabliranje zahvaljujući svojoj sistematičnosti, omogućava jednostavno i efikasno administriranje mrežom, lako proširivanje instalacije i što je možda i najvažnije, potpuno je nezavisno od tipa aktivnih uređaja koji se koriste kako za telefonsku, tako i za računarsku mrežu. Čak se i uređaji koji ne odgovaraju standardima strukturnog kabliranja i nemaju adekvatne konektore mogu uz pomoć odgovarajućih jednostavnih adaptera priključiti na sistem.

Sistem strukturiranog kabliranja se sastoji od horizontalnih i vertikalnih kablovskih trasa. Razvodni orman pokriva deo horizontalne površine, poštujući tehničko ograničenje trase od najviše 90m dužine, tako da se zavisno od arhitekture objekta, postavlja jedan ili više razvodnih ormana po spratnoj osnovi, u kojima se koncentrišu kablovske trase i smešta odgovarajuća aktivna mrežna

oprema. Vertikalne trase povezuju spratne razvodne ormane. I horizontalne i vertikalne kablovske trase se izvode u formi zvezde, da bi se obezbedilo da u slučaju prekida pojedine trase ostatak sistema radi. Ovaj sistem se osim horizontalnih trasa odnosi i na vertikalne, tako da se i sve vertikalne trase završavaju u jednom centralnom razvodnom ormanu, a kablovska struktura ima oblik složene zvezde, kojoj je početak u centralnom razvodnom ormanu, a kraj u priključnoj kutiji u okviru radnog mesta.

Sistemi strukturnog kabliranja se realizuju na tri hijerarhijska nivoa:

1. Kabliranje kampusa (kabliranje između više bliskih poslovnih zgrada);
2. Kabliranje kičme (vertikalno kabliranje);
3. Horizontalno kabliranje (kabliranje spratova).

Kabliranje kampusa se odnosi na kabliranje između razdelnika pojedinih zgrada (BD) i razdelnika kampusa (CD). Za prenos govora, alarmnih i upravljačkih signala se koriste bakarni parični kablovi, kategorije 5, 5E i 6. Za prenos video signala i podataka koriste se optički kablovi. Maksimalna dužina kablova iznosi 1500m.

Vertikalno kabliranje (okosnica, kičma zgrade) vrši povezivanje spratnih razdelnika (FD) i razdelnika zgrade (BD). U vertikalnom razvodu u zavisnosti od aplikacije razdvojeni su kablovski sistemi.

Horizontalno kabliranje se odnosi na deo kablovskog sistema između spratnog razdelnika (FD) i zidne utičnice (TO). Između razdelnika i zidne utičnice razvlači se ili bakarni parični kabl (kategorije 5, 5E, 6) ili optički kabl. Za bakarne kablove, i razdelnik i zidna utičnica koriste RJ 45 konektore, dok se za optičke kablove koriste ST konektori. Maksimalna dužina kablova između spratnog razdelnika i zidnih utičnica ne sme da pređe 90m.

Horizontalno kabliranje obuhvata najveći broj kablova u celom kablovskom sistemu za sve primenljiv. Horizontali kablovski sistem, ukoliko je dobro dimenzionisan može se, za sve primene, koristiti u dužem vremenskom periodu.

3.2. Aktivna mrežna oprema

3.2.1. Ripiter (*Repeater*)

Ripiteri su jednostavni uređaji sa dva porta, koji rade na fizičkom nivou. Pojednostavljeno rečeno, na jednom portu (priključku) ripiter prima signal i prenosi na drugi port. Pritom ripiteri imaju tzv. *3R* funkcionalnost:

- *Reamply*
- *Reshape*
- *Retim*e

tj. obnavljaju amplitudu, oblik i vremenske reference primljenog signala pre nego što ga proslede. Ripiter nema informacija o signalu koji pojačava, što znači da se podjednako odnosi i prema ispravnom i prema neispravnom signalu. Radi na prvom sloju OSI modela.

Dobra strana ripitera je u tome što predstavlja jeftin način za povećanje maksimalnih rastojanja u mreži. Međutim, mana mu je što može da počne emitovanje dok je emitivanje paketa sa neke stanice u toku, što dovodi do sudara. Zbog toga je dobro da oba porta ripitera imaju po jednu diodu za indikaciju emitovanja i diodu za indikaciju problema.

3.2.2. Hab (*Hub*)

Hab je mrežni uređaj koji takođe funkcioniše na prvom OSI sloju (fizičkom sloju). Na habu postoji više konektora (obično su to RJ-45 konektori). Na svaki konektor se priključuje po jedan kabl, preko kojeg se povezuje po jedna radna stanica ili server. Omogućava povezivanje više segmenata mreže u jedan segment. Hab funkcioniše slično kao ripiter: ono što primi na jednom svom portu hab emituje na svim ostalim portovima. Može se posmatrati kao višeportni ripiter. U Ethernet mrežama sa UTP i optičkim kablovima hab je čvor koji povezuje stanice i servere. Svaki uređaj povezan na Hub deli isti *Broadcast* domen i *Collision* domen. Zbog toga, samo jedan od računara povezanih na Hub može u jednom trenutku da vrši transmisiju podataka. Može se koristiti kao centralna tačka u topologiji zvezde. Habovi uglavnom sadrže između 6 i 24 porta i mogu se postavljati i uklanjati u zavisnosti od potreba i u skladu sa razvojem mreže. Najčešće se koriste pri konfigurisanju mreža. Habovi često imaju još jedan dodatni port koji se naziva *uplink* port. On služi za međusobno povezivanje dva haba. Povezivanje se vrši tako što se spaja uplink port jednog haba sa običnim portom drugog haba.

Slika 3.9 Različite veličine habova

Hab kao uređaj polako nestaje iz računarskih mreža zbog sve niže cene svič uređaja koji nude znatno bolje performanse.

3.2.3. Mrežni most (*Bridge*)

To je uređaj koji povezuje udaljene mrežne segmente. Radi u drugom sloju OSI modela, tj. u sloju veze podataka. Do sada smo videli da u datom trenutku na mreži može da emituje samo jedna stanica. Ostale stanice osluškuju saobraćaj i kada zaključe da je medijum slobodan šalju svoje pakete. Može se zaključiti da bi bilo veoma zgodno logički podeliti mrežu na segmente koji se sastoje iz stanica koje međusobno najviše komuniciraju. To bi značilo da po dve stanice u različitim segmentima mogu da komuniciraju istovremeno. Ako stanica iz jednog segmenta šalje podatke stanici u drugom segmentu, tada ostalim stanicama nije dozvoljeno da komuniciraju.

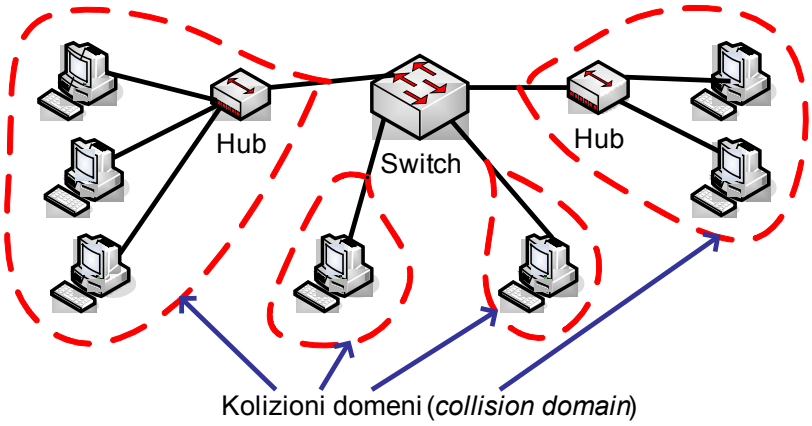
Segmentaciju mreže možemo izvršiti uređajem koji se zove mrežni most. Spolja je sličan ripiteru, a funkciono ima sve njegove osobine uz dodatak nekoliko novih koje su veoma značajne. Most proverava sadržaj zaglavlja primljenog paketa da bi saznao MAC (fizičku) adresu izvora i odredišta. Na osnovu toga, on formira tabelu MAC adresa za svaki port. Pojedini segmenti mreže se nazivaju kolizioni domeni. Kada dobije broadcast paket (paket za sve računare u mreži), mrežni most ga samo prosleđuje i ne pamti MAC adresu iz njegovog zaglavlja.

Postoji pravilo u segmentiranju mreže po kome 80% saobraćaja treba da se odvija u okviru kolizionih domena, a 20% da ide preko mosta. To znači da ukoliko neke dve stanice često međusobno komuniciraju (npr. neka radna stanica i određeni server), ne treba stavljati most između njih. Mrežni most unosi određeno kašnjenje kao posledicu obrade paketa, ali se ono uglavnom ne oseća.

3.2.4. Svič (*Switch*) – skretnica

Svič je za mrežni most isto što je i hab za ripiter. Dakle, na sebi ima veći broj portova. To je uređaj koji prosleđuje podatke od jednog mrežnog segmenta do drugog putem određene linije. Svaki port, kao i kod mosta, ima izvestan stepen inteligencije, odnosno ne vrši samo retransmisiju paketa, već upisuje MAC adrese u odgovarajuću tabelu. Za razliku od hub uređaja, svitč podatke ne šalje svim segmentima mreže već samo segmentu kome su oni upućeni. Ovo se postiže

tako što svitč pravi namenske veze između segmenata. Veoma značajna mogućnost koju svič poseduje je da se na svaki port sviča može priključiti stanica, a ne segment mreže. Kolizioni domen u ovom slučaju čini stanica sa odgovarajućim portom. Sobraćaj koji vidi stanica je samo onaj koji je direktno upućen za nju, kao i broadcast poruke.



Slika 3.10 Svič omogućava podelu LAN-a na više kolizionih domena

Problem koji se javlja kod upotrebe sviča je preopterećenje. Brzina kojom paketi pristižu na svič je regulisana upotrebom neke od ARQ tehnika između dolaznog porta i uređaja koji na svič šalje pakete. Međutim, može se desiti da je većina dolaznog saobraćaja upućena na neki od portova koji treba da ih prosledi dalje i koji to nije u stanju da uradi jer kapacitet odlazne veze to ne može da podrži. Paketi koji pristižu mogu da se baferuju do izvesne granice, posle koje se odbacuju. Svičevi se bolje ili lošije nose sa ovim problemom u zavisnosti od njihovog kvaliteta (veličine bafera - memorija i brzina obrade).

Kao što smo videli, mreža ne mora sadržati samo svičeve ili samo habove, već je treba balansirati u zavisnosti od potreba i budžeta. Na primer, veoma je čest slučaj u praksi da se na jedan port sviča poveže hab, a na taj hab više stanica.

3.2.5. Usmerivač (*Router*)

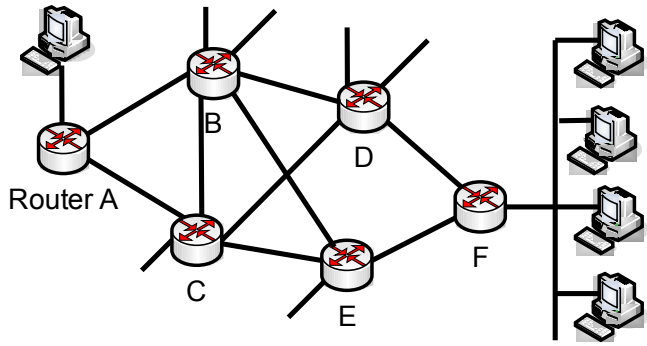
Za razliku od mrežnih uređaja koje smo do sada videli i koji rade na prvom i drugom OSI nivou, ruteri rade na trećem nivou, odnosno mrežnom sloju. Glavna uloga rutera u mreži je da rutiraju (usmeravaju) pakete kako bi oni stigli do svog odredišta. Informacija koja se koristi za ovu funkciju je odredišna adresa smeštena u paketu. Ruter obavlja ovu funkciju tako što po prispeću paketa izvuče odredišnu adresu, zatim nađe odgovarajući zapis u tabeli rutiranja gde su smešteni podaci na koji port treba paket da se prosledi i odredi adresu sledećeg

rutera na putu ka kojem se paket usmerava. Ovaj proces se naziva „*address lookup*“. Kada se dobije ova informacija vrši se proces komutacije (*switching*) gde se paket komutira sa ulaza na odgovarajući izlazni port odakle se šalje dalje.

Pored ovih osnovnih funkcija ruteri vrše i druge funkcije kao npr. provera ispravnosti paketa, obrada kontrolnih paketa itd. Najnoviji trendovi su da ruteri treba da obavljaju i dodatne funkcije kao npr. „*security*“ protokoli, kvalitet servisa i sl. koji nameću dodatne zahteve ruterima. Takođe, broj korisnika računarskih mreža je u stalnom porastu tako da je saobraćaj koji generišu korisnici sve veći. Saobraćaj se takođe uvećava usled novih aplikacija koje zahtevaju veoma velike propusne opsege (npr. prenos video materijala u realnom vremenu). Da bi se zadovoljili zahtevi za povećanim saobraćajnim koriste se linkovi sve većeg kapaciteta (do nekoliko desetina gigabita po sekundi) sa tendencijom da se ti protoci podignu na terabitske brzine. To znači da obrada paketa mora biti veoma brza i efikasna jer ruter pri takvim kapacitetima linkova mora da procesira milione paketa u sekundi i da ih prosleđuje na odgovarajuće izlazne portove. Postoji više algoritama (algoritmi rutiranja) koji treba ovaj proces da načine što efikasnijim.

Tabela rutiranja za ruter A

Odredište	Sledeći skok
A	.....
B	B
C	C
D	B
E	C
F	E



Slika 3.11 Ruteri usmeravaju pakete na osnovu tabele rutiranja

Ruter se konfiguriše i održava svoje tabele rutiranja na osnovu mrežnih adresa. Kada primi paket, ruter prvo proveri da li je adresa odredišta na istoj mreži kao i adresa izvora. Ako jeste, paket se odbacuje. U suprotnom, ruter prosleđuje paket odredišnom uređaju ako je njegova mreža povezana na ruter ili sledećem ruteru na putanji do željenog uređaja. Ruta se sastoji od tri elementa: destinacija, sledeći uređaj na putanji i rastojanje, odnosno cena ukupne rute do odredišta (koje se još naziva i metrika). U nekim protokolima metrika predstavlja samo broj linkova na putanji do odredišta, na nekim vreme u sekundama i/ili ostale parametre.

Svaki protokol rutiranja koristi različiti algoritam za utvrđivanje kada su dostupne nove rute i koja je ruta najbolja na osnovu metrike. Prosleđivanje

paketa do mreža sa kojima ruter nije u direktnoj vezi može da se vrši na dva načina:

- **Statičke putanje** - Reč je o putanjama koje administrator određuje statički. U slučaju da se topologija mreže izmeni (usled kvarova, novih zahteva i sl.) administrator mora da izmeni putanje u skladu sa novom situacijom.
- **Dinamičke putanje** - Ove putanje ruter automatski saznaje nakon što administrator konfiguriše protokol rutiranja. Za razliku od statičkih putanja, čim mrežni administrator uključi dinamičko rutiranje, informacije o rutiranju se samim procesom rutiranja automatski ažuriraju svaki put kada se od nekog rutera u okviru mreže primi informacija o novoj topologiji.

3.2.6. Mrežni prolaz (*gateway*)

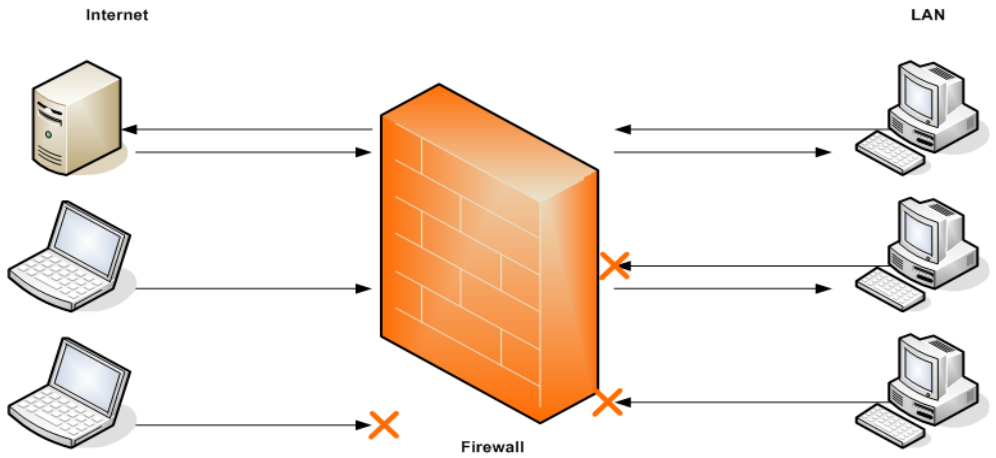
Mrežni prolaz je hardverski uređaj i/ili softverski paket koji povezuje dva različita mrežna okruženja. Omogućava komunikaciju između različitih arhitektura i okruženja. Vrši prepakivanje i pretvaranje podataka koji se razmenjuju između potpuno drugačijih mreža, tako da svaka od njih može razumeti podatke iz one druge. Mrežni prolaz je obično namenski računar, koji mora biti sposoban da podrži oba okruženja koja povezuje kao i proces prevođenja podataka iz jednog okruženja u format drugog. Svakom od povezanih mrežnih okruženja mrežni prolaz izgleda kao čvor u tom okruženju. Zahteva značajne količina RAM memorije za čuvanje i obradu podataka. Radi u sloju sesije i aplikativnom sloju. Kako povezuje različite mreže, mrežni prolaz menja format poruka da bi ih prilagodio krajnjim aplikacijama kojima su namenjene, vrši prevođenje podataka (iz ASCII u EBCDIC kod, na primer) kompresiju ili ekspanziju, šifrovanje ili dešifrovanje, i drugo.

Dakle, osnovna namena mrežnih prolaza je konverzija protokola. Radi između transportnog i aplikativnog sloja OSI modela. Danas u svetu postoji veliki broj autonomnih mreža, svaka sa svojim različitim hardverom i softverom. Autonomne mreže međusobno se mogu razlikovati po više karakteristika: algoritmima za rutiranje, implementiranim protokolima, procedurama za administriranje i vođenje politike mreže i dr. No nezavisno od nabrojanih razlika, korisnici jedne mreže imaju potrebu da komuniciraju sa korisnicima povezanim na drugu mrežu.

3.2.7. Bezbednosna barijera (*firewall*)

Firewall je bezbednosni hardverski ili softverski uređaj, najčešće smešten između lokalne mreže i javne mreže (Interneta), čija je namena da štiti podatke u mreži

od neautoriziranih korisnika (blokiranjem i zabranom pristupa po pravilima koje definiše usvojena bezbednosna politika). Služi za sprečavanje komunikacije zabranjene određenom mrežnom polisom. Vrlo često ne moraju svi korisnici u LAN-u da imaju jednaka prava pristupa mreži. Postavljanjem *firewall* uređaja između dva ili više mrežnih segmenata mogu se kontrolisati i prava pristupa pojedinih korisnika pojedinim delovima mreže.



Slika 3.12 Princip rada *firewall*-a

Firewall može biti softverski ili hardverski. Osnovna prednost hardverskih firewall-a je brzina rada i realizacija na specijalizovanom namenskom operativnom sistemu što ga čini neranjivijim na tom nivou. Osnovna prednost softverskog *firewall*-a je proširivost. Proširivost u ovom slučaju predstavlja mogućnost proširenja skupa parametra paketa koji se mogu uzeti u obzir pre donošenja odluke šta će se sa paketom uraditi. Osnova rada *firewall*-a je u ispitivanju IP paketa koji putuju između klijenta i servera, čime se ostvaruje kontrola toka informacija za svaki servis po IP adresi i portu u oba smera.

Odgovoran je za više važnih stvari u okviru jednog informacionog sistema:

- implementira bezbednosnu politiku
- beleži sumnjive događaje
- upozorava administratora na pokušaje napada i pokušaje kompromitovanja bezbednosne politike
- u nekim slučajevima obezbeđuje statistiku korišćenja

Samo posedovanje *firewall*-a (hardverskog ili softverskog) ne znači da je

računar/mreža koju on štiti bezbedan. Naprotiv, *firewall* predstavlja samo alat koji je moguće iskoristiti za zaštitu ukoliko je dobro podešen (ukoliko su dobro definisana bezbednosna pravila). Najbolji način da se *firewall* podesi (ukoliko administrator nema iskustva u toj oblasti) je da se blokira sav saobraćaj a da zatim za svaku konekciju posebno donese odluku da li je treba dopustiti, trajno ili privremeno, i za koje klijente.

3.2.8. Proxy

Uređaj tj. mrežni servis koji omogućava klijentima da prave indirektne mreže sa ostalim mrežnim segmentima/servisima. Uloga indirektnih pristupa može imati značajnu ulogu kada je u pitanju bezbednost, privatnos i/ili performanse mreže. Bezbednosni aspekt proksi uređaja ga najčešće izjednačuje sa naprednijim firewall uređajima. Aspekt vezan za performanse mreže se odnosi na mogućnost proksi uređaja da udaljeni resurs (kome je već ostvaren pristup) privremeno sačuva u lokalnoj memoriji i na taj način na ostale zahteve za istim resursom odgovori bez pristupa originalnom izvoru. Ovaj proces se naziva "keširanje". Mana ovakvog pristupa jeste mogućnost nesinhronizovanosti resursa skladištenog na proksi uređaju i u međuvremenu izmenjenog resursa na originalnom izvoru.

Kod nekih servisa (npr. e-mail, video-konferencije i sl.) nije moguće iskoristiti proksi uređaj za povećanje performansi mreže i takvi pokušaju mogu imati katastrofalne posledice u bezbednosnom pogledu. Proksi uređaji su se uglavnom koristili kod pristupa HTML resursima ali i u toj oblasti sve više izlaze iz upotrebe usled sve većih kapaciteta komunikacionih kanala i personalizacije Web sadržaja.

Privatnost, kao treći mogući razlog korišćenja proksi uređaja, predstavlja mogućnost klijenata da sve zahteve (ili samo zahteve vezane za određeni sajt, grupu resursa i sl.) ostalim računarima u mreži uputi putem proksi uređaja i na taj onemogući tačno utvrđivanje izvora zahteva. Proksi uređaji koji omogućavaju ovakav rad su česti na Internetu ali sve više izlaze iz upotrebe usled zakonskih propisa koji zabranjuju mogućnost anonimnosti, pre svega zbog kriminala i napada na regularne resurse.

3.3. Interfejsi računara

3.3.1. Mrežna kartica

Mrežna kartica je uređaj koji povezuje računar sa računarskom mrežom. Često se naziva: mrežni adapter, mrežni interfejs, NIC... Jedan od važnijih elemenata svake mrežne kartice je MAC adresa koja čini da ovaj uređaj radi na 2. sloju OSI modela. MAC adresa predstavlja 48-bitni seriski broj koje IEEE (*Institute of Electrical and Electronics Engineers*) dodeljuje proizvođaču.

Mrežne kartice su se ranije najčešće u računarima mogle naći u vidu zasebnih kartica dok se danas uglavnom integrišu u matične ploče računara. U jednom računaru se može naći i više mrežnih kartica, bilo na matičnoj ploči, bilo u vidu zasebnih kartica.

Mrežne kartice uglavnom imaju RJ-45 (UTP), BNC i/ili AUI (*Attachment Unit Interface*) konektore. Takođe, na mrežnim karticama se uglavnom nalaze i LED diode koje služe za praćenje aktivnosti kartice. Najčešće brzine na kojima rade mrežne kartice su 10/100/1000 Mbit/s. Glavni proizvođači mrežnih kartica su 3Com, Intel, Realtek, Marvell, VIA...

3.3.2. Modem

Modem je uređaj koji moduliše noseći signal da bi enkodirao digitalnu informaciju i demoduliše noseći signal da bi dekodirao prenešenu informaciju. Najčešće se koriste za pristup Internetu putem telefonskih linija - POTS (*Post Office Telephone Service*).

Kod PC računara se mogu naći kao interni (povezuju se na ISA ili PCI slot) ili eksterni (povezuju se na serijski port). Winmodemi ili Softmodemi su vrsta modema sa osiromašenim hardverom čiju ulogu zamenjuje centralni procesor putem drajvera za određeni OS (najčešće MS Windows). Najčešća maksimalna brzina prenosa je 56.000 bita/s (7KB/s).

3.3.3. ISDN Terminal Adapter

ISDN Terminal Adapter je uređaj koji povezuje terminal (npr. računar) sa ISDN mrežom. Pošto obavlja istu funkciju kao

modem kod POTS mreža, često se naziva i ISDN modem. Ovaj naziv je pogrešan jer kod ISDN (*Integrated Services Digital Network*) mreže nije potrebna modulacija/demodulacija

Postoje uređaji koji kombinuju funkcionalnost ISDN TA i funkcionalnost klasičnih modema sa interfejsom ka ISDN liniji. Takođe, postoje i uređaji koji imaju mogućnost povezivanja i sa ISDN mrežom i sa Ethernet mrežom. Ovakvi uređaji najčešće poseduju i mogućnost rutiranja.

Sa stanovišta OSI modela ISDN linije rade na sledeća tri sloja:

1. fizičkom sloju
2. sloju podataka
3. mrežnom sloju

3.3.4. ADSL/DSL modem

ADSL/DSL modem je uređaj koji povezuje jedan ili više računara na telefonsku liniju u cilju korišćenja ADSL (DSL) usluge. ADSL modemi koji omogućavaju ADSL uslugu za više od jednog računara nazivaju se i ADSL ruteri.

ADSL/DSL modemi rade na ADSL/DSL komunikacionoj tehnologiji koja omogućava daleko brži prenos podataka putem telefonske linije nego što je to slučaj sa standardnim modemima. Brzina prenosa podataka kod ADSL tehnologije je asimetrična tj. ADSL omogućava veću brzinu primanja podataka od slanja. Dolazna brzina prenosa se kreće od 256 kbit/s do 8 Mbit/s u okviru od 1500 metara. Odlazna brzina prenosa se kreće od 64 kbit/s do 1024 kbit/s. ADSL koristi dva opsega frekvencija - opseg od 25,875 kHz do 138 kHz se koristi za slanje podataka dok se opseg od 138 kHz do 1104 kHz koristi za prijem podataka. S obzirom da PSTN (*Public Switched Telephone Network*) radi na opsegu od 0 do 4kHz, korišćenjem ADSL tehnologije je putem jedne telefonske linije moguće u isto vreme slati i primati podatke i obavljati telefonske pozive.

3.4. Protokoli

Prenos podataka kroz mrežu se obavlja po protokolima – utvrđenim pravilima koja su poznata svim učesnicima u komuniciranju. Protokol predstavlja standard (konvenciju) za ostvarivanje i kontrolu veze i prenosa podataka između dve krajnje tačke. Komunikacioni protokol predstavlja set standardizovanih pravila za predstavljanje podataka, signalizaciju, proveru autentičnosti i kontrolu grešaka, neophodnih da bi se informacija prenela komunikacionim kanalom. Ključni elementi protokola kojim se dogovara spremnost za slanje, spremnost za prijem, format podataka i sl. su:

- sintaksa - format podataka i nivoi signala,
- semantika – kontrolne informacije u prenosu i kontrola grešaka,
- tajming – brzina prenosa.

Razmena podataka u računarskoj mreži je izuzetno složena. Sa povećanjem broja umreženih računara koji komuniciraju i sa povećanjem zahteva za sve savršenijim uslugama (servisima) neophodno je i usavršavanje protokola. Posao komuniciranja je toliko složen da je bilo neophodno razviti protokole u više slojeva. Svaki sloj je namenjen za jedan odgovarajući posao. Kod prvobitnih računarskih mreža, umrežavanje se vršilo zavisno od proizvođača računarske opreme. Sav hardver i softver su bili vezani za jednog proizvođača, tako da je bilo veoma teško vršiti izmene, unapređivanja mreže i sve je bilo izuzetno skupo. Uvođenjem standarda za komuniciranje po logički jasno definisanim slojevima, pojavilo se više proizvođača softverske opreme. Standardima se omogućilo kombinovanje hardvera i softvera od različitih proizvođača, što je sve zajedno dovelo do pada cena opreme i softvera za umrežavanje i do povećanja kvaliteta usluga u mrežama.

Jedna od najbitnijih stvari kod umrežavanja je adresiranje. Ako se posmatraju samo dva računara, nema potrebe za adresiranjem, jer sve što se pošalje sa jednog računara namenjeno je drugom. Već kada mrežu čine tri računara, pojavljuje se potreba za adresiranjem. Poslati podaci sa jednog računara mogu biti namenjeni jednom od preosta dva računara. Dodatno usložnjavanje nastaje ako se posmatra više aplikacija na jednom računaru, koje mogu da komuniciraju sa više aplikacija na drugom računaru. Ovde nije dovoljno samo adresirati računar, već i aplikaciju sa kojom se komunicira.

Koraci protokola moraju da se sprovedu u skladu sa redosledom koji je isti za svaki računar u mreži. U predajnom računaru ovi koraci se izvršavaju od vrha ka dnu. U prijemnom računaru ovi koraci moraju da se sprovedu u obrnutom redosledu.

Na predajnom računaru protokol:

- deli podatke u manje celine, nazvane paketi, koje može da obrađuje,
- paketima dodaje adresne informacije tako da odredišni računar na mreži može da odluči da li oni pripadaju njemu,
- priprema podatke za prenos kroz mrežnu karticu i dalje kroz mrežni kabl.

Na prijemnom računaru, protokoli sprovode isti niz koraka, ali obrnutim redosledom:

- preuzimaju se podaci sa kabla
- kroz mrežnu karticu unose se paketi podataka u računar.
- iz paketa podataka uklanjaju se sve informacije o prenosu koje je dodao predajni računar.
- kopiraju se podaci iz paketa u prihvatnu memoriju (bafer) koja služi za ponovno sklapanje.
- ponovno sklopljeni podaci prosleđuju se aplikaciji u obliku koji ona može da koristi.

Osnovni principi u dizajnu protokola su efikasnost, pouzdanost i robustnost i prilagodljivost. Potrebno je da oba računara, predajni i prijemni, svaki korak izvedu na isti način kako bi primljeni podaci imali istu strukturu kakvu su imali pre slanja. U mreži, više protokola mora da radi zajedno. Njihov zajednički rad obezbeđuje ispravnu pripremu podataka, prenos do željenog odredišta, prijem i izvršavanje. Rad više protokola mora da bude usaglašen kako se ne bi događali konflikti ili nekompletne operacije, odnosno nekompletan prenos informacija. Rezultat tog usaglašavanje naziva se slojevitost (*layering*).

Uspostavljanje veze, prenos podataka i raskid veze određeni su setom protokola koji su nadležni za jedan od sledećih poslova:

- "Handshaking" - uspostavljanje veze;
- Pregovaranje o različitim karakteristikama veze;
- Definicija početka i kraja poruke;
- Definicija formata poruke.
- Definisanje pravila za obradu oštećenih ili nepravilno formatiranih poruka (ispravka grešaka);

- Utvrđivanje neočekivanog prekida veze i definisanje daljih koraka u tom slučaju;
- Prekid veze.

3.4.1. Protokoli bez uspostavljanja veze

Pri korišćenju protokola bez uspostavljanja veze inicijalni korak pri prenosu podataka jeste samo slanje podataka. Ovom koraku ne prethodi procedura vezana za uspostavljanje veze kao što je to slučaj kod protokola sa uspostavljanjem veze. Iako je uspostavljanje veze najčešće osobina protokola sa pouzdanim prenosom, postoje protokoli koji omogućavaju pouzdan prenos bez uspostavljanja veze kao i protokoli koji ne garantuju bezbedan prenos iako koriste uspostavljanje veze.

3.4.2. Protokoli sa uspotavljanjem veze

Pri korišćenju protokola sa uspostavljanjem veze dve strane moraju da uspostave vezu između sebe kao preduslov za razmenu podataka. Proces uspostavljanja veze može se porediti sa pozivanjem telefonskog broja:

1. Strana koja poziva inicijalizuje liniju (podizanjem slušalice) i unosi odredišni broj.
2. Nakon poziva broja uspostavlja se veza koja još uvek nije adekvatna za prenos podataka i čeka se na primaoca poziva da podigne slušalicu.
3. Nakon podizanja slušalice primalac poziva obaveštava pozivaoca da je spreman za razmenu podataka signalom "halo".
4. Nakon primanja signala "halo" veza adekvatna za prenos podataka je uspostavljena i razmena može da počne.

Jasno je da procedura potrebna za uspostavljanje veze zahteva određeno vreme i angažovanje obe strane. Međutim, ona obezbeđuje pouzdaniji (ali ne i potpuno pozdan) prenos podataka i umanjuje mogućnost greške. Uspostavljanje veze se praktikuje kod protokola koji imaju za cilj da osiguraju pouzdan prenos podataka. Primer protokola koji radi sa uspostavljanjem veze je TCP (*Transmission Control Protocol*). Protokoli servisa kod kojih su performanse bitnije od pouzdanog prenosa podataka najčešće ne uključuju uspostavljanje veze.

3.5. Standardizacija i organizacije

Osnovni razlog za postavljanje standarda jeste omogućavanje korišćenja komponenti različitih proizvođača i njihove međusobne kompatibilnosti u kompleksnim sistemima (kakav je npr. računarska mreža). Standardizacija omogućava proizvođačima oslanjanje svog proizvoda na proizvode drugih proizvođača a korisnicima daje slobobodu time što ih ne ograničava na proizvode samo jednog proizvođača. Na ovaj način standardi pozitivno utiču na razvoj tržišta i cene proizvoda.

Standardi se mogu podeliti na formalne standarde i *de facto* standarde. Formalne standarde razvija i propisuje zvanično ovlašćeno industrijsko ili vladino telo. Proces razvijanja formalnog standarda se sastoji od tri faze:

1. specifikacija
2. prepoznavanje opcija
3. prihvatanje standarda

U fazi specifikacije se razvija nomenklatura i identifikuju problemi. U fazi prepoznavanja opcija se za identifikovane probleme nalaze moguća rešenja i odabiraju se optimalna. U fazi prihvatanja standarda se definiše celokupno rešenje i standard se promoviše kod industrijskih lidera u oblasti za koju je standard nadležan. Treća faza jasno ukazuje na to da čak i na formalne standarde veliki uticaj mogu imati velike industrijske korporacije ili vladina tela.

De facto standardi su standardi koji se pojavljuju na tržištu, podržani su od strane jednog ili više proizvođača ali nisu zvanično potvrđeni od strane organizacija nadležnih za standardizaciju. Ovakvi standardi mogu postati formalni u slučajevima kada postanu široko prihvaćeni na tržištu.

3.4.1 Organizacije za standardizaciju

Vodeće organizacije za standardizaciju su:

- *International Organization for Standardization* (ISO)
- *International Telecommunications Union - Telecommunications Group* (ITU)
- *Institute of Electrical and Electronics Engineers* (IEEE)
- *Internet Engineering Task Force* (IETF)
- *American Nationas Standards Institute* (ANSI).

*International Organization for Stan*dardization (ISO) predstavlja jedno od najvažnijih svetskih tela za standardizaciju. Sedište ove organizacije je u Ženevi a članice organizacije su sedišta u zemljama članicama. ISO organizacija je član ITU-a. ISO i ITU uglavnom sarađuju na standardima vezanim za telekomunikacije. Adresa Web sajta ISO organizacije je www.iso.ch.

International Telecommunications Union - Telecommunications Group (ITU) predstavlja telo za standardizaciju čiji je fokus rada usmeren na telefoniju, telegraf i prenos podataka. Članstvo ove organizacije su do 1993. godine uglavnom činile javne telefonske kompanije preko 200 zemalja sveta. 1993. godine je izvršena reorganizacija tako da sada članstvo čine i organizacije privatnog sektora (npr. AT&T). Sedište ove organizacije je takođe u Ženevi a adresa Web sajta www.itu.int.

Institute of Electrical and Electronics Engineers (IEEE) organizacija predstavlja profesionalno udruženje u čijem sklopu postoji i odeljenje za standarde (Standards Association, IEEE-SA). Najpoznatiji standardi ove organizacije su usmereni ka LAN mrežama. Sedište organizacije je u SAD a Web sajt se nalazi na adresi standards.ieee.org.

Internet Engineering Task Force (IETF) je telo za standardizaciju čiji je fokus rada usmeren ka razvoju Internet mreže. Specifičnost ove organizacije je u tome što nema zvanično članstvo što znači da svi zaintesovani pojedinci i organizacije mogu imati pristup mejling-listama, prisustvovati sastancima ili davati sopstvene predloge u razvoju standarda. Web sajt IETF-a se nalazi na adresi www.ietf.org.

American Nationas Standards Institute (ANSI) je američka nacionalna organizacija za standardizaciju. Sastoji se od oko 1000 članova koje čine organizacije iz državnoj i privatnog sektora. Fokus rada ove organizacije jeste razvoj nacionalnih standarda uz očuvanje kompatibilnosti sa ISO standardima. ANSI organizacija je članica ISO i ITU organizacija.

4. Tipovi mreža (kategorizacija)

Današnje računarske mreže su u stadijumu razvoja u kome ne postoji samo jedan tip mreža ili samo jedno pravilo po kome se one realizuju i koriste. Prepoznavanje računarskih mreža kao komunikacione infrastrukture jedinstvenih mogućnosti uslovilo je različita tehnička rešenja da bi se one omogućile i u najrazličitijim uslovima. Takođe, evolucijom potreba čovečanstva koje se baziraju na računarskim mrežama, i njihova svrha i primena su počele da obuhvataju različite domene ljudskog interesovanja.

Podelu računarskim mreža je moguće vršiti po više kriterijuma. U skladu sa medijumom koji se koristi za prenos podataka računarske mreže mogu biti:

1. kablirane mreže
2. bežične mreže

Po topologije računarske mreže mogu biti:

1. Bus network
2. Star network
3. Ring network
4. Mesh network
3. Star-bus network

Po vremenskoj postojanosti računarske mreže mogu biti:

1. fiksne
2. privremene

Po protstoru na kome se prostiru računarske mreže mogu biti:

1. Personal Area Network (PAN)
2. Local Area Network (LAN)
3. Metropolitan Area Network (MAN)
4. Wide Area Network (WAN)
5. Global Network (Internet)

Po arhitekturi (funkcionalnom odnosu članova) računarske mreže mogu biti:

1. Host-based
2. Klijent-server

3. Peer-to-peer

Po specifičnoj funkciji koju obavljaju računarske mreže mogu biti:

1. Storage area network
2. Server farm network
3. Process control network
4. Value added network
5. SOHO network
6. Wireless community network
7. XML appliance network

Treba imati u vidu da su računarske mreže jedna dinamična oblast u kojoj su česte promene tako da je svaki pokušaj striktne kategorizacije osuđen na kratkotrajnu tačnost.

4.1. Mediji i načini prenosa podataka

4.1.1. Kablirane mreže

Osnovna karakteristika kabliranih mreža jeste postojanje fizičkog kanala (u obliku kabla) za prenos podataka. Glavna prednost kabliranih mreža jeste izolovanost medija za prenos podataka što znači da je on otporniji na spoljne uticaje i greške koje se usled njih javljaju. Mana kabliranih mreža jeste potreba da se između članova mreže koji se povezuju obezbedi putanja i na toj putanji postavi kabl što zahteva i vremenske i finansijske resurse. Tendencija kod kabliranih računarskih mreža jeste iskorišćenje već postojećih kabliranih infrastruktura (telefonija, kablovska televizija, mreža za distribuciju električne energije i sl.) zarad smanjenja pomenutih troškova. Postoje i situacije u kojima nije moguće povezivanje kablovima (brodovi i podmornice, avioni, vozila, sateliti...) te se u tim situacijama koristi bežični prenos podataka.

Kablirane mreže najčešće koriste električne impulse kao noseći signal podataka. Mana ovakvih impulsa je slabljenje u skladu sa rastojanjem i podložnost uticaju elektromanetnog zračenja. Ovi nedostaci zahtevaju dodatak uređaja za pojačavanje signala i zaštitne slojeve kablova. Drugi tip kabliranih mreža koji je znatno otporniji na pomenute nedostatke jesu optičke mreže. Ove mreže koriste optičke kablove kod kojih je glavni nosilac podataka svetlosni signal. Optičkim mrežama je moguće ostvariti znatno veća rastojanja i brzine prenosa podataka. Mana optičkih mreža je manja fleksibilnost kablova i visoka cena.

4.1.1.1. Javna telefonska mreža

Telefonija se često naziva i javna telefonska komutirana mreža (*Public Switched Telephone Network*, PSTN). Ova mreža je projektovana davno sa osnovnim ciljem da se uspešno prenese govorni signal. Karakteristika komutacione mreže je da se u fazi uspostave veze bira jedan od mogućih puteva prenosa, a za vreme održavanja veze informacija se prenosi uspostavljenim fizičkim putem. Sasvim je moguće, da se za dve uzastopne uspostave veze sa istih lokacija izabere potpuno različit fizički put prenosa informacije. Često se kaže da su ovo primeri čvrste direktne veze. Telefonija je od izuzetnog interesa za WAN mreže zato što je široko rasprostranjena. Što se tiče prenosa podataka, sistem telefonije nudi više načina prenosa informacija od izvorišta ka odredištu. To su komutirane veze, zakupljene linije i razne tehnologije sa paketskom komutacijom.

Da bi se ovom mrežom mogli prenositi podaci, potrebno je na oba kraja veze postaviti modeme, uređaje koji vrše modulaciju i demodulaciju digitalnog signala iz računara. Signali u računaru su digitalni, a telefonske linije su analogne tako da modem na izlazu vrši konverziju digitalnog signala u analogni, a na ulazu u

računar prevodi analogni signal u digitalni. Pošto je telefonska mreža konstruisana za prenos govora, njen propusni opseg je mali - do 3.4 kHz što dovodi do toga da su brzine prenosa podataka kilobitskog, a ne megabitskog reda veličine. Analogna transmisija i primena modemske tehnologije dostiže maksimalnu brzinu od 56 kbit/s pomoću savremenih modulacionih tehnika (TCM - *Trellis Coded Modulatiori*), kao i tehnika kompresije. Što je protok veći, veći je i uticaj šuma. Osim toga, šum se javlja i pri D/A i A/D konverziji. Takođe, brzine prenosa čak i pri uslovima bliskim idealnim ne postižu maksimalne nominovane vrednosti. Na primer, modem od 56 kbit/s pri najboljim uslovima može postići brzinu između 45 i 50 kbit/s (i to ako je centrala digitalna).

Imajući u vidu ove prednosti i nedostatke, dial-up analogna veza nalazi primenu u povezivanju kućnog računara sa Internetom, kućnog računara sa LAN mrežom na poslu, kao i backup veza u WAN mreži kada servis preko kojeg je WAN mreža primarno realizovana otkaže.

Ova tehnologija omogućava prenos digitalnih podataka preko postojećih telefonskih linija i zbog toga je vrlo brzo postala prihvatljivo rešenje za kućne korisnike i mala preduzeća, koji žele relativno brzu vezu sa Internetom, a nemaju dovoljno sredstava za neku drugu tehnologiju. Da bi se izvršilo spajanje na određnu mrežu, korisnik je odgovoran za deo opreme i instalacije koji se nalazi u njegovim prostorijama, dok je za instalacije van korisnikovih prostorija odgovorna telefonska kompanija.

Računarski modemi mogu biti interni i eksterni:

- Interni modem se postavlja u slot na matičnoj ploči računara i na poleđini ima utičnicu RJ-11 (četvorožični telefonski priključak) pomoću koje se modem, odnosno računar, priključuje na standardnu telefonsku utičnicu na zidu.

- Eksterni modem je zaseban uređaj sa zasebnim napajanjem. Sa računarom je povezan serijskim kablom (RS-232) ili putem USB magistrale. Eksterni modemi imaju utičnicu RJ-11 za povezivanje na liniju i signalne diode koje označavaju razne režime rada i stanja modema. Eksterni modemi imaju jednu prednost nad internim - mogu se resetovati nezavisno od računara, mogu se isključiti i ponovo uključiti, a da se pri tome ne mora isključivati ili resetovati računar.

4.1.1.2. Iznajmljene linije

Iznajmljene linije su telekomunikacione (analogne ili digitalne) veze koje međusobno spajaju dve udaljene lokacije. Nasuprot tradicionalnim telefonskim vezama, nepotreban je telefonski broj učesnika, zato što je svaka strana u

komunikaciji u stalnoj vezi sa drugom stranom. Koriste se za telefoniju, prenos podataka i Internet servise. Preko iznajmljenih linija ostavruju se brzine od 56 k, 64k, 128k, 256k, 512k ili 2Mb/s. Plaćaju se paušalno - na određeni vremenski period, bez obzira na stepen korišćenja. Dakle, to su veze tipa tačka-tačka gde se ne može se menjati destinacija kao kod *dial-up* veze. Najčešće služe za povezivanje udaljenih geografskih lokacija,i to na dva načina:

- Iznajmljena linija se prostire celom dužinom između dve lokacije,
- Iznajmljena linija ide do lokalnog telekom operatera, a veza od njega je realizovana nekom drugom tehnologijom, kao štoje na primer frame relay. Krajnjem korisniku se garantuje kvalitet usluge.

4.1.1.3. X.25

X.25 je ITU-T standard, protokol za WAN mreže koji koristi javnu telefonsku mrežu ili ISDN kao hardversku osnovu. Njime se definiše standardni fizički sloj, sloj veze podataka i mrežni sloj (slojevi 1 do 3) OSI modela. Protokoli X.25 mreže su razvijani u vreme dosta nepouzdanijih prenosnih linkova nego što je to slučaj danas. Razvojem komunikacione tehnike, višestruki mehanizmi za detekciju i korekciju grešaka koji su implementirani na drugom i trećem nivou protokol steka X.25 mreže, postali su nepotreban teret obrade paketa u čvorovima mreže. Novije tehnologije, kao što su brza paketska komutacija poznata pod nazivom frame relay, iskoristile su manje verovatnoće pojave grešaka modernih WAN linkova, za brži i jednostavniji prenos podataka. Takve tehnologije se oslanjaju na sposobnosti viših nivoa protokola (obično transportnih protokola) da vrše detekciju i korekciju eventualno nastalih grešaka.

Pored svojih dobrih karakteristika X.25 je ipak zastarela tehnologija. Kašnjenja koja su uzrokovana nepotrebno velikim procesiranjem u svakom čvoru mreže su primetna, naročito u slučaju višestruke razmene kratkih poruka sa kraja na kraj mreže. Međutim, i dalje postoje brojne aplikacije, pre svega prenos podataka vezan za finansijske transakcije, kojima odgovaraju, kako relativno mali protoci, tako i visoka pouzdanost i veliko iskustvo koje se godinama formiralo u održavanju i upravljanju X.25 mreža širom sveta. Danas se X.25 mreže koriste u velikom broju primena uglavnom od strane kompanija i institucija i to najčešće za:

1. Preuzimanje podataka iznacionalnih i međunarodnih baza podataka
2. Saobraćaj od terminala ka serverima (*Transactions Processing*)
3. Prenos fajlova
4. Elektronska pošta

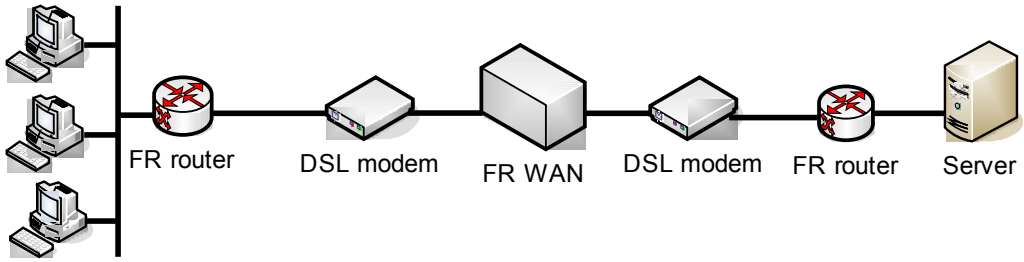
5. Bankomati (ATM - *Automatic Teller Machines*), itd.

Primenjivost X.25 mreže je ograničena protokom korisničkog pristupa, koji je tradicionalno za X.25 protokol ograničen na maksimalnih 64 kbit/s, do eventualno 2 Mbit/s kod nekih novijih varijanti X.25 mreža. Protoci ovog reda veličine danas su nedovoljni npr. za povezivanje LAN mreža. Frame relay i ATM predstavljaju u ovom smislu adekvatne naslednike X.25 protokola.

4.1.1.4. Frame relay

Zastarela X.25 mreža je sredinom osamdesetih godina u potpunosti zamenjena *frame relay* mrežama. Osnovna karakteristika ovakvih mreža je da rade sa uspostavljanjem direktne veze, a u njima ne postoji kontrola grešaka niti upravljanje tokom podataka. Paketi se na strani predajnika isporučuju u strogom redosledu. Njegova najvažnija primena je u povezivanju LAN mreža koje su lokacijski udaljene.

Bez obzira kako je rešena infrastruktura na lokaciji, povezivanje se sprovodi na isti način. Sa svake strane veze treba da bude obezbeđen od strane korisnika FR-a ruter koji se sa jedne strane priključuje na infrastrukturu (direktno na radnu stanicu, server, preko swich-a na LAN...) a sa druge strane se priključuje na DSL modem. Od DSL modema vodi veza prema tekomunikacionom operateru.



Slika 4.1 Osnovna šema Frame Relay veze

4.1.1.5. ATM

Asinhroni transportni mod ATM (*Asynchronous Transfer Mode*) je mrežni standard za prenos podataka na velikim brzinama. ATM prenosi informacije korišćenjem kratkih paketa fiksne dužine koji se nazivaju ćelije. Ćelije omogućavaju prenos svih oblika informacija - od govora do podataka - preko bilo kojeg komunikacionog medijuma - optičkih vlakana, bakarnih parica, kabla. Koristi se u telefonskim sistemima za interni prenos podataka, a često za prenos IP paketa.

4.1.2. Bežične mreže

Osnovna karakteristika bežičnih mreža jeste rad bez korišćenja komunikacionih kanala u vidu kablova. Bežične mreže za prenos podataka koriste radio talase ili svetlosne signale s tim da su radio talasi daleko češće u upotrebi jer za njihovo korišćenje nije potrebna optička vidljivost. Jedan od glavnih kriterijuma za kategorizaciju bežičnih mreža jeste razdaljina na kojoj je razmena podataka putem njih moguća. U skladu sa tim, bežične mrežese mogu podeliti na:

Bežične mreže kratkog dometa:

- Bluetooth

Bežične mreže srednjeg dometa:

- IEEE 802.1

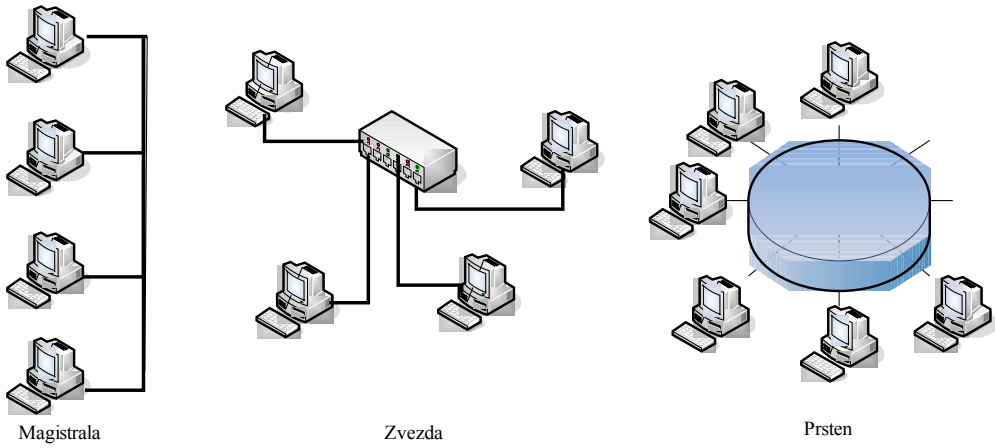
Bežične mreže velikog dometa:

- Satelitske mreže
- Mobilna telefonija
- Paging mreže

Kod računarskih mreža je najčešće korišćena IEEE 802.1 tehnologija (koja je i inače namenski razvijana za računarske mreže) ali se za veća rastojanja koriste i mreže mobilne telefonije kao i satelitske mreže.

4.2. Topologije

Postoje tri osnovne LAN topologije: magistrala (*bus*), prsten (*ring*) i zvezda (*star*). Ove topologije predstavljaju logičku arhitekturu mreže, ali fizički, uređaji ne moraju da budu stvarno raspoređeni u ovom obliku. Bus i ring logičke topologije su često fizički organozovane kao star topologija odnosno u obliku zvezde. Izbor i specifikacija topologije LAN mreže zavisi od: fizičkih lokacija na kojima se nalaze korisnici sistema, količine podataka u lokalnim bazama podataka kao i potrebnog ažuriranja tih baza, od učestanosti pristupa bazama na drugim lokacijama i zahteva za komuniciranjem između dve korisničke lokacije.



Slika 4.2 Osnovne topologije mreža

Topologija zvezde je linearna LAN arhitektura, kod koje se prenos podataka obavlja celom dužinim fizičkog mediuma kojim se prenose podaci i podaci se prenose svim radnim stanicama. Prednosti topologije magistrale: lako je dodati novi mrežni uređaj ovoj topologiji, zahteva daleko manje kabla nego ostale topologije. Mane: cela mreža može biti u prekidu ako negde postoji prekid na glavnom kablu i teško je otkriti problem kod mreže.

Ring topologija ili topologija prstena predstavlja način na koji su uređaji međusobno logički povezani. Ovakva vrsta mreže se sastoji od više uređaja povezanih jedan sa drugim tako da se obrazuje zatvorena kružna putanja. IBM mreže Token Ring/IEEE 802.5 i FDDI koriste implementaciju ring topologije.

Star topologija ili topologija zvezde predstavlja takav oblik arhitekture gde su krajnji čvorovi na mreži povezani preko posebne veze na centralni hub ili svič. Logičke bus ili ring topologije su često fizički implementirane kao star topologije. Prednosti ove topologije: lako se instalira i povezuje; nema prekida u mreži pri dodavanju novog uređaja ili uklanjanja; lako je otkriti greške i zameniti

delove i sl. Mane ove topologije: podložna je zagušenjima sobraćaja, zahteva više kabla nego linearna topologija; ako se hub ili switch pokvari svi čvorovi su ugašeni; mnogo skuplja topologija od npr. bus topologije.

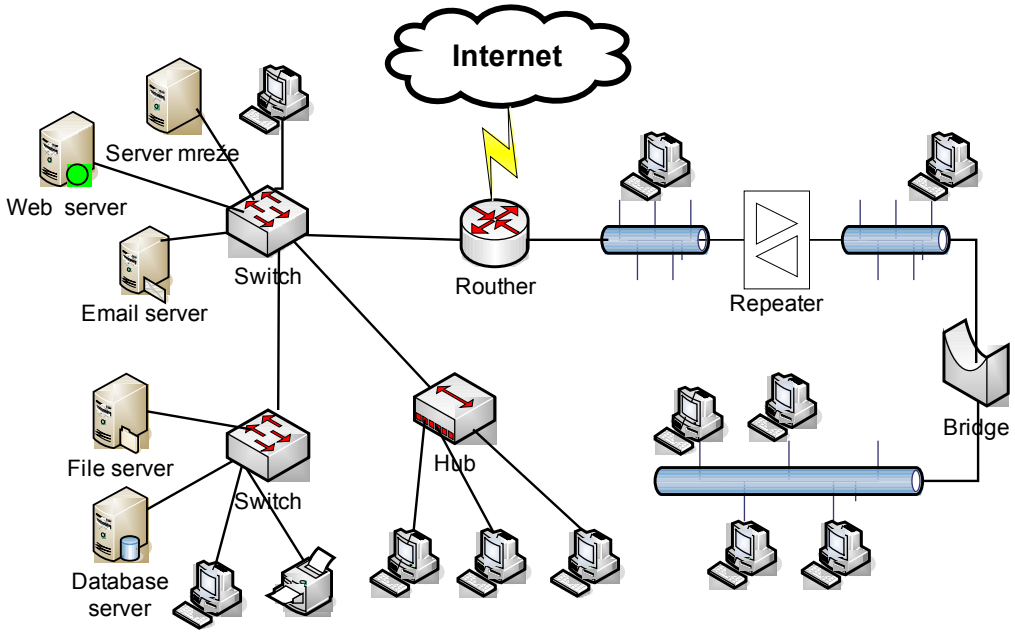
4.3. Veličina

Prema prostoru koji obuhvataju, računarske mreže se mogu podeliti na

- lokalne (LAN)
- regionalne računarske mreže (WAN) – mreže šireg područja

4.3.1. Lokalna računarska mreža (*Local Area Network*, LAN)

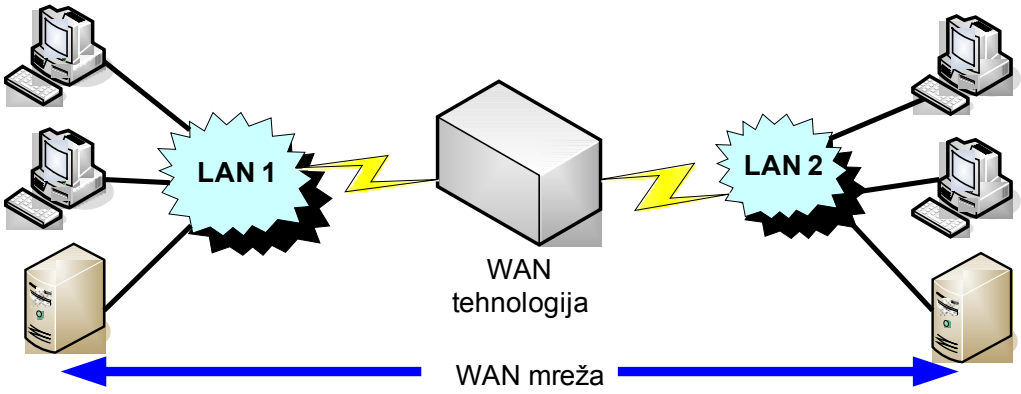
Predstavlja osnovni tip mreže. Ona može biti jednostavna kada imamo dva računara povezana kablom, ili složena kada su povezane stotine računara i periferijskih uređaja u jednoj velikoj organizaciji. Osnovno obeležje lokalne računarske mreže je to što je ona prostorno ograničena.



Slika 4.3 Lokalna računarska mreža(LAN) sa vezom ka Internetu

4.3.2. Regionalna računarska mreža (*Wide Area Network*, WAN)

Za razliku od LAN mreže WAN mreža nije prostorno ograničena. Ona može da poveže računare i uređaje širom sveta. Regionalnu računarsku mrežu čini veliki broj povezanih lokalnih mreža. Za povezivanje se koriste usluge telekomunikacionih operatera. Neke od tehnologija za povezivanje LAN-ova su: E1(T1), E3(T3), ATM, ISDN, ADSL, prespajanje okvira (*Frame Relay*), radio veze i slično. Ove mreže se nazivaju i okosnice ili kičma-mreže (*backbone*).



Slika 4.4 Regionalna računarska mreža (WAN)

4.4. Funkcionalni odnos članova (arhitektura aplikacija)

Funkcionalni odnos članova nije u direktnoj vezi sa fizičkom organizacijom i topologijom računara već se ovaj odnos određuje na osnovu arhitekture aplikativnog sloja. U skladu sa tim, mogu se izdvojiti tri osnovne arhitekture aplikacija:

- Host-based arhitektura
- Klijent-server
- Peer-to-peer

4.4.1. Host-based mreže

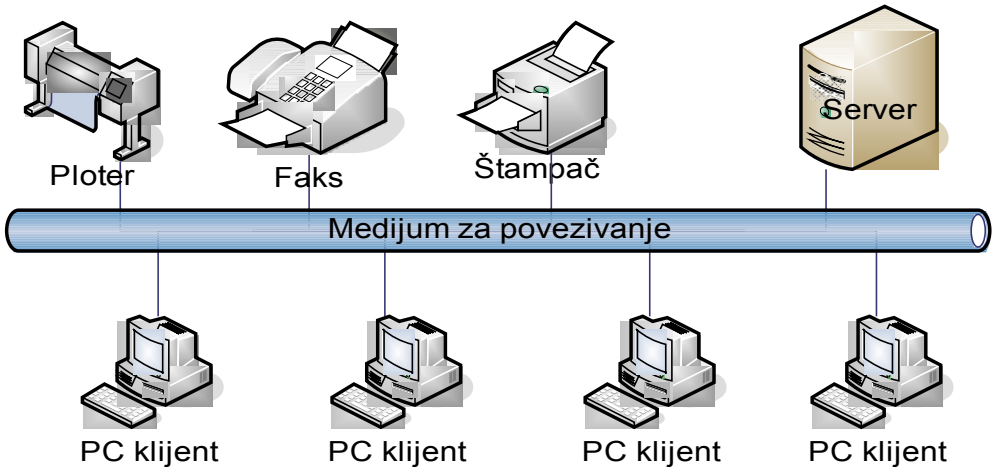
Host-based mreže su zasnovane na jednoj od najstarijih mrežnih arhitektura. Kod mreža ovog tipa u centru mreže se nalazi jak *mainframe* računar na koga su povezani terminali. Razlika između *mainframe* i terminal članova je u tome što *mainframe* računar obavlja sva izračunavanja dok terminali služe samo kao interfejs sa korisnicima. Host-based arhitektura svoju popularnost u ranim fazama razvoja računara i računarskih mreža duguje visokoj ceni procesorske moći koju je bilo neekonomično pridruživati korisničkim računarima, terminalima.

Danas se mreže sa host-based arhitekturom retko sreću u svom izvornom obliku. Razlog zbog koga je host-based arhitektura danas u upotrebi nije velika razlika u ceni između terminala i centralnih servera već je u pitanju smanjenje troškova kroz centralizovanu administraciju.

4.4.2. Klijent-server mreže

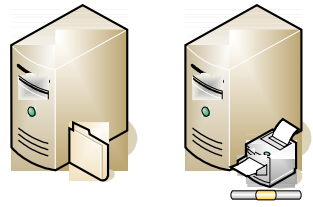
U mreži sa više od 10 korisnika, mreža ravnopravnih korisnika u kojoj se računari ponašaju i kao klijenti i kao serveri, nije adekvatno rešenje. U takvim situacijama postoje namenski serveri. Namenski server je računar čija je jedina uloga opsluživanje ostalih članova mreže i ne koristi se kao klijent ili radna stanica. Za servere se kaže da su „namenski" zato što oni ne obavljaju ulogu klijenta, već su optimizovani da brzo opsluže zahteve mrežnih klijenata i osiguraju bezbednost datoteka i direktorijuma.

Kako se mreža povećava brojem računara, njihovom međusobnom udaljenošću i saobraćajem između njih, nastaje potreba za većim brojem servera. Podela poslova na nekoliko servera obezbeđuje da se svi poslovi obavljaju na najefikasniji mogući način. Raznovrsnost i složenost poslova koje serveri treba da obave je velika. Mnoge velike mreže imaju različite vrste namenskih servera (*dedicated servers*):



Slika 4.5 Serverska mreža

- **Server za datoteke i štampanje**



Server za datoteke i štampanje upravlja pristupom korisnika i korišćenjem datoteka i štampača kao resursa. Dokument sa kojim želimo da radimo, a koji se čuva na serveru za datoteke i štampanje, učitava se u memoriju našeg računara, tako da možemo lokalno da ga uređujemo i koristimo. Ova vrsta servera služi za čuvanje datoteka i podataka.

- **Server za aplikacije**

Server za aplikacije klijentu na raspolaganje stavlja klijentsku stranu klijent/server aplikacije. U serverima se nalazi velika količina različitih podataka koji su organizovani tako da je njihovo pozivanje jednostavno. Razlika između servera za datoteke i štampanje i servera za aplikacije nalazi se u načinu odgovora na zahtev računara koji je zatražio podatke. U slučaju servera za datoteke i štampanje, podaci ili datoteke se učitavaju u računar koji ih zatraži. Međutim, kod servera za aplikacije, centralna logika aplikacije i osnovni podaci ostaju na serveru, a u računar koji je zatražio podatke učitavaju se samo rezultati zahteva. Klijentska aplikacija radi lokalno i pristupa podacima iz serverske aplikacije. Umesto da se u lokalni računar učitava čitava baza podataka, učitavaju se samo rezultati koji se dobijaju kao odgovor na upit. Na primer, ukoliko nam je iz baze podataka radnika potrebno da izdvojimo one koji su rođeni u novembru, server za aplikacije nam, na naš zahtev, neće odgovoriti učitavanjem čitave baze podataka. Umesto toga, na lokalni računar će biti poslat samo odgovor na postavljeni zahtev.

- **Komunikacioni server**

Komunikacioni serveri upravljaju protokom podataka i elektronskih poruka između mreže u kojoj je sam server i drugih mreža, glavnih računara (engl. mainframe) i udaljenih korisnika koji putem modema i telefonskih linija pristupaju serveru. E-pošta (E-mail) je važna komponenta savremene komunikacije. Serveri e-pošte upravljaju razmenom poruka između korisnika na mreži. U većini slučajeva, serveri elektronske pošte su slični serverima aplikacija, jer poruke e-pošte obično ostaju na serveru.

- **Serveri za organizaciju podataka**

Ovi serveri omogućavaju korisnicima da pronađu, smeste i zaštite podatke u mreži. Na primer, mrežni softver može računare da grupiše u logički organizovane grupe koje se zovu domeni, a to omogućava svim korisnicima mreže pristup svakom mrežnom resursu. Sa širenjem mreže, planiranje specijalizovanih servera dobija na značaju. Planer mreže mora da uzme u obzir očekivani rast mreže tako da se mreža ne poremeti ukoliko se javi potreba da se uloga nekog servera promeni.

- **FTP serveri**

Značajan udeo u saobraćaju na Internetu ima prenos datoteka

(*file transfer*), na primer preuzimanje novih verzija softvera i prenošenje poslovne dokumentacije. Serveri koji koriste FTP protokol za prenos podataka (*File Transfer Protocol*) omogućavaju prenos jedne ili više datoteka između računara.

Usluge koje server pruža klijentima se realizuju preko namenskih softverskih paketa (ili su zasnovane na mogućnostima operativnog sistema). Na jednom računaru je moguće instalirati više različitih softverskih paketa i na taj način dobiti multifunkcionalni server. Ovakav pristup je opravdan ukoliko hardverska moć računara može da podrži istovremeno izvršavanje pomenutog softvera i ukoliko sve usluge koristi uglavnom ista grupa korisnika. U protivnom, kombinovanje servisa na jednom računaru može u slučaju greške u jednom softverskom paketu ugroziti bezbednost i dostupnost ostalih servisa na tom računaru. Noviji odgovor za ovaj problem leži u virtualizaciji. Virtualizacija servera predstavlja korišćenje specijalnog sistemskog proširenja operativnog sistema koje omogućava kreiranje većeg broja "logičkih" računara koji dele stvarne (fizičke) resurse. Na svakom od logičkih servera se može instalirati različit operativni sistem sa različitim softverskim paketima i na taj način omogućiti određeni servis u mreži.

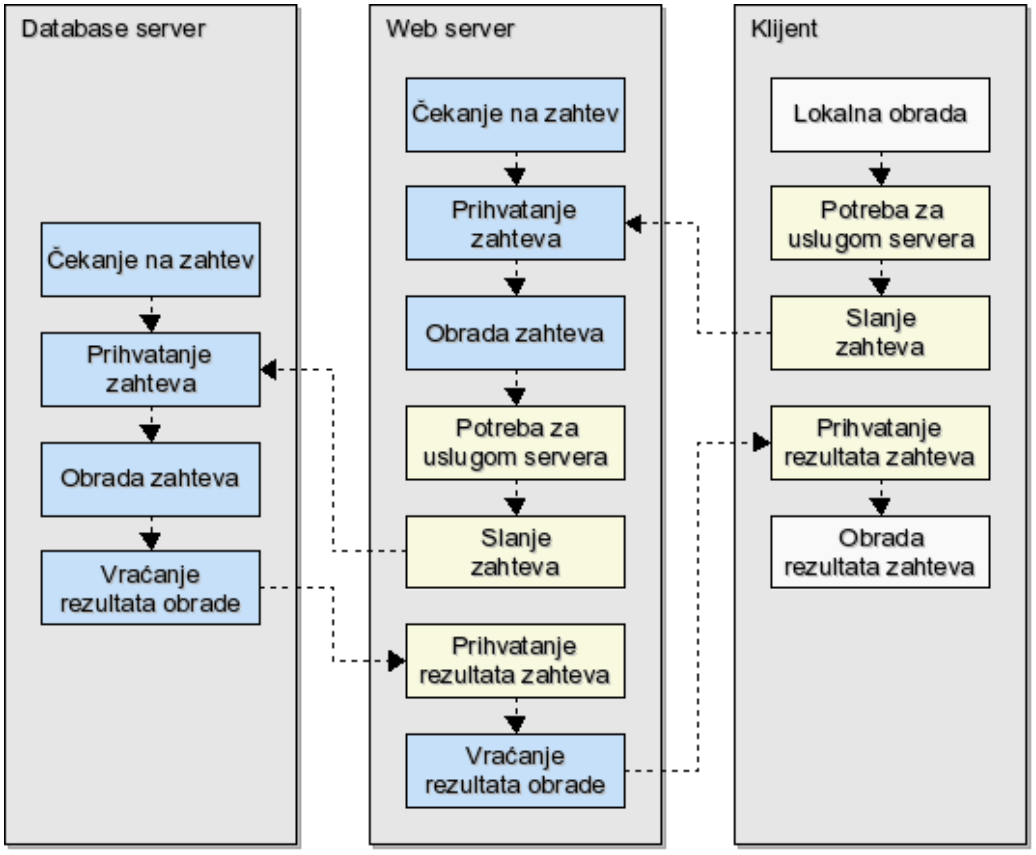
Postoji i situacija suprotna prethodnoj u kojoj hardverske mogućnosti jednog računara nisu u stanju da odgovore potrebama velikog broja korisnika servisa istovremeno. U tom slučaju se ista uloga raspodeljuje na veći broj fizičkih servera. Ukoliko se veći broj fizičkih servera krajnjima korisnicima predstavi kao jedna (logička) jedinica, takva konfiguracija servera se naziva klaster.

Iako su instaliranje, konfigurisanje i upravljanje kod serverskih mreža znatno složeniji nego kod mreža ravnopravnih korisnika, one imaju brojne prednosti. Server je napravljen tako da omogući pristup brojnim datotekama i štampačima, uz odgovarajuće performanse i bezbednost. Kod serverskih mreža je moguće administriranje i kontrolisanje zajedničkog korišćenja resursa iz jednog centra. Ovako se resursi lakše pronalaze i čine dostupnijim nego kod mreža ravnopravnih korisnika. Bezbednost je najčešće osnovni razlog opredeljivanja za serversku mrežu. U ovakvom okruženju jedan administrator može da definiše bezbednost i to, onda, važi za svakog korisnika mreže. U zavisnosti od važnosti podataka, moguće je praviti rezervne kopije više puta dnevno ili nedeljno. Kako su najhitniji podaci centralizovani na jednom ili nekoliko servera, ovaj proces je vrlo jednostavan.

Serverske mreže mogu imati hiljade korisnika. Takvom mrežom se ne bi moglo upravljati kada bi se primenio princip ravnopravnih korisnika, ali savremeni alati za nadgledanje i upravljanje mrežama omogućavaju da serverska mreža normalno funkcioniše i sa ogromnim brojem korisnika.

4.4.2.1. Klijent – server arhitektura aplikacija

Klijent-server arhitektura je jedan od najčešće korišćenih pristupa kod distribuirane obrade podataka. Koreni ove arhitektura se nalaze kod *mainframe* računara (host-based arhitektura) i njima priključenih terminala. Sličnost sa ovom arhitekturom jeste postojanje jednog člana sposobnog za izvršavanje zadataka koji su van mogućnosti ostalih članova mreže. Postoje, međutim, bitne razlike između ove dve arhitekture. Kod host-based arhitekture terminali nemaju nikakvu mogućnost obrade podataka dok kod klijent-server arhitekture klijenti od servera dobijaju podatke koje zatim koriste u lokalnom procesu obrade. Zatim, *mainframe* računari predstavljaju autonomne članove mreže koji za proces obrade podataka koriste lokalne resurse. Nasuprot tome, server se u vidu klijenta može obratiti drugim serverima u mreži za određeni resurs ili distribuiranu obradu.



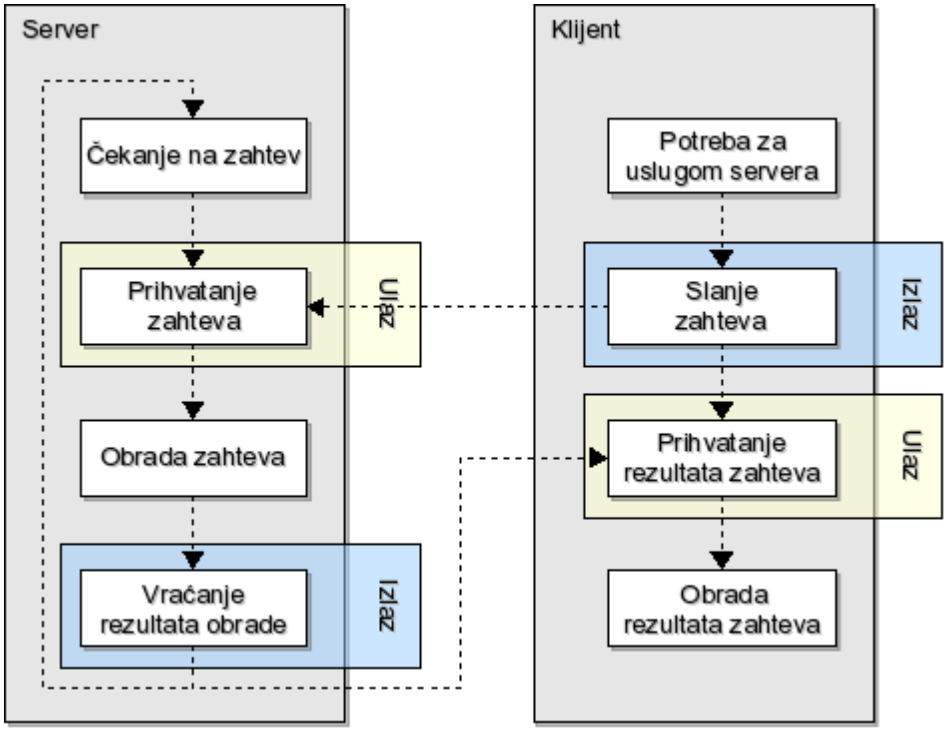
Slika 4.6 Slojevita klijent-server arhitektura

4.4.2.2. Iterativna i konkurentna obrada zahteva

U zavisnosti od načina obrade zahteva servere možemo podeliti na:

- servere sa iterativnom obradom zahteva
- servere sa konkurentnom obradom zahteva.

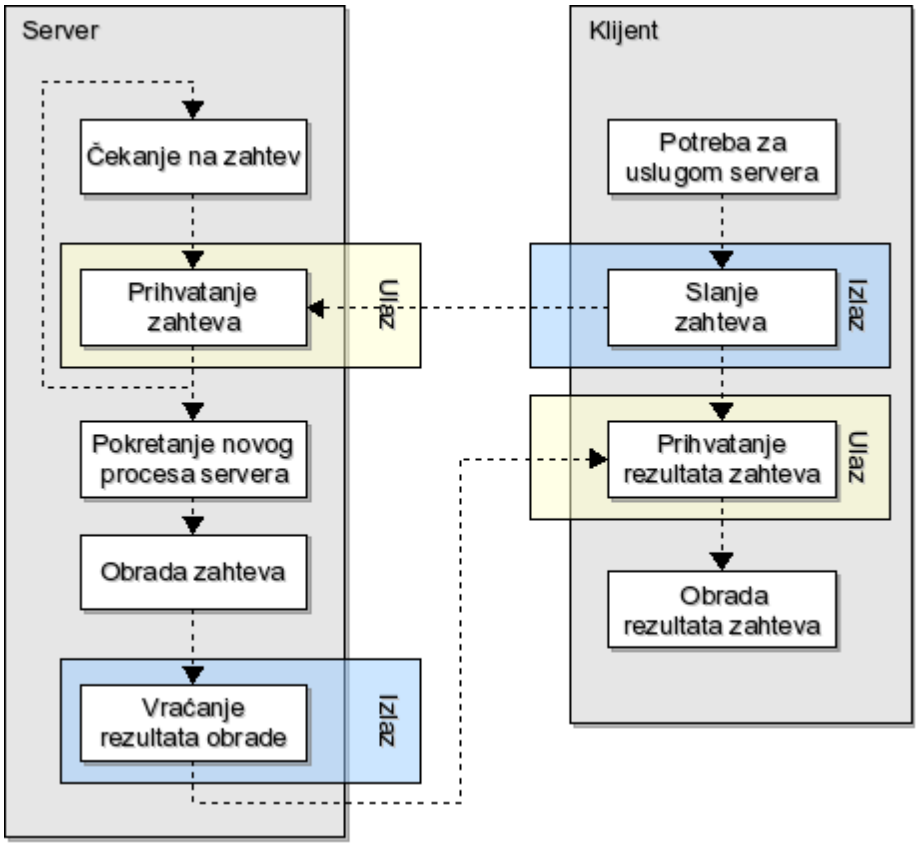
Serveri sa iterativnom obradom zahteva osluškuju na dodeljenom portu čekajući na zahtev klijenta. Nakon prihvatanja zahteva klijenta zahtevi ostalih klijenata se odbacuju ili čekaju u ulaznom baferu sve dok se prihvaćeni zahtev ne obradi i rezultati njegove obrade pošalju natrag klijentu.



Slika 4.7 Iterativna obrada zahteva

Mana iterativne obrade zahteva je u tome što takav pristup može znatno uticati na performanse u smislu broja obrađenih zahteva po jedinici vremena. Ukoliko obrada jednog zahteva u toku svog izvršenja zauzme sve resurse servera performanse se mogu smatrati optimalnim. Međutim, ukoliko obrada zahteva oduzme dodatno vreme usled čekanja na resurs koji nije potreban za obradu ostalih zahteva (koji su odbačeni ili čekaju u ulaznom baferu), iterativni pristup pokazuje lošije performanse od konkurentog. Glavna prednost iterativnog pristupa jeste eliminisanje problema konkurentnog pristupa internim resursima servera time što se u jednom trenutku obrađuje samo jedan zahtev tako da ne može doći do višestrukih zahteva za istim resursom.

Konkurentna obrada zahteva je pristup koji nudi bolje performanse od iterativnog pristupa u situacijama u kojim server obrađuje veliki broj zahteva od strane više klijenata. Poboljšanje pefromansi potiče od mogućnosti obrade više zahteva paralelno. Paralelna obrada se postiže pokretanjem novog procesa (ili niti procesa, u zavisnosti od operativnog sistema) za obradu zahteva kod svakog klijentskog zahteva.

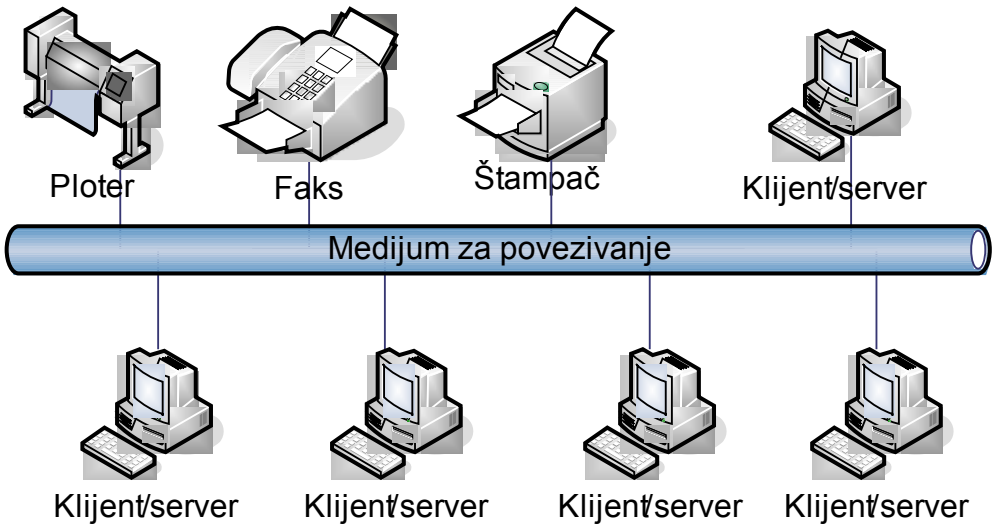


Slika 4.8 Konkurentna obrada zahteva

Za ovakav pristup je potreban kompleksniji serverski softver koji se sastoji od dispečerskog dela (dela koji je zadužen za prihvatanje zahteva i pokretanje procesa njihove obrade) i dela koji je zadužen za konkretnu obradu zahteva. Konkurentna obrada zahteva može u određenim situacijama pokazati slabije performanse od iterativne obrade usled trošenja procesorskog vremena na pokretanje novih procesa za obradu zahteva. Takođe, softver koji omogućava konkurentnu obradu je kompleksniji jer interno rešava konkurentni pristup sistemskim resursnima. Softver za konkurentnu obradu najčešće unapred pokreće određen broj procesa za obradu zahteva a po potrebi taj broj povećava do konfiguracione vrednosti ili ograničenja sistemskim resursima.

4.4.3. Peer-to-peer (P2P) mreže

Kod mreža ravnopravnih računara (*peer-to-peer* mreže) ne postoje namenski serveri niti hijerarhija računara. Svi računari su jednaki, odnosno ravnopravni. Nude jednostavan pristup povezivanju računara radi zajedničkog korišćenja resursa i međusobne komunikacije. Svaki računar funkcioniše i kao klijent i kao server, pa ne postoji administrator koji bi bio odgovoran za celu mrežu. Korisnik svakog računara sam određuje koji se resursi na njegovom računaru mogu deliti preko mreže.



Slika 4.9 Mreža ravnopravnih računara (peer-to-peer) sa zajedničkim mrežnim uređajima

Mreže ravnopravnih računara se često nazivaju i radne grupe. Ovaj termin se odnosi na malu grupu ljudi. Ovakvu mrežu najčešće čini 10 ili manje računara. Mreže ravnopravnih računara su relativno jednostavne. U situaciji kada svaki računar funkcioniše i kao klijent i kao server, ne postoji potreba za moćnim centralnim serverom, ili drugim komponentama svojstvenim mrežama velikog kapaciteta. Stoga su ove mreže jeftinije od serverskih mreža.

U ovim mrežama mrežni softver ne mora da ima isti nivo performansi i bezbednosti kao mrežni softver namenjen namenskim serverima. Mogućnost umrežavanja u mrežu ravnopravnih korisnika ugrađena je u mnoge operativne sisteme. Zbog toga nije potreban nikakav dodatni softver.

U tipičnom mrežnom okruženju, ova vrsta mreža pruža sledeće prednosti:

- Umrežavanje je jednostavno.

- Ne zahteva se kupovina posebnog softvera za umrežavanje.
- Korisnici su sami sebi administratori i sami planiraju bezbednost.
- Ispad nekog računara iz mreže ima uticaj samo na eventualno deljene resurse na datom računaru. Ostali računari mogu da nastave rad.

Ove mreže su dobar izbor u sledećim situacijama:

- Na lokaciji ima manje od 10 korisnika.
- Korisnici dele zajedničke resurse, kao što su datoteke i štampači, ali ne postoje specijalizovani serveri.
- Pitanje bezbednosti nije značajno.
- U doglednoj budućnosti organizacija i mreža se neće znatno proširiti.

Bezbednost, sprečavanje neovlašćenog pristupa računarima i podacima, podrazumeva definisanje lozinke za resurs, recimo za određeni direktorijum, koji se koristi preko mreže. U mreži ravnopravnih korisnika, svaki korisnik sam podešava sopstvenu bezbednost, pa je zato teško sprovesti centralnu kontrolu. Ovaj nedostatak kontrole ima značajne posledice na bezbednost mreže, jer pojedini korisnici mogu da ne primenjuju nikakve mere bezbednosti. Stoga, ukoliko je bezbednost bitan faktor, bolje rešenje predstavlja serverska mreža.

Peer-to-peer (P2P) arhitektura predstavlja vid distrubuiranog računarstva u kome svaki čvor (eng. *node*) ima dvostruku ulogu. Svaki čvor P2P mreže komunikaciju sa ostalim članovima P2P mreže obavlja putem simetričnog softvera koji se može ponašati i kao klijent (zahtevajući podatke ili usluge od ostalih čvorova) i kao server (odgovarajući na zahteve ostalih čvorova). Na ovaj način P2P arhitektura omogućava veću autonomiju članova mreže. P2P arhitektura se uglavnom primenjuje kod potreba u kojima postoji veća tolerancija greške kod distribuirane odbrade. Glavne primene su:

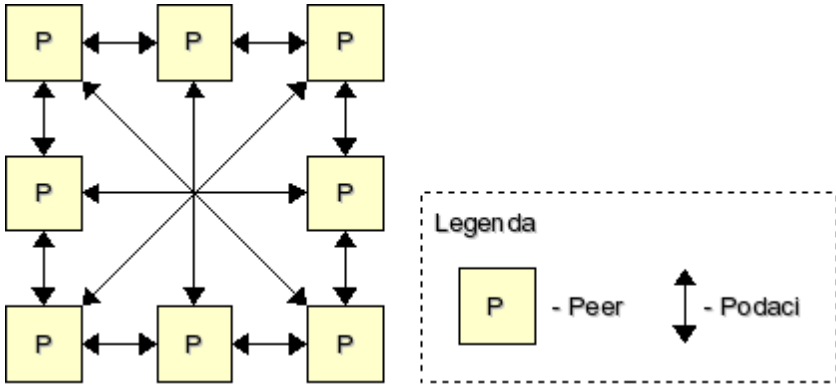
- Razmena fajlova
- Komunikacija
- Distribuirana obrada ogromne količine podataka
- Heš tabele
- Softver za zabavu

Glavni nedostatak P2P arhitekture jeste adresiranje članova mreže. Dok je kod klijent-server mreža potrebno samo da klijenti imaju informaciju o tome koji serveri su dostupni na mreži (i koja je njihova adresa) kod P2P arhitekture je

potrebno da svaki član ima informaciju dostupnosti ostalih članova. Iz tog razloga postoji više različitih arhitektura unutar P2P arhitekture:

- decentralizovana arhitektura
- centralizovana arhitektura
- hibridna arhitektura

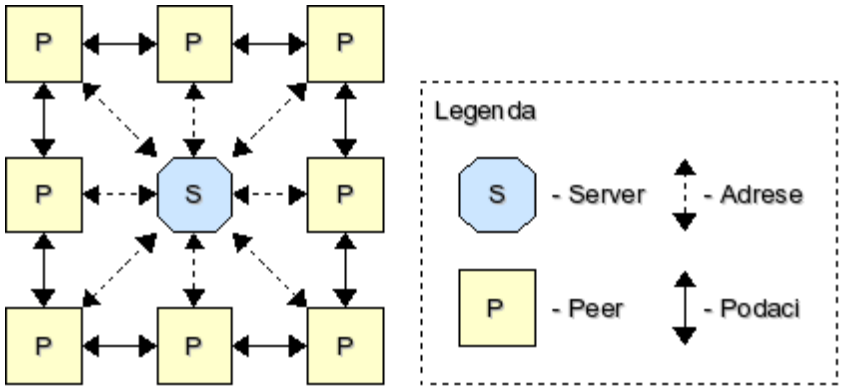
Decentralizovana P2P arhitektura predstavlja arhitekturu najbližu osnovnom P2P modelu. Ona je sačinjena isključivo od *peer* čvorova koji međusobno komuniciraju direktno.



Slika 4.10 Šema decentralizovane P2P mreže

Kod decentralizovane P2P arhitekture ne postoji centralni registar članova već se otkrivanje ostalih članova vrši preko internog protokola (najčešće u vidu *broadcast* zahteva).

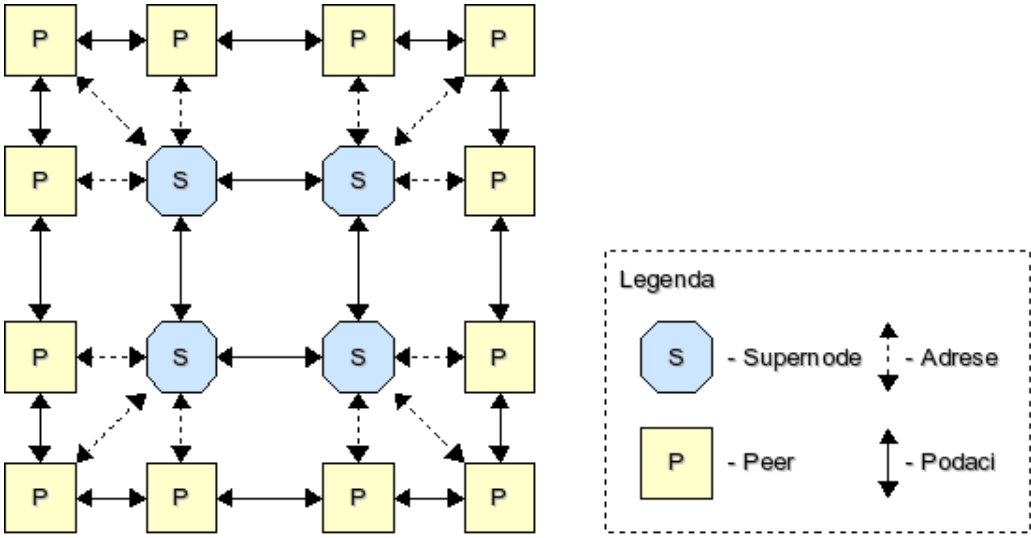
Centralizovana P2P arhitektura predstavlja mešavinu P2P i klijent-server arhitektura.



Slika 4.11 Šema centralizovane P2P mreže

Kao i kod decentralizovane P2P arhitekture mrežu čine *peer* čvorovi koji međusobno komuniciraju direktno sa tom razlikom da postoji centralni server čiji je zadatak evidentiranje *peer* članova mreže.

Hibridna P2P arhitektura predstavlja varijantu centralizovane P2P arhitekture koja se koristi u slučajevima kada se mreža sastoji od velikog broja *peer* čvorova i/ili uloga servera podrazumeva i dodatne operacije sem evidentiranja.



Slika 4.12 Šema hibridne P2P mreže

Kod hibridne P2P arhitekture ulogu servera preuzima veći broj *Supernode* čvorova. Ove čvorove najbliži *peer* čvorovi koriste kao servere dok adresne informacije vezane za *peer* čvorove *supernode* čvorovi međusobno razmenjuju.

5. Slojevitost i referentni modeli

U ranim fazama razvoja računarskih mreža većinu računarskih sistema su činili Unix *mainframe* računari sa priključenim korisničkim terminalima. Iako su korisnički terminali bili povezani komunikacionim kanalima sa *mainframe*-om takva mreža se ne može u smatrati punom smislu reči računarskom pre svega zbog nedostatka računske moći terminala - veza između terminala i *mainframe*-a je imala za zadatak prenos korisničkih instrukcija do *mainframe*-a i rezultata obrade do terminala. U takvoj situaciji je ekskluzivno pravo na razvoj hardvera, softvera i komunikacionih kanala uglavnom imao samo jedan proizvođač koji je svoja rešenja držao zatvorenim za ostale proizvođače. Komunikacija između rešenja različitih proizvođača je najčešće bila nemoguća usled nekompatibilnosti između hardverskih interfejsa i formata podataka.

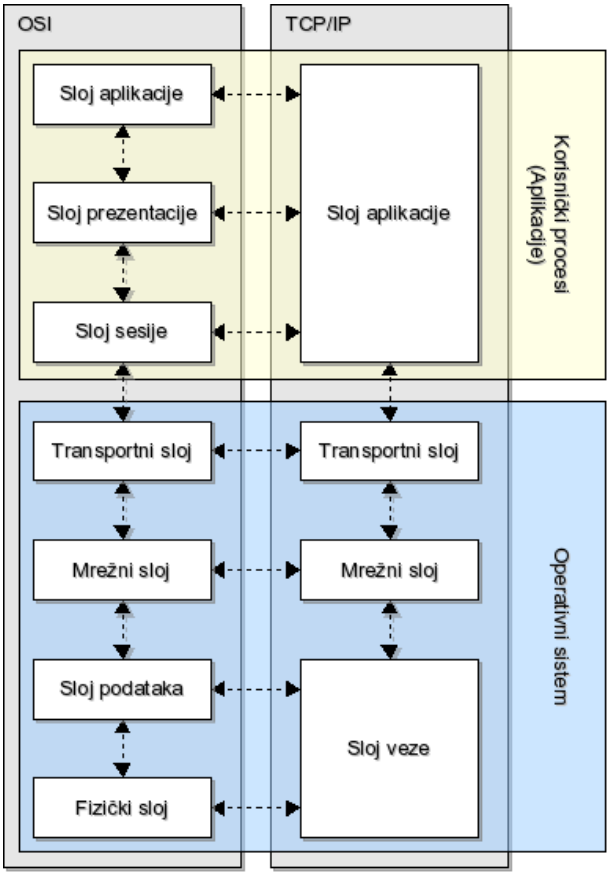
Paralela

Korisnik A pomoću aplikacije napisane u Java programskom jeziku koja se izvršava na MS Windows operativnom sistemu šalje putem Interneta HTTP zahtev Web serveru X. Računar korisnika je bežično povezan sa lokalnom mrežom čiji gateway radi pod Cisco operativnim sistemom i sa ISP-om je povezan optičkim kablom. Komunikacioni serveri ISP-a rade pod NetBSD operativnim sistemom i koriste satelitski link ka Internetu. Web server X HTTP zahteve obrađuje preko softvera napisanog u C programskom jeziku koji se izvršava pod Linux operativnim sistemom. Server je od direktnog pristupa sa Interneta zaštićen firewall-om koji radi pod FreeBSD operativnim sistemom i sa kojim je povezan putem Ethernet tehnologije.

Korisnik B je vlasnik mobilnog telefona čiji softver nije izmenljiv, podržava pozivanje, prihvatanje i odbijanje poziva i ograničen je na korišćenje Y operatera mobilne telefonije.

Pad cene računske moći preko sve jeftinijih tehnologija za razvoj mikroprocesora i računarske opreme doveo je do pojavljivanja većeg broja proizvođača računarskih sistema. Takav razvoj je omogućio decentralizaciju računske moći koja je ukazala na potrebu za kompleksnijom komunikacijom između radnih stanica. Takođe, postojanje većeg broja proizvođača ublažilo je različitost i nekompatibilnost njihovih rešenja a ubzo se uvidela i potreba za univerzalnim komunikacionim standardima.

Na ovu temu se krajem 70-ih godina dvadesetog veka oglasila i Internacionalna Organizacija za Standardizaciju (ISO) razvijanjem modela za komunikaciju između raznorodnih sistema. Model je objavljen 1984. godine i nazvan je *Open System Interconnection Basic Reference Model* ili, skraćeno, OSI model. Ovaj model je ponudio fazno prevođenje formata podataka kroz sedam slojeva pa se stoga naziva i OSI sedmoslojni model. Prihvatanjem ovog ISO standarda proizvođači su bili u mogućnosti da ostvare potpunu komunikaciju sa sistemima bez uvida u njihovu internu specifikaciju i format podataka.



Slika 5.1 OSI i TCP/IP modeli

Jedna od glavnih mana OSI modela jeste nepotrebno zalaženje u interne delove računarskih sistema tj. definisanje komponenti koje nisu direktno zadužene za među-sistemsku komunikaciju. Kao posledica toga se javio veći broj korisničkih aplikacija koje nisu u potpunosti poštovale OSI standard a ipak su bile u mogućnosti da nesmetano komuniciraju korišćenjem nižih slojeva modela. Ovakva tendencija se rezultovala pojavljivanjem jednostavnijeg Internet modela (TCP/IP) koji daje veću slobodu pri izboru arhitekture aplikativnog softvera.

Također, ovaj model apstraktno gleda i na najniže slojeve OSI modela s obzirom na to da se komponente tih slojeva najsporije razvijaju i to uglavnom od strane velikih organizacija.

5.1. OSI model

Open Systems Interconnection Reference Model (OSI model) je razvijen 1984. godine od strane ISO organizacije. Iako je OSI model formalni standard danas se u praksi češće koristi jedostavniji *de facto* standard - Internet model (TCP/IP). OSI model definiše sedam slojeva:

1. **Fizički sloj**
   Fizički sloj OSI modela je zadužen za prenos bitova (nula i jedinica) putem komunikacionog kanala. Ovaj sloj definiše pravila po kojima se bitovi prenose, koji električni napon je potreban, koliko bitova se šalje po sekundi i fizički format korišćenih kablova i konektora.

2. **Sloj veze**
   Sloj veze upravlja prenosom putem fizičkog sloja i omogućava prenos oslobođen grešaka na ovom i fizičkom sloju. Zadatak sloja veze jeste da zaštiti slojeve višeg nivoa od grešaka nastalih pri prenosu podataka. Takođe, s obzirom na to da je jedinica prenosa fizičkog sloja bit, sloj veze upravlja i formatom poruka (definiše početak i kraj poruke).

3. **Mrežni sloj**
   Zadatak mrežnog sloja jeste određivanje jedne ili više putanja kojima će poruka biti prosleđena od izvorišta do odredišta. Mrežni sloj je zadužen da u svakom čvoru mreže (stanici do odredišta) odredi koji je sledeći računar kome poruka treba biti prosleđena.

4. **Transportni sloj**
   Zadatak transportnog sloja jeste obrada poruka na krajnjim tačkama - izvorištu i odredištu. Ovaj sloj uspostavlja, održava i prekida virtuelne veze za prenos podataka između izvorišta i odredišta. Transporni sloj je zadužen za nabavku mrežne adrese odredišta, podelu podataka u segmente pogodne za slanje, prilagođavanje brzine prenosa mogućnostima strane sa slabijim performansama, osiguravanje prenosa svih segmenata, eliminisanju dupliranih segmenata i sl. Takođe, ovaj sloj može izvršiti i dodatnu kontrolu grešaka pri prenosu (dodatnu u smislu da je ona već izvršena na sloju veze).

5. **Sloj sesije**
   Sloj sesije je zadužen za uspostavljanje, održavanje i prekid logičkih sesija između krajnjih tačaka. Svrha sesija jeste definisanje stanja (ili faza) svakog dijaloga radi definisanja validnih akcija u svakom od stanja. Na osnovu toga se vrši upravljanje transportnim slojem i provera podataka dobijenih od njega. Dodatna uloga sesija jeste i obračunavanje sesija (eng. *session accounting*).

6. **Sloj prezentacije**

Sloj prezentacije formatira podatke za prezentaciju korisniku. Zadatak ovog sloja jeste da uskladi format podataka između učesnika u komunikaciji i sloju aplikacije dostavi ove podatke u formatu koji on zahteva. Na primer, sloj prezentacije može originalne podatke dobijene od sloja aplikacije kompresovati radi efikasnijeg prenosa. Ovakve podatke sloje prezentacije na strani drugog učesnika ne može direktno proslediti sloju aplikacije već je pre toga neophodno izvršiti dekompresiju.

7. **Sloj aplikacije**
   Sloj aplikacije predstavlja interfejs mreže ka korisniku. Osnovna uloga ovog sloja je omogući pristup mreži korisničkim programima.

5.2. Internet model (TCP/IP)

Nasuprot OSI modelu koji je formalno standardizovan Internet model (TCP/IP) je *de facto* standard. Ovaj model je razvijan za potrebe Interneta i jednostavniji je od OSI modela. Jednostavnost ovog modela se ogleda u apstraktnom gledanju na najviša tri sloja OSI modela tako da Internet model propisuje samo sloj aplikacije naspram slojeva aplikacije, prezentacije i sesije kod OSI modela. Takođe, usled nedostatka formalne standardizacije Internet modela u nekim izvorima se ovaj model definiše sa 5 a u nekim sa 4 sloja. Današnje implementacije mrežnog softvera ulgavnom koriste Internet model.

6. Fizički sloj

6.1. RS-232

RS-232 ili serijski port računara je jedan od najčešće korišćenih interfejsa za umrežavanje računara u prošlosti. Iz tog razloga su računari proizvedeni krajem prošloga veka dolazili sa dva integrisana RS-232 porta na matičnoj ploči. Prednost RS-232 portova je bila njihova niska cena i mogućnost direktnog povezivanja dva računara putem ovih interfejsa. Takođe, čest uređaj na serijskim portovima su i modemi koji omogućavaju umrežavanje putem telefonskih linija.

Danas se RS-232 portovi sve ređe sreću kao sastavni deo matičnih ploča računara. Razlog tome je prevaziđenost ovih portova u smislu brzine (maksimalna brzina je 115.200 bitova po sekundi) i pojava USB (Universal Serial Bus) standarda.

6.2. USB (Universal Serial Bus)

USB standard se može smatrati naslednikom RS-232 serijskog načina povezivanja. Prednosti USB magistrale nad RS-232 magistralom su daleko veće brzine prenosa podataka i mogućnost povezivanja više od jednog uređaja po portu.

Opis USB podrške u Linux OS

Universal Serial Bus (USB) is a specification for a serial bus subsystem which offers higher speeds and more features than the traditional PC serial port. The bus supplies power to peripherals and allows for hot swapping. Up to 127 USB peripherals can be connected to a single USB host in a tree structure.

The USB host is the root of the tree, the peripherals are the leaves and the inner nodes are special USB devices called hubs. Most PCs now have USB host ports, used to connect peripherals such as scanners, keyboards, mice, modems, cameras, disks, flash memory, network links, and printers to the PC.

Say Y here if your computer has a host-side USB port and you want to use USB devices. You then need to say Y to at least one of the Host Controller Driver (HCD) options below. Choose a USB 1.1 controller, such as "UHCI HCD support" or "OHCI HCD support", and "EHCI HCD (USB 2.0) support" except for older systems that do not have USB 2.0 support. It doesn't normally hurt to select them all if you are not certain.

If your system has a device-side USB port, used in the peripheral side of the USB protocol, see the "USB Gadget" framework instead.

Iako je putem USB magistrale moguće direktno povezivanje dva računara pomenute prednosti ovog standarda se ogledaju pre svega u velikom broju raličitih uređaja koji služe za umrežavanje računara (Ethernet adapteri, modemi, ISDN terminal-adapteri, ADSL modemi itd.) kao i uređaja koji nisu vezani za računarske mreže (štampači, skeneri, audio-adapteri, tastature, miševi...).

6.3. FireWire (IEEE1394)

FireWire standard predstavlja IEEE standard pod brojem 1394. Ovaj standard se može najbliže porediti sa USB standardom jer nudi serijsku magistralu visokih performansi.

Opis FireWire podrške u Linux OS
IEEE 1394 describes a high performance serial bus, which is also known as FireWire(tm) or i.Link(tm) and is used for connecting all sorts of devices (most notably digital video cameras) to your computer. If you have FireWire hardware and want to use it, say Y here. This is the core support only, you will also need to select a driver for your IEEE 1394 adapter.

FireWire standard je manje popularan od USB-a ali postoji priličan broj uređaja koji ga koristi za povezivanje sa računarom.

6.4. IrDA (Infrared Data Association)

Infrared način prenosa podataka podrazumeva infracrvene svetlosne signale kao osnovne nosioce komunikacije. IrDA adapteri omogućavaju korišćenje ovih signala za prenos podataka između računara.

Opis IrDA podrške u Linux OS
Say Y here if you want to build support for the IrDA (TM) protocols. The Infrared Data Associations (tm) specifies standards for wireless infrared communication and is supported by most laptops and PDA's.

Glavni nedostatak infrared načina prenosa podataka jeste potreba za optičkom vidljivošću i preciznim usmerenjem svetlosti kao i mala brzina prenosa pdoataka. Iz tog razloga se IrDA interfejsi koriste za premošćenje malih udaljenosti a ovim adapterima su uglavnom opremljeni mobilni telefoni, lap-top ralunari i PDA uređaji. IrDA interfejsi sve više izlaze iz upotrebe usled Bluetooth tehnologije koja omogućava robusniji prenos podataka na malim udaljenostima putem radio talasa.

6.5. Bluetooth

Bluetooth je bežična tehnologija prenosa podataka i govora, razvijena od strane proizvođača raznovrsne elektronske opreme, sa ciljem da se njihovi proizvodi – od kompjutera i telefona do tastatura i bežičnih slušalica, umreže na malim udaljenostima (do 10 metara) bez upotrebe kablova, brzo i jednostavno. Ideja iz koje je potekao bluetooth, nastala je 1994. godine kada je Ericsson Mobile Communications odlučio da ispita mogućnosti povezivanja mobilnih telefona sa njihovim dodacima preko jeftine radio veze sa malom potrošnjom struje. Ideja je bila da se u svaki uredjaj ugradi mali radio i na taj način iz upotrebe izbace kablovi. Godinu dana kasnije, pravi potencijal te ideje je počeo da se kristališe. Glavna istraživanja obavljana su u Ericsson-ovim laboratorijama u Lundu, Švedska. Ericsson je pre usvajanja imena bluetooth tehnologiju nazivao „Multi-Communicator Link“ (MC Link). Originalna zamisao bila je da se poveže bežična slušalica sa mobilnim telefonom, a to što su otkrili da na isti način mogu da povežu većinu elektronskih uređaja, bila je, po njihovim rečima – srećna slučajnost. Početkom 1997. godine Ericsson je uradio nešto sasvim neočekivano – odlučio je da tehnologiju ne naplaćuje, i svim zaintresovanim kompanija dao besplatne licence, jer je to bio najbolji način da tehnologija postane globalni standard. Ericsson je započeo razgovore sa kompanijama iz različitih sfera proizvodnje elektronske opreme (Nokia – mobilni telefoni, IBM i Toshiba – prenosni kompjuteri i Intel – čipovi za digitalnu obradu signala) sa ciljem da se osnuje konzorcijum koji će dalje razvijati i promovisati tehnologiju.

Opis Bluetooth-a

Bluetooth je bežična tehnologija povezivanja uređaja na kratkim rastojanjima koja primenjuje male snage zračenja. Dizajnirana je kao zamena za kablovske sisteme povezivanja, kao i druge tehnologije kratkog dometa (kao što je infracrveno zračenje IrDA. Bluetooth se primenjuje u personalnom okruženju koje se tipično proteče u radijusu do 10 metara. Više informacija o Bluetooth-u može se naći na adresi <http://www.bluetooth.com/>.

Bluetooth tehnologija javnosti je zvanično predstavljena 20. maja 1998. godine kada je pet kompanija, Ericsson, IBM, Intel, Nokia i Toshiba, održalo simultanu konferenciju za štampu u Londonu, Tokiju i San Hozeu, na kojoj je objavljeno da su se pet kompanija udružile ne bi li razvile besplatnu tehnologiju, otvorene specifikacije za bežično umrežavanje.

6.5.1. Bluetooth proizvodi

Danas kad je bluetooth već postao standard za umrežavanje na malim udaljenostima, mogućnosti bluetooth tehnologije su razne i teško ih je nabrojati – od originalne zamisli, povezivanje bežične slušalice sa mobilnim telefonom,

preko upravljanja kompjuterom uz pomoć mobilnog telefona i razmena podataka između dva mobilna telefona, pa do nalaženja partnera (toothing), kontrole zamrzivača i mikrotalasne rerne, kao i „bežičnog“ pisanja sa bluetooth olovkom.

U današnje vreme većina uređaja dolazi sa ugrađenom podrškom za bluetooth (mobilni telefoni, laptop i palmtop kompjuteri), ali je naravno moguće kupiti i posebne bluetooth adaptere za većinu elektronskih uređaja.

Bluetooth USB adapter

COM Bluetooth bežična PC kartica

Bluetooth adapter za kola

Logitech Bluetooth bežična slušalica

6.5.2. Princip rada

Bluetooth je tehnologija koja koristi radio talase za uspostvljanje point-to-point i point-to-multipoint transfere govora i podataka u radijusu od 10 metara. Kada se dva ili više Bluetooth uređaja spoje, kreira se tzv. piconet. Svaki piconet može da sadrži do 8 različitih uređaja (jedan master i sedam slave uređaja), a više piconeta (najviše 10, odnosno ukupno 80 uređaja) može biti spojeno u scatternet.

Frekvencijski opesg za bluetooth prenos je definisan u granicama 2.4GHz do 2.48 GHz. Teoretska najveća moguća brzina prenosa po Bluetooth specifikaciji iznosi 2.1 Mb/s. U praksi je to naravno malo drugačije. Maksimalna dvosmerna brzina prenosa (fullduplex, komunikacija u oba pravca u isto vreme) je 462 Kbps.

Asimetrična transmisija omogućava brzinu prenosa od 721 Kbps u jednom pravcu, i 56 Kbps u drugom. U slučaju prenosa govora, koriste se tri sinhrona kanala brzine od 64 Kbps (svaki).

Bluetooth radio podržava tri simultana sinhrona kanala za govor i jedan asihroni kanal za podatke (ili: jedan kanal koji simultano podržava ashironi prenos podataka i sinhroni prenos govora).

Bluetooth uređaji se u svakom trenutku nalaze u neka od dva glavna stanja: stanje uspostavljene konekcije (Connection) i stanje pripravnosti (Standby). Uređaj je u stanju connection ako ima uspostavljenu vezu sa drugim uređajem (ili uređajima) i ako obavlja neku aktivnost (primanje/slanje). U slučaju da nema uspostavljene veze niti aktivnosti, uređaj se automatski prebacuje u standby stanje radi ekonomičnijeg trošenja energije.

Da bi se izbegla interferencija bluetooh uređaja sa drugim uređajima iz ISM opsega (a i da bi se povećala sigurnost), koristi se spread spectrum frequency hopping tehnika Kada je uređaj u stanju standby, on na svakih 1.28 sekunde „osluškuje“ poruke od drugih uređaja. Svako „osluškivanje“ se obavlja na 32 različite frekvencije.

U bluetooth specifikaciji, definisana su tri moguća bezbednosna moda:

- Mode 1: *Non-Secure*: u ovom modu, ne koriste se nikakve procedure zasigurnu transmisiju.
- Mode 2: *Service-Level Enforced Security*: u ovom modu, bluetooth uređaj primenjuje procedure za sigurnu transmisiju nakon uspostavljanja konekcije.
- Mode 3: *Link-Level Enforced Security*: u ovom modu, bluetooth uređaj primenjuje procedure za sigurnu transmisiju pre uspostavljanja konekcije.

6.6. Ethernet

Ethernet je najviše korišćena mrežna tehnologija u LAN mrežama. Razvila ga je sredinom 1970ih godina Korporacija Xerox, a 1979. godine Digital Equipment Corporation (DEC) i Intel su ujedinili snage sa Xeroxom da bi standardizovali sistem. IEEE je uveo 1983. godine službeni standard za Ethernet i nazvao ga IEEE 802.3 po imenu radne grupe odgovorne za njegov razvoj, a 1985. godine uvedena je verzija 2 (IEEE 802.3a). Ethernet je preživeo niz godina, u dosta velikoj meri zahvaljujući svojoj velikoj fleksibilnosti i relativnoj jednostavnosti za implementaciju i razumevanje. Razlog uspeha je u tome što Ethernet ima dobru ravnotežu izmedju brzine, cene i lakoće instalacije.

Prednosti Ethernet mreža su:

- mreže su jednostavne za planiranje i ekonomične za instalaciju;
- mrežne komponente su jeftine;
- tehnologija se pokazala kao pouzdana;
- jednostavno je dodati i ukloniti računare sa mreže;
- podržavaju ga mnogi softverski i hardverski sistemi.

Glavni problem Etherneta je što se korisnici takmiče za pristup mreži i nema garancije da će korisnik moći da pristupi mreži uvek kada ima podataka za slanje. Naime, do problema dolazi kada dva ili više korisnika želi da koristi mrežu u isto vreme. U tom slučaju dolazi do sudara (kolizije) podataka različitih korisnika. Korisnici mora da prestanu sa slanjem i da sačekaju određeno vreme dok mreža ne postane slobodna.

Ethernet sam po sebi ne obezbeđuje nikakvu sigurnost, on je jednostavan i otvorena fizička sredina za prenos podataka. Nije imun na prisluškivanje i špijuniranje. Slabosti Etherneta su:

- Ethernet je otvorena arhitektura gde svaki čvor može da šalje ili da prima;
- koristi širokodifuzne (broadcast) komunikacije;
- lako ga je prisluškivati;
- nema nikakav hardver za obezbeđenje;
- lako je onesposobiti mrežu.

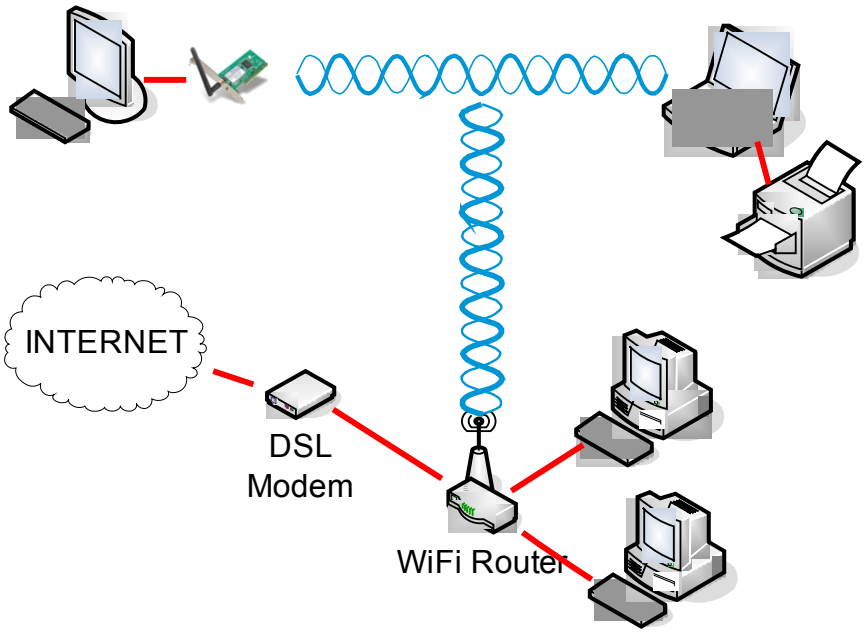
Postoje nekoliko glavnih standardnih tipova Ethrneta:

- standardni, ili sa debelim kablom (thickwire) Ethernet (10BASE5)
- sa tankim kablom, thinnet (ili thinwire) Ethernet ili Cheapernet (10BASE5)
- Ethernet sa upredenim paricama (10BASET)
- Ethernet sa optičkim kablovima (10BASEFL)
- Brzi Ethernet (100BASETX ili 100VGAnyLAN)
- Gigabitni Ethernet (1000BASET ili 1000BASE)

Ograničenja performansi Etherneta su prevaziđena verzijom 100BaseT, koja je poznata kao "Brzi Ethernet". Njome su podržane brzine prenosa podataka od 100 Mb/s. Kod Gigabit Etherneta brzina je od 1 Gb/s. Sa komutiranim Ethernetom, svaki par pošiljaoca i primaoca ima puni propusni opseg.

6.7. 802.11 (WiFi)

Bežično (wireless) umrežavanje je verovatno najjednostavniji način umrežavanja, nudi srednju brzinu i ne zahteva dodatne kablove. WiFi tehnologija obuhvata WiFi kartice (interna ili eksterna) uz koje se obično isporučuju i dogovarajuće antene. Na ovaj način moguće je formirati manje mreže (mreže do 30 m). Za veća rastojanja koriste se eksterne antene koje vrše dodatno pojačanje signala. Za priključivanje na neku mrežu potreban je tzv. *Hotspot*, odnosno čvorište na koji se spajaju svi ostali korisnici. Ako je mreža osigurana ona će tražiti WEP ili noviji WPA (2) ključ, a ako je slobodna onda nema nikakvih ograničenja za spajanje.



Svako može biti hotspot, jedino umesto obične kartice je potrebno kupiti Wireless Acces Point koji nudi pokrivenost od oko 30 metara, dok je uz razne pojačavače moguće bitno proširiti pokrivenost. Najskuplja varijanta, ali ona najbolja, je uzeti Wireless Access Point Router koji sadrži priključak za DSL modem, Router, Ethernet Hub, Firewall i Access Point. Uz sve to moguće na samo taj uređaj priključiti jednu Ethernet mrežu na koju će biti povezani korisnici sa WiFi karticama, tako da bi svi zajedno imali pristup internetu putem DSL modema.

Standardi Wi-Fi

- 802.11a standard ima teoretsku brzinu od 54 megabita u sekundi, no najčešće ona iznosi oko 30 megabita/s. Ovaj standard je skuplji jer WiFi kartice zasnovane na a standardu rade na višim frekvencijama (5GHz, za razliku od 2.4 GHz kod b i g standarda)

- 802.11b standard predstavljen 1999. u isto vrijeme kada i 802.11. U ovakvim mrežama brzina protoka podataka je do 11 megabita u sekundi, ali uz velike prepreke i smetnje brzina može spasti na malih 1 do 2 megabita/s. Ovo je ujedno i najjeftinija varijanta WiFi mreže.

- 802.11g je predstavljen 2003. godine i objedinio je prethodna dva standarda. Rradi na 2.4 GHz, ali ima skoro istu brzinu kao i 802.11a standard.

- 802.11n se očekuje sredinom 2007. godine. Prema očekivanjima standard bi trebao raditi 2.4 GHz, sa dosta povećanom najvišom brzinom koja će iznositi do 540 Mbps.

6.8. ISDN (Integrated Services Digital Network)

ISDN (*Integrated Services Digital Network*) je, prema ITU-T, mreža integrisanih servisa koja obezbeđuje digitalnu vezu između korisničkih mrežnih interfejsa. Predstavlja digitalni ekvivalent analogne telefonske mreže, a u odnosu na nju obezbeđuje bolji kvalitet i veću brzinu prenosa. Početkom 70-tih godina XX veka prvi put se javila ideja o integrisanim servisima tj. ideja da se preko jedne jedinstvene mreže korisnicima ponudi čitava paleta servisa. Osim standardnih servisa telefonije, telegrafije i prenosa podataka korisnicima bi se ponudio i prenos faksa, zvuka , muzike i videa. 1984. donet je prvi paket preporuka za realizaciju i primenu ISDN-a. ISDN se može posmatrati i kao set protokola za uspostavljanje i raskidanje digitalne veze. Primer je mreže sa komutacijom veza (*circuit switched connections*).

Termin: mreža integrisanih servisa koja obezbeđuje digitalnu vezu odnosi se na tri bitne stvari:

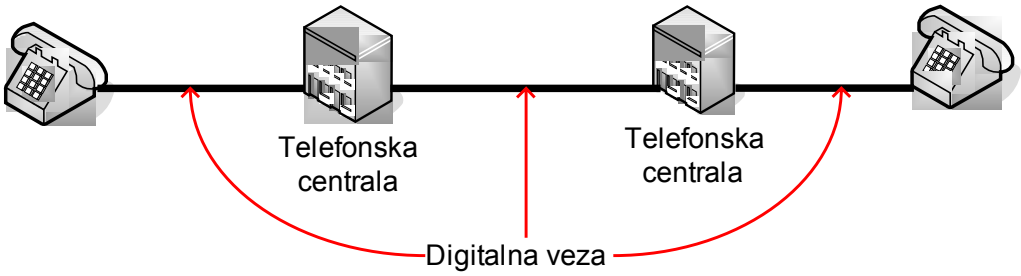
- **Integrisani servisi.** ISDN omogućava minim dve istovremene veze (bilo koja kombinacija prenosa podataka, govora, videa ili faksa) preko samo jedne fizičke linije. Na ISDN se mogu povezati različiti uređaji, kako bi se zadovoljile različite čovekove potrebe za komunikacijom. Nije potrebno obezbeđivati višetruke analogne telefonske linije, a omogućena je daleko veća brzina prenosa.

- ***Digitalna veza.*** Misli se na digitalni prenos u odnosu na analogni prenos kod standardnih telefonskih linija. Ako se na Internet povezujete standardnom analognom telefonskom linijom, modem kod vašeg Internet provajdera vrši D/A konverziju sajta kojeg ste posetili pre nego što vam ga pošalje. Vaš modem kod kuće vrši A/D konverziju, Ovakve konverzije se neprekidno dešavaju na svaki klik mišem. Ako se povezivanje vrši preko ISDN-a ne postoje D/A i A/D konverzije. Podaci se prenose digitalno, a dobro su poznate prednosti digitalnog prenosa.

- ***Mreža.*** ISDN nije jednostavna digitalna veza od tačke do tačke, kao što je npr. iznajmljena linija. ISDN mreža se proteže od lokalne telefonske centrale sve do udaljenog korisnika uključujući sve telekomunikacione uređaje i centrale na prenosnom putu.

ISDN predstavlja nadgradnju, odnosno viši stepen postojeće javne komutirane telefonske mreže. Veći deo komutacionih sistema (telefonskih centrala) i prenosnih sistema između centrala je digitalizovan, kako u svetu, tako i kod nas. Međutim, pretplatnički deo mreže je ostao analogan. Uvođenjem ISDN-a i pretplatnički deo mreže postaje digitalan, i to korišćenjem postojećih bakarnih parica. Ovo je svakako najbitnija činjenica - digitalna veza od kraja do kraja

preko postojeće telefonske mreže bez dodatnih ulaganja u infrastrukturu.



Slika **6.x** ISDN obezbeđuje kompletan digitalni prenos od kraja do kraja

Postoje dva tipa ISDN pristupa: bazni (BRI – *Basic Rate Interface*) i primarni (PRI – *Primary Rate Interface*). Bazni pristup podrazumeva dva B kanala (kanali po kojima se prenosi informacija) od po 64 kbit/s i jedan D kanal (kanal po kome se prenose informacije neophodne za sinhronizaciju i korisničku signalizaciju) od 16 kbit/s, što je ukupno 144 kbit/s. Namenjen je kućnim korisnicima. Primarni pristup PRI (30B+D) sadrži trideset B kanala protoka 64kbit/s za govor i prenos podataka i jedan D kanal protoka 64kbit/s za sinhronizaciju, signalizaciju i prenos podataka (ukupno 2Mbit/s), i uglavnom je namenjen za poslovne korisnike. Po istoj bakarnoj parici po kojoj je realizovan analogni telefonski priključak realizuje se i bazni priključak BRI (2B+D), dok je za primarni priključak PRI (30B+D) potrebno dve bakarne parice.

Na ISDN liniju se mogu priključiti različiti terminalni uređaji:

1. ISDN telefon
2. Terminalni adapter (TA) za priključenje postojećih analognih uređaja
3. ISDN kartice (za prenos podataka potrebna je ISDN kartica u računaru ili eksterni ISDN adapter)
4. ISDN LAN router ili bridge
5. ISDN multiplekseri
6. FAX grupe 4
7. ISDN PABX – pretplatničke (kućne) centrale ISDN tipa.

6.9. xDSL (Digital Subscriber Line)

Termin DSL (*Digital Subscriber Line*) (ili xDSL) predstavlja način prenosa digitalnih signala po bakarnim paricama većim brzinama (počev od 144 kb/s pa sve do 50 Mb/s). Inicijalno je nastao koristeći već usvojene prednosti načina prenosa iz ISDN-a (isti linijski kod i dvosmerni prenos po jednoj parici) uz povećanje ukupnog protoka do 2 Mb/s (u Americi 1,5 Mb/s) i raspodele signala na dve, ili čak tri parice, čime bi se smanjila efektivna linijska brzina i time povećao domet do 4 km, ili 6 km.

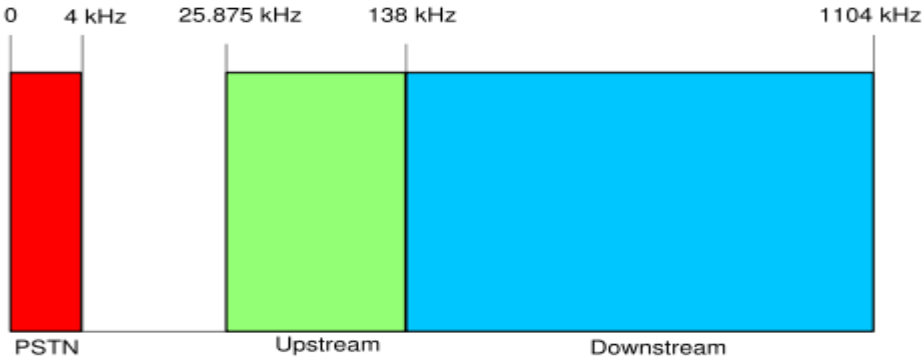
Postoji nekoliko varijanti DSL:

- Asimetrični (ADSL)
- High-bit rate (HDSL)
- Single Line (SDSL)
- Very-High-Data-Rate (VDSL)

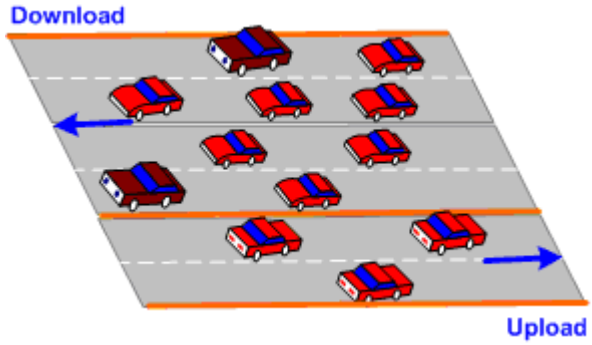
Tabela 2.32 Varijante DSL-a

xDSL tehnologija	Brzina do/od korisnika	Najveća udaljenost
VDSL	52/1.6 ili 8/8 Mbit/s	0.9 km
ADSL	8/1 Mbit/s	5.5 km
HDSL	2/2 Mbit/s	4.6 km
SDSL	784/784 kbit/s	6.9 km
IDSL	144/144 kbit/s	5.5 km
ISDN	128/128 kbit/s	5.5 km

U tehnologiji DSL-a postoji nekoliko podvrsta, međutim, ona koja se danas najčešće koristi je takozvana asimetrična digitalna pretplatnička linija (ADSL-*Asymetric Digital Subscriber Line*). Kao što joj i samo ime kaže, osnovna karakteristika ove vrste DSL realizacije je asimetričnost. Upravo ona je i čini najzanimljivijom DSL realizacijom za privatne i poslovne korisnike. Asimetričnost, zapravo, znači mogućnost mnogo bržeg prenosa podataka od mreže ka korisniku (*downstream*) nego što slanje podataka od korisnika ka mreži (*upstream*).



Slika 6.x Princip ADSL-a – podela frekvencijskog opsega



Slika 6.x Plastičan prikaz ADSL-a

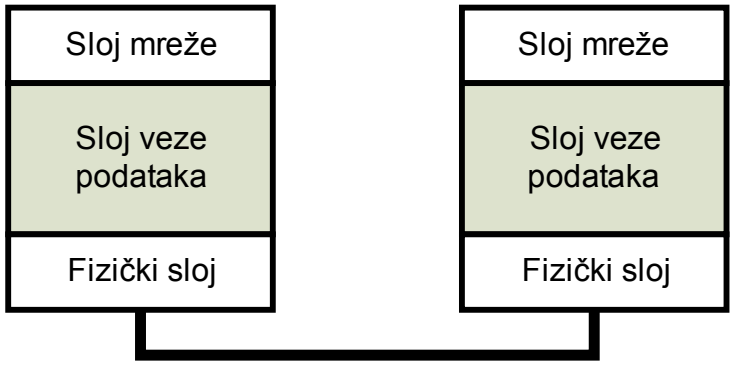
Većina najzanimljivijih aplikacija za korisnike na mreži su asimetične (video na zahtev, pristup udaljenim lokalnim mrežama, pristup Internetu, multimedijalni pristup, home shopping, itd.), gde puno više informacija korisnik uzima sa mreže nego što ih u nju šalje. Ta asimetričnost čini ADSL idealnim za ove aplikacije.

ADSL usluga je bazirana na stalnom i brzom pristupu Internetu po već postojećoj telefonskoj liniji (parici) bez njenog zauzeća ili promene telefonskog broja. Realizuje se instalacijom dva uređaja na strani korisnika gde se nalazi delitelj frekvencije(spliter) ADSL primopredajnik (ADSL modem). i može se realizovati preko obične telefonske linije ili baznog ISDN priključka. Prilikom puštanja ADSL servisa na postojeću običnu ili ISDN liniju na raspolaganju su istovremeno obe veze tj. obična ili ISDN i ADSL veza. Zahtevani tehnički uslovi su da postoji slobodna parica i da ima slobodnih resursa na uređaju u reonskoj telefonskoj centrali.

Sa ADSL-om je moguće ostvariti brzinu konekcije u rasponu od 256/64 Kb/s do 768/192 Kb/s za *download* i *upload*. Protok se definiše posebno za dolazni a posebno za odlazni saobraćaj s tim da se veći protok određuje za dolazni saobraćaj.

7. Sloj veze

Zbog mogućnosti pojavljivanja grešaka prilikom prenosa podataka, kao i potrebe za usaglašavanjem brzine prenosa podataka i sposobnosti prijemnika da prihvati pristigle podatke, neophodan je sloj koji će kontrolisati svaki uređaj u komunikaciji i obezbediti funkcije kao što su: formiranje okvira, kontrola toka podataka, detekcija i eventualno ispravljanje grešaka. Taj kontrolni sloj je poznat kao sloj veze.



Slika 7.1 Položaj sloja veze podataka

Sloj veze podataka (DL-*Layer*, *Data Link Layer*) ili sloj digitalne veze, ima zadatak da omogući pouzdan prenos podataka s jednog računara na drugi kroz fizičku vezu i pri tome treba da otkrije i ako je moguće ispravi greške nastale na fizičkom sloju. Generalno, na ovom sloju se operiše sa okvirima ili ramovima (*frames*), a u okviru njega postoji više protokola. Osnovna funkcija ovih protokola je postizanje pouzdane i efikasne komunikacije između dva susedna računara. Sloj veze podataka se naslanja na fizički sloj, a sa gornje strane on daje svoje usluge mrežnom sloju.

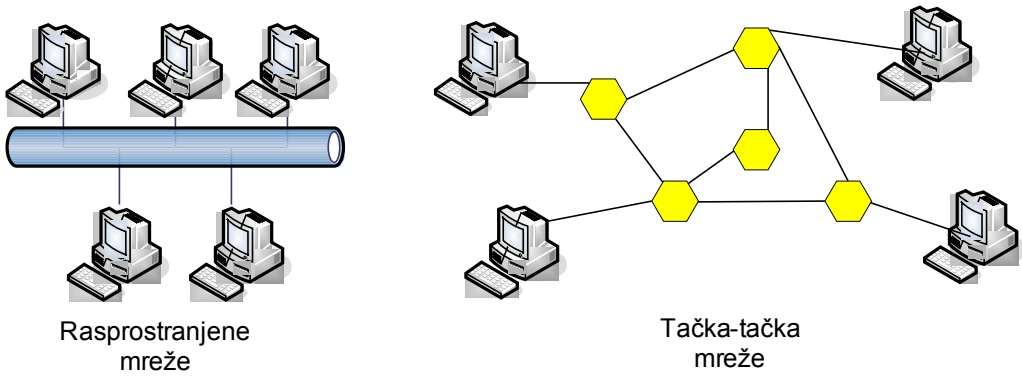
Sloj veze ima tri funkcije a to su:

- kontrola kada računar šalje podatke (kontrola pristupa medijima),
- detekcija i korekcija greške u prenosu (kontrola greške),
- određivanje početka i kraja okvira

Postoje dva tipa mreža na sloju veze podataka a to su:

- **rasprostranjene (broadcast) mreže -** jedan komunikacioni kanal koga dele svi računari u mreži

- **tačka–tačka (*point-to-point*) mreže -** postoji više veza među pojedinim parovima računara



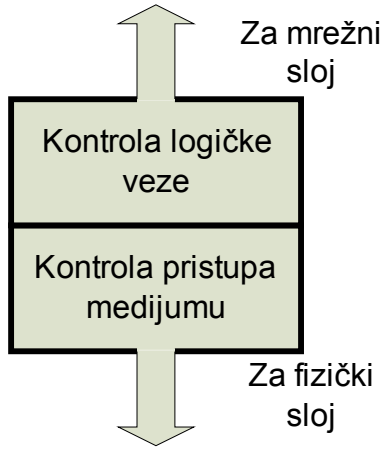
Slika 7.2 Tipovi mreža

Lokalne računarske mreže su rasprostranjene mreže a regionalne računarske mreže su tačka-tačka mreže.

7.1. Podela sloja veze

IEEE (*Institute of Electrical and Electronic Engineers*) je podelio sloj veze podataka na dva podsloja, a to su:

- podsloj kontrole pristupa medijima i
- podsloj kontrole logičke veze.



Slika 7.3 Funkcionalna podela sloja veze podataka

7.1.1. Kontrola pristupa medijimu (*Media Access Control*, MAC)

Kontrola pristupa medijimu predstavlja podsloj u sastavu sloja veze podataka referentnog modela OSI. MAC podsloj određuje ko ima pravo pristupa fizičkom sloju u bilo kom trenutku vremena. Ponaša se kao interfejs između podsloja logičke kontrole povezivanja i fizičkog sloja. Obezbeđuje pristup mrežnim medijima i sistem adresiranja, koji se koristi za prenos okvira podataka kroz mrežu. Neophodno je da se osigura da dva računara ne pokušaju da prenose podatke istovremeno, a ako se to i desi, mora da se pronađe način da se problem reši. Postoje dve suštinski različite kontrole pristupa medijima a to su:

- Kontrola pristupa i
- Pristup na osnovu sadržaja

7.1.2. Kontrola pristupa

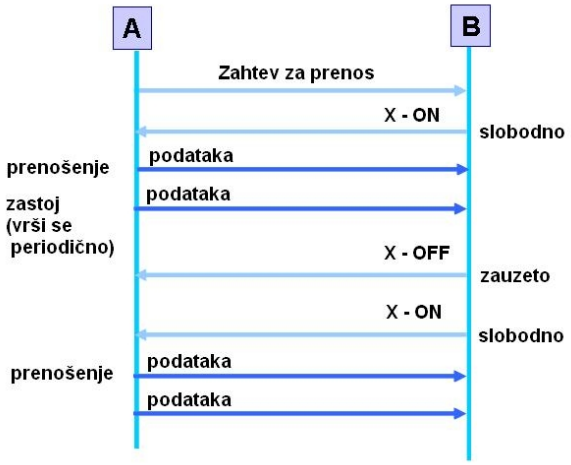
Kontrola pristupa se uobičajeno koristi na velikim računarima – (*mainframe*s)

gde veliki računari kontrolišu i određuju koja veza ima pristup glavnom računaru u datom vremenu. Koristi se u nekim LAN protokolima kao što je Token ring. Glavni metodi za kontrolu pristupa su:

- X-ON/X-OFF i
- Poliranje (*Polling*)

7.1.2.1. X-ON / X-OFF

X-ON/X-OFF predstavlja jedan od najstarijih protokola za kontrolu pristupa. Koristi se za prenos samo tekstualnih poruka. Još uvek se koristi između računara i štampača, a sreće se i u pojedinim poludupleksnim režimima rada.



Slika 7.4 Princip rada X-On/X-OFF protokola

Njegov koncept je jednostavan. Računar A šalje zahtev za prenos podataka računaru B, a računar B potvrđuje da je spreman da prima podatke slanjem X-ON signala, koji računaru A govori da započne prenos. Računar A šalje podatke računaru B sve dok B strana ne pošalje X-OFF poruku. Prenos podataka se zaustavlja sve dok strana B ne pošalje X-ON signal. Zbog lakog gubitka X-ON i X-OFF signala tokom prenosa, koriste se mnogo savršeniji pristupi, pa je sve ređa primena ovog protokola.

7.1.2.2. Poliranje

Poliranje je proces prozivanja klijenta (računara ili terminala) koji nakon

prozivanja mogu da pošalju podatke (ukoliko ih imaju). Ako klijent ima podatke šalje ih nakon prozivanja, a ako nema podatke za slanje klijent odgovara negativno, a server proziva sledećeg klijenta. Postoje dve vrste poliranja i to su:

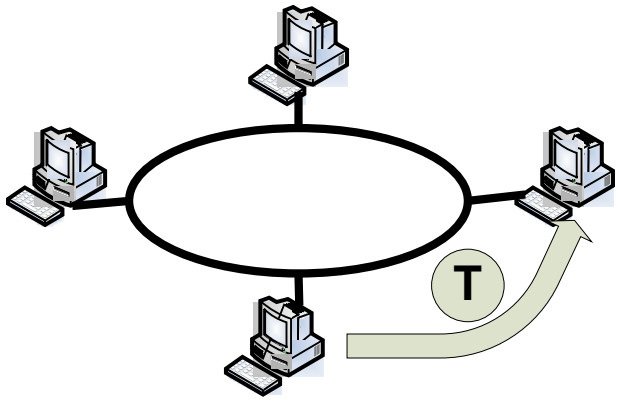
- Pozivanje po redosledu (*Roll call polling*)
- Hub polling (prosleđivanje žetona - *Token passing*)

Pozivanje po redosledu (*Roll Call Polling*)

Server testira svakog klijenta (redom i periodično po spisku) da vidi da li imaju nešto za prenos: A, B, C, D, E, A, B, … Klijenti mogu imati prioritete pa mogu biti češće prozivani npr. A, B, A, C, A, D, A, E, A, B, .. Ova vrsta prozivanja često sadrži čekanje zato što server mora da prozive klijente a zatim da čeka odgovor. Odgovor može da bude dolazeća poruka koja čeka da bude poslata ili negativan odgovor koji nagoveštava da nema šta da se pošalje. Obično je neophodan tajmer da bi se sprečilo zaključavanje kada klijent ne odgovara posle nekoliko sekundi.

Prosleđivanje žetona (*Token-passing*)

Prenošenje tokena je deterministički metod za pristup medijumu kojim se token prenosi sa čvora na čvor, prema ranije utvrđenom redosledu. Token je specijalni paket ili okvir. Jedan računar startuje poliranje i token se šalje do drugog računara. U bilo kom trenutku token može biti dostupan ili u upotrebi. Kada dostupan token stigne na čvor, taj čvor može da pristupi mreži. Tada se token šalje do sledećeg računara i tako sve dok se ne vrati do prvog računara koji ceo proces ponovo započinje. Nakon prihvaćenih podataka ciljni računar oslobađa token, on postaje dostupan, nakon čega sledeći računar može započeti predaju po prijemu dostupnog tokena.



Slika 7.x Kontrola pristupa prosleđivanjem žetona

Mrežne arhitekture koje podržavaju prenošenje tokena kao metod za pristup mreži su ARCnet, FDDI, kao i IBM-ova arhitektura Token Ring.

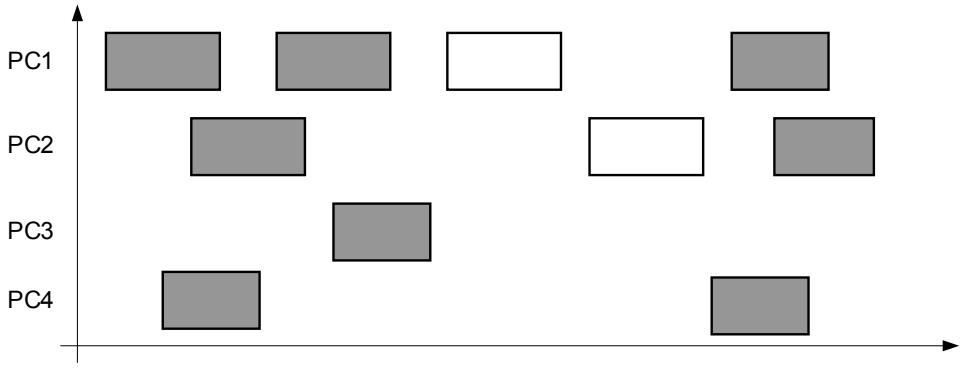
7.1.3. Pristup na osnovu sadržaja

Pristup na osnovu sadržaja je suprotan od kontrole pristupa. Računar čeka da se oslobodi komunikacioni deljeni medijum (ni jedan računar u tom trenutku ne šalje podatke), i tada započinje prenos. Obično se koristi kod Ethernet LAN-a. U njemu se mogu javiti kolizije kada više računara istovremeno šalju podatke. Osnova za savremene protokole ovog tipa je Aloha protokol. Prva verzija je bila jednostavna i sastojala se u sledećim koracima:

- ako ima podataka za prenos oni se odmah šalju,
- ako je došlo do sudara sa drugim prenosom, pokušati kasnije.

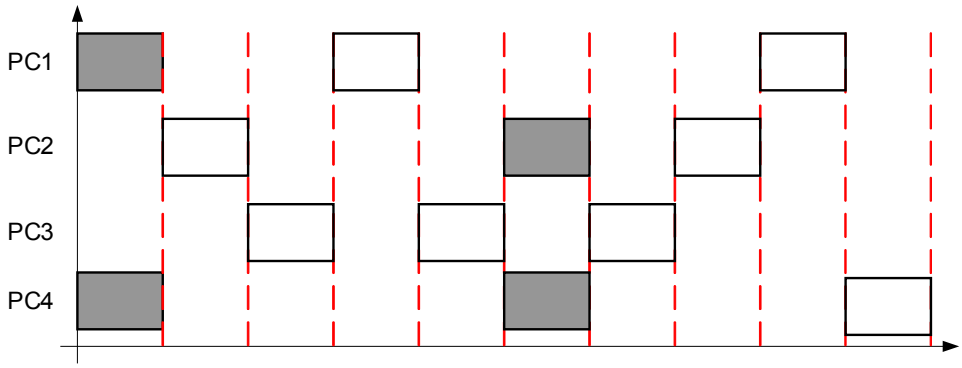
Razlika izmedju alohe i etherneta na deljenom medijumu je da ethernet koristi CSMA/CD protokol. U ovom protokolu koristi se signal da obavesti sve računare povezane na kanal da se desila kolizija, terajući računare na mreži da odbiju tekući paket ili frejm.

Čista aloha ima oko 18.4% maksimalne propusnosti. Ovo znači da je 81.6% od ukupne propusne moći mreže praktično neiskorišćeno.



Slika 7.x Čista aloha – sivo su obeleženi okviri koji propadaju

Poboljšanje originalnog aloha protokola je **vremenski raspodeljena aloha**, koja je diskretno uvela podelu vremena i povećanu propusnost od 36.8%. Stanica ne može slati bilo kad, već samo na početku deljenja vremena, i stoga je kolizija smanjena.



Slika 7.x Vremenski raspodeljena aloha – sivo su obeleženi okviri koji propadaju

Treba primetiti da se karakteristike alohe ne razlikuju puno od eterneta, Wi-Fi-a i slično zasnovanih sistema. Postoji izvesna količina prisutne neefikasnosti kod tih sistema. Na primer 802.11b dostiže stvarnu propusnu moć od 2-4 Mbit/s sa nekoliko stanica, dok je teoretska moć od 11 Mbit/s. Često se može videti da ovi tipovi mrežne propusnosti padaju dok se broj korisnika i poruka povećava.

Sa vremenski raspodeljenom alohom, centralni časovnik šalje okvire podataka do udaljenih stanica. Te stanice imaju dozvolu da odmah, po primanju tih okvira, pošalju njihove okvire. Ako postoji samo jedna stanica koja šalje okvir, garantovano neće doći do kolizije. S druge strane ako postoje dve stanice koje šalju okvire, ovaj algoritam garantuje da će biti kolizije, i ceo period do sledećeg sata je propao. Ovaj protokol uopšteno poboljšava korišćenje kanala, tako što smanjuje verovatnoću kolizije za pola. Relativno niska iskorišćenost je u stvari mala cena u odnosu na prednosti. Mala modifikacija ovog sistema za žične mreže poboljšava izbegavanje kolizije na zauzetim mrežama, i ovo je postao standard za eternet. Danas ova tenhika je poznata kao CSMA/CD. Mehanizmi za otkrivanje kolizije su mnogo teži za implementiranje kod bežičnih mreža uporedjujuci ih sa žičnim/kabliranim sistemima.

7.1.4. MAC adresa

MAC adresa je jedinstven identifikator kod mnogih oblika mrežne opreme. Većina protokola drugog sloja korisiti jednu od tri brojevne šeme upravljanih od strane IEEE:

- MAC-498,
- EUI-48 (*Extended Unique Identifier*-48),
- EUI-64,

koji su dizajnirani da budu globalno jedinstveni. Ne koriste svi kommunikacioni protokoli MAC adrese, i ne zahtevaju svi tako jedinstvene identifikatore. IEEE je položio prava na imena EUI-48, EUI-64.

Na mrežama kao što su eternet, MAC adrese dozvoljavaju svakom računaru da bude jedinstveno identifikovan i dozvoljava okvirima da budu obeleženi za specifične računare. Originalna IEEE 802 MAC adresa, sada zvanično nazvana MAC-48, dolazi iz eternet specifikacije. Otkad su originalni dizajneri eterneta predvideli korišćenje prostora adrese od 48 bita, postoji približno 2^{48} ili 281.474.976.710.656 mogućih MAC adresa.

Sva tri brojevna sistema koriste isti format, a razlika je samo u dužini identifikatora. Adrese mogu biti univerzalno ili lokalno administrirane. Univerzalne i lokalno administrirane adrese se razlikuju po podešavanju bita ispod najvažnijeg bita adrese; ako je taj bit binarno 0, adresa je univerzalno administrirana, ako je 1 onda je lokalno administrirana.

MAC-48 i EUI-64 adrese se obično prikazuju u heksadesimalnom obliku, sa svakom oktavom odvojenim kolonom ili redom. Primer MAC adrese bi bio 00-78-74-4c-7f-1d. Ako se zanemare prve tri oktave sa IEEE OUI dodelama, vidi se da je ova MAC adresa došla od *Dell Computer Corp*. Poslednje tri oktave predstavljaju serijski broj dodeljen adapteru od strane proizvođača.

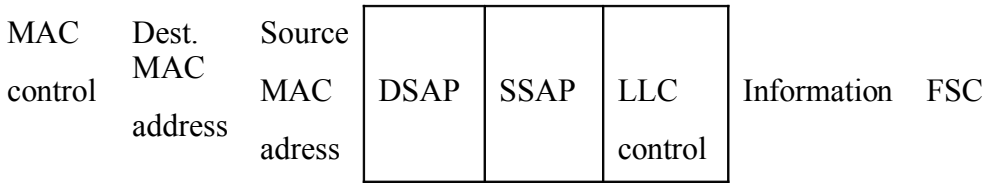
Sledeće tehnologije koriste MAC-48 format:

- Eternet
- 802.11 bezicna mreza
- Bluetooth
- IEEE 802.5 Token prsten
- većina drugih IEEE 802 mreža
- FDDI
- ATM (samo virtualne konekcije)
- SCSI i Fiber kanal

7.1.5. Kontrola logičke veze (*Logic Link Control*, LLC)

Kontrola logičke veze održava vezu između računara pošaljioca i računara primaoca, tokom prenosa podataka. Paket kontrole logičke veze se sastoji od tri polja: odredišna pristupna tačka usluge - DSAP (*destination service acess point*),

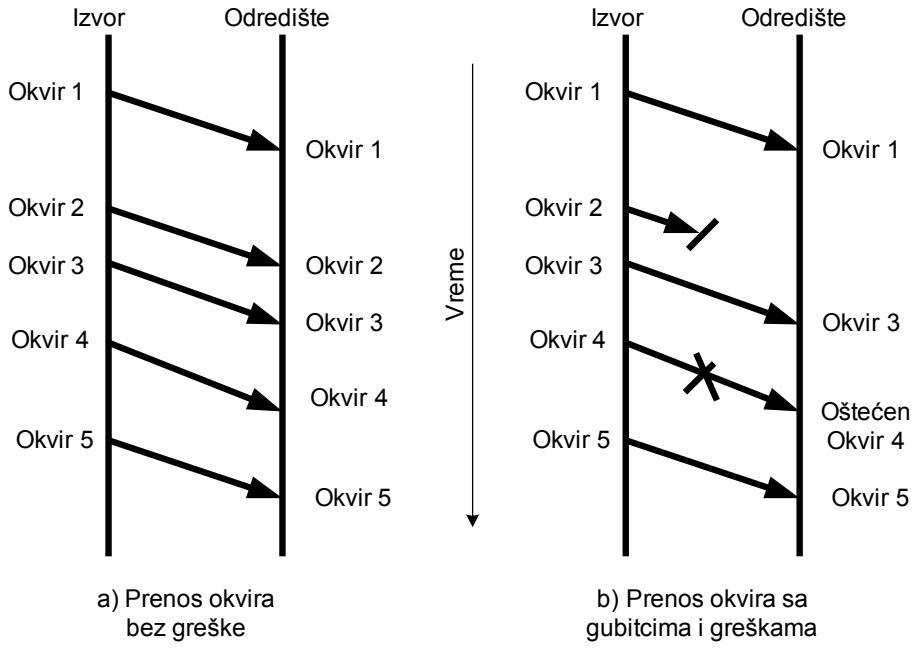
izvorišna pristupna tačka usluge –SSAP (*source service acess point*) i LLC control.



7.2. Kontrola toka

Kontrola toka je mehanizam kojim se obezbeđuje da predajnik ne "pretrpa" prijemnik sa podacima. Podacima koji se primaju obično se dodeljuje međumemorija maksimalne dužine za prenos. Kada se podaci primaju, primalac mora da obradi određen deo podataka pre nego što dođu do softvera.

Na slici se vidi mehanizam kontrole pristupa. Na slici levo, vidi se ispravan odnos slanja i primanja. Svaka strelica predstavlja jedan okvir podataka koji prolazi kroz veze podataka između dve stanice. Okviri podataka se šalju po određenom redosledu, gde svaki okvir podataka sadrži deo podatka i kontrole. Vreme koje je potrebno da se pošalju svi biti na medijum za komunikaciju se naziva vreme slanja. Vreme koje je potrebno da biti stignu od predajnika do prijemnika kroz komunikacioni medijum se naziva vreme propagacije. Za sada, prihvata se tačnim da su svi okviri podataka, koji su se prenosili, uspešno primljeni; nijedan se nije izgubio i nijedan nije stigao sa greškama. Osim toga, stizali su po istom redosledu kao što su poslati. Ipak svaki okvir podataka proizvoljno kasni pre prijema.



Slika 7.x Prenos okvira od izvorišta do odredišta

7.3. Kontrola greške

Kontrola greške se odnosi na mehanizme koji detektuju i ispravljaju greške koje se javljaju prilikom prenošenja podataka. Postoji mogućnost pojavljivanja dva tipa grešaka i to: promenjen podatak i izgubljen podatak. Greške u mreži mogu da se dese svakih 5 sati, minuta ili sekundi zbog šuma na liniji. Nijedna mreža ne može da odstrani greške, ali većina grešaka može biti sprečena, otkrivena i eventualno ispravljena. Nivo greške predstavlja jedan pogrešan bit na *n* poslatih bita (npr 1 na 500000). Greške se obično pojavljuju u grupama. U grupnim greškama, više bita je narušeno u isto vreme, i greške nisu uniformno raspoređene. Osnovne funkcije kontrole greške su:

- Sprečavanje grešaka;
- Detekcija grešaka i
- Ispravljanje grešaka.

7.3.1. Izvori grešaka

Osnovni uzroci izvora grešaka su šum na liniji i degradacija signala. Šum je nepoželjan električni signal koji se nalazi negde između prenosa i prijema podataka. Može se očekivati na električnim medijima gde se pojavljuje kao neočekivan električni signal. Manifestuje se na dva načina i to: dodatni biti – umetanje ili nedostajući biti – brisanje.

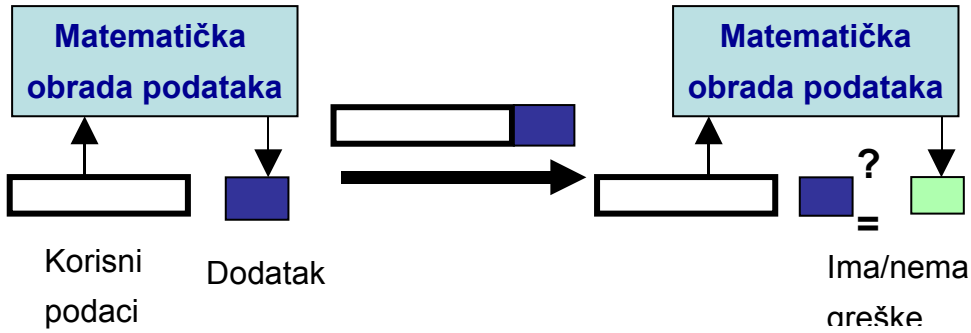
Postoji više vrsta izvora grešaka a to su:

- **Prekid linije –** je katastrofalan uzrok greške i nemoguć je prenos. Često, prekidi se dešavaju na kratko vreme. Ovaj tip greške mogu da uzrokuju greške uređaja, spoljnog prekida, gubitak nosećeg signala i sl.
- **Beli Gausov šum –** nastaje kod svih električnih signala. On ne predstavlja problem sve dok ne postane toliko jak da nadvlada proces prenosa podataka. Kao prevencija, povećava se snaga signala.
- **Impulsni šum** – je osnovni uzrok grešaka prilikom prenosa podataka. Može da traje $^{1}/_{100}$ sekunde. Uzrokuju ga nagle promene struje, a kao prevencija se vrši oklapanje kablova i eventualno njihovo izmeštanje.
- **Preslušavanje –** uzrokuju ga bliski kablovi i nedovoljno razmaknuti opsezi frekvencija. Kao prevencija povećava se frekvencijski opseg signala i vrši se izmeštanje kablova.
- **Eho –** uzrokuju ga loše veze gde se signal reflektuje (vraća) do izvorišta**.** Kao prevencija proveravaju se konektori ili podešavaju uređaji.

- **Slabljenje** – je gubitak jačine signala dok putuje od prijemnika do predajnika. Povećava se sa rastojanjem, a kao prevencija se upotrebljavaju ripiteri ili pojačivači.
- **Intermodulacioni šum** – u njemu signali iz dva kola se spajaju i stvaraju nov signal koji upada u frekvenciju koja je rezervisana za drugi signal. Uzrokuje ga signal nastao kombinacijom iz više prenosnih sistema a kao prevencija upotrebljavaju se oklopljeni kablovi i vrši se njihovo izmeštanje.
- **Džiter** – uzrokuje promena analognih signala (amplituda, frekvencija, faza) a kao prevencija se vrši podešavanje uređaja.
- **Harmonijska izobličenja** – uzrok su pojačivači koji menjaju fazu (nekorektno pojačanje ulaznog signala) a kao prevencija se takođe vrši podešavanje uređaja.

7.3.2. Detekcija greške

Kod detekcije greške pošiljalac izračunava dodatak i šalje ga zajedno sa korisnim podacima. Kad se poveća dužina korisnih podataka, bolja je detekcija greške ali je manja efikasnost prenosa. Primalac izračunava dodatak i poredi ga sa dobijenim. Ako je dodatak isti kao što ga je pošaljilac izračunao, nema greške u prenosu, a ako je različit postoji greška u prenosu.



Slika 7.x Tehnika detekcije greške

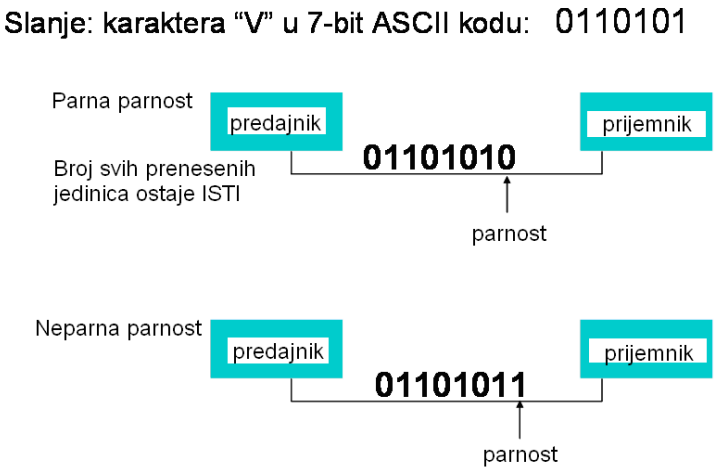
Tehnike za detekciju greške su:

- Provera parnosti
- Longitudinalna redudantna provera (Longitudinal Redundancy Checking, LRC) i

- Polinomijalna provera (Checksum, Cyclic Redundancy Check (CRC)).

7.3.2.1 Provera parnosti

Provera parnosti predstavlja najstariji i najednostavniji metod detekcije greške pri kome se jedan bit dodaje svakom karakteru. Ako karakter ima jednak broj jedinica to se naziva parna parnost (*even parity*), a ako ima neparan broj jedinica to je neparna parnost (*odd parity*). Prijemnik prima i ponovo računa bit parnosti pri čemu se može uočiti neparan broj pogrešnih bita. Iako je jednostavan metod, detektuje se oko 50% grešaka. Primena provere parnosti nije jednostavna, kad su šumovi često dovoljno dugi da mogu da unište i više od jednog bita, posebno pri velikim brzinama prenosa podataka.

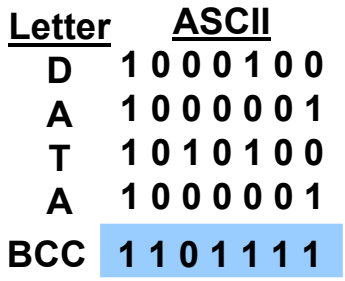


Slika 7.x Provera parnosti

7.3.2.2 Longitudinalna provera redudanse

Kod longitudinalne provere redudanse dodaje se jedan dodatni karakter, koji se zove karakter za svaki blok podataka, na kraju cele poruke ili paketa podataka. Vrednost tog karaktera se određuje isto kao kod provere parnosti, ali se računa duž cele poruke kao i vertikalno kroz svaki karakter. Prvi bit longitudinalne provere redudanse se određuje brojanjem broja jedan kao prvog bita svih karaktera u poruci i postavljanjem prvog bita kao nula ili jedan što zavisi od toga da li je zbir paran ili neparan. Drugi bit se određuje izračunavanjem broja 1 u

drugom bitu karaktera u poruci i tako dalje se izračunavaju svi bitovi karaktera za svaki blok podataka. Ima lošije karakteristike za detekciju pojedinačno pogrešnih bita, ali predstavlja mnogo bolju proveru od jednostavne parnosti.



Slika 7.x Princip longitudinalne provere parnosti

7.3.2.3 Polinomijalna redudantna provera

Kod polinomijalne redudantne provere dodaje se jedan ili serija karaktera, zasnovanih na matematičkom algoritmu, na kraj poruke. Postoje dva tipa ovakve provere a to su:

- Ciklična redudantna provera (Cyclic Redundancy Check, CRC) i
- Kontrolna suma (Checksum)

Ciklična provera redudanse - Cyclic Redundancy Check (CRC)

CRC je rezultat matematičkog izračunavanja, koje se stavlja u prateći zapis okvira podataka. Ona dodaje poruci 8, 16, 24 ili 32 bita. Poruka se tretira kao jedan dug binaran broj. Pre prenosa, sloj veze podataka deli P sa fiksnim binarnim brojem G i kao rezultat daje ceo broj Q i ostatak R/G. Izračunava se i na polaznom i na odredišnom računaru. Dakle, ciklična provera redudanse se određuje izračunavanjem sledećeg ostatka:

$$P / G = Q + R / G$$

Ostatak R se dodaje poruci kao karakter za proveru greške pre prenosa. Prijemnik deli primljenu poruku sa istim G, što za rezultat daje R. Prijemnik proverava da li se primljeno R slaže sa stvarnim R. Ako se ne slažu, smatra se da je došlo do greške.

Ona predstavlja najjaču i najviše upotrebljavanu proveru i sa njom se detektuje 100% grešaka ako je broj grešaka manji ili jednak od veličine R.

Kontrolna suma

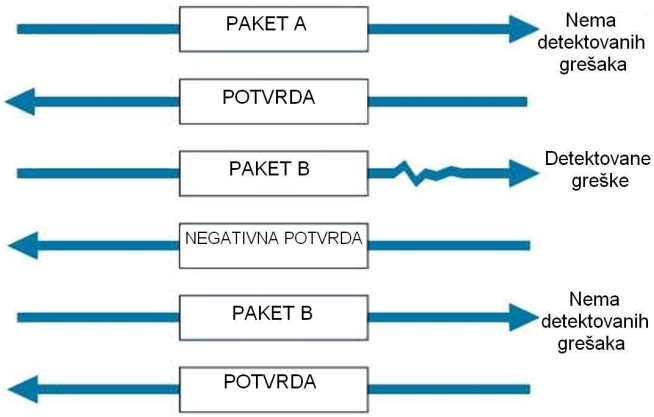
Kontrolna suma predstavlja kod detekcije greške zasnovan na operaciji sabiranja koja se vrši nad bitovima koji trebaju da se provere. Izračunava se sabiranjem decimalnih vrednosti svakog karaktera u poruci, ukupna vrednost se zatim deli sa 255 a ostatak deljenja (1 bajt) je kontrolna suma. Efikasnost kontrolne sume je 95%.

7.3.3. Korekcija greške

Jednom kada se detektuje greška, ona mora da se ispravi. Jednostavan, efikasan, jeftin i najčešće u upotrebljavani metod za korekciju greške je retransmisija.U njoj, prijemnik, kada detektuje grešku, traži od predajnika da ponovo pošalje poruku sve dok se poruka ne primi bez greške. Čest naziv je automatski zahtev za ponavljanje (*Automatic Repeat Request, ARQ*). Postoje dva tipa ARQ a to su: stani i čekaj i kontinualni ARQ.

7.3.3.1. Stani i čekaj automatski zahtev za ponavljanje

U stani i čekaj automatskom zahtevu za ponavljanje predajnik staje i čeka odgovor od prijemnika za svaki paket podataka. Posle prijema paketa, prijemnik šalje ili potvrdu ako je paket primljen bez greške, ili negativnu potvrdu, ako poruka sadrži grešku. Ako primi negativnu potvrdu, predajnik ponovo šalje prethodnu poruku. Ako primi potvrdu, predajnik nastavlja da šalje sledeću poruku. Po definiciji, ovo je poludupleksna tehnika prenošenja.

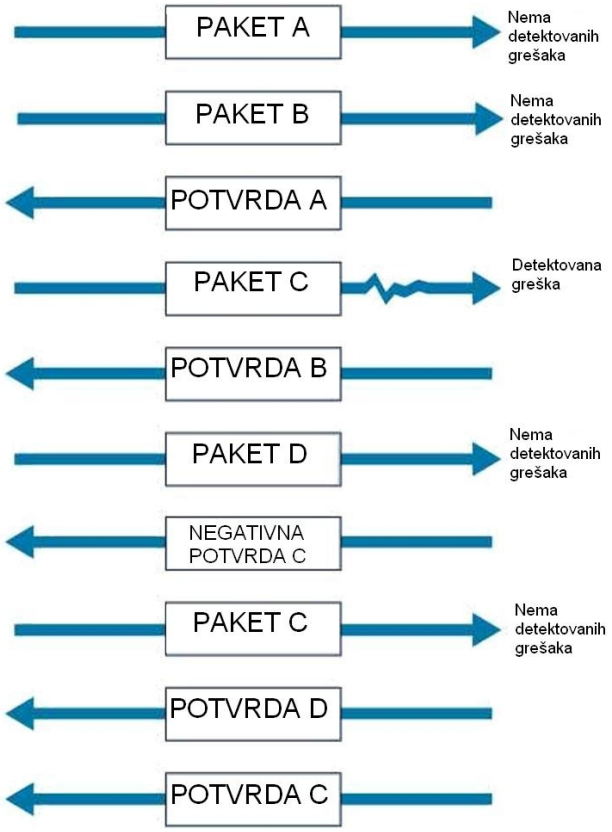


Slika 7.x Korekcija greške postupkom Stani i čekaj

7.3.3.2. Kontinualni automatski zahtev za ponavljanje

U ovom procesu predajnik ne čeka potvrdu pre nego što pošalje poruku, odmah

šalje sledeću poruku. Iako su poruke poslate, predajnik ispituje povratne potvrde. Ako dobije negativnu potvrdu, predajnik ponovo šalje potrebne poruke. Paketi koji se ponovo šalju mogu biti samo one poruke koje sadrže grešku ili može da bude prvi paket sa greškom i svi paketi posle njega.



Slika 7.x Korekcija greške kontinialnim postupkom

7.3.3.3. Korekcija greške unapred (*Forward Error Correction*)

Korekcija greške unapred koristi kodove koji sadrže dovoljno redudanse da spreče greške detektovanjem i ispravljanjem istih pri prijemu bez ponovnog slanja originalne poruke. Dodatni biti variraju od malog procenta ekstra bitova do 100% redudanse, sa brojem detektovanih grešaka koji su okvirno jednaki broju bitova podatka. Obično se koristi za satelitske komunikacije. Primer za korekciju greške unapred je *Hamming code*. Ako se promeni bilo koji bit (parity ili data) može se detektovati i promeniti baš taj bit.

7.4. Protokoli na sloju veze - Data Link Protocols

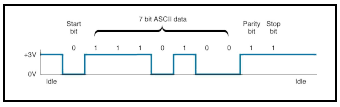
Protokoli na sloju veze se dele na:

- Asinhroni prenos
- Sinhroni prenos

Razlikuju se prema zapisu, dužini i strukturi rama.

7.4.1. Asinhroni prenos

Kod asinhronog prenosa, predajnik može da prenese karakter kad god je to zgodno a prijemnik će primiti taj karakter. Da bi se karakter odvojio, mora da se utvrde početni bit, poslednji bit i oni su obično suprotni. Pri prenosu, svaki karakter se šalje nezavisno od drugih karaktera. Kada predajnik čeka da korisnik ukuca sledeći karakter, nijedan podatak se ne šalje. Prijemnik mora da zna brzinu po kojoj prima bitove da bi mogao da *sempluje* liniju na regularne intervale i utvrdio vrednost svakog primljenog bita. Dve tehnike se obično koriste u ovu svrhu a jedna od njih je asinhroni prenos. U njemu, svaki karakter podatka se obrađuje posebno. Svaki karakter počinje sa početnim bitom koji nagoveštava prijemniku da karakter stiže. Prijemnik *sempluje* svaki bit karaktera i tada traži početak sledećeg karaktera. Ova strategija se koristi da bi se izbegao problem sa vremenom da se ne bi poslali dugi, prekinuti tokovi bita. Svaki karakter se šalje nezavisno, gde je svaki dužine od pet do osam bita. Asinhroni prenos se ponekad naziva start-stop prenos. Koristi se u point-to-point full duplex mrežama (mreže koje imaju samo dva računara).



Slika 7.x Asinhroni prenos karaktera

7.4.1.1. Asinhroni prenos fajlova

Protokoli su napravljeni da bi preneli podatke bez greške između dva računara i da bi se podaci podelili u grupe i tako prenosili istovremeno. Ovaj protokol je napravljen za asinhrone point-to-point mreže, koje su tipične za telefonske linije uz primenu modema. Popularni FTP protokoli su:

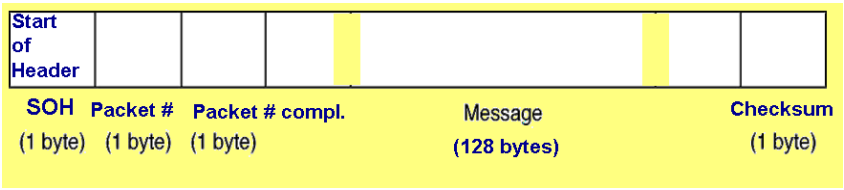
1. Xmodem
2. Zmodem
3. Kermit

Xmodem

Xmodem protokol uzima prenesene podatke i deli ih na blokove. Svaki blok ima početni karakter, broj od jednog bajta, 128 bajtova podatka i jedan bajt kontrolne sume za proveru greške. Ovaj protokol se često koristi za komunikacije između glavnog (master) i ostalih računara. Koristi stani i čekaj automatski zahtev za ponavljanje.

Xmodem-CRC poboljšava tačnost detekcije greške Xmodem protokola. On zamenjuje kontrolnu sumu sa jednim bitom ciklične provere redudanse.

Xmodem-1K koristi blokove podataka od 1024 bajtova umesto blokova od 128 karaktera.



Slika 7.x Okvir podataka kod Xmodem protokola

Zmodem

Zmodem ima osobine nekoliko protokola. Koristi CRC-32 metod detekcije greške sa kontinualnim automatskim zahtevom za ponavljanje. On dinamički prilagošava veličinu paketa u zavisnosti od uslova komunikacije da bi povećao efikasnost.

Kermit

Kermit je vrlo poularan protokol koji koristi pakete od 1000 bajtova ili stani i čekaj ARQ ili kontinualni ARQ. Koristi CRC-24 i dužine poruke za prenos od 1K, ali se može podešavati. Čak koristi programe sa kodovima od sedam ili osam bita da bi omogućio transfer sa proverom greške.

7.4.2. Sinhroni prenos

Kod sinhronog prenosa, svaki karakter podatka se šalje istovremeno kao blok podatka. Blokovi se još zovu ramovi ili paketi, što zavisi od protokola ali im je značenje isto. U njemu se mora označiti početak i kraj celog paketa. Uobičajeno se koristi kod multipoint mreža.

Obeležavanje početka i kraj svakog paketa se obično vrši dodavanjem sihronizacionog karaktera. Zavisno od protokola, mogu da budu između jednog i osam karaktera. Tada predajnik šalje dugi niz podataka koji mogu da sadrže

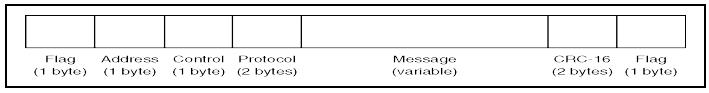
hiljade bita. Ako zna koji kod se koristio, prijemnik broji odgovarajući broj od prvog karaktera. Zatim broji bite drugog karaktera i tako dalje.

Sinhroni prenos znači da se celi blokovi podataka prenose kao paketi pošto se predajnik i prijemnik sinhronizovani. Postoji mnogo protokola za sinhroni prenos. Dele se na tri široke kategorije a to su:

- protokoli orijentisani na bajtu (PPP),
- protokoli orijentisani na bitu (SDLC, HDLC) i
- protokoli u kojima se broje bajtovi (Ethernet).

7.4.2.1. Protokol od tačke do tačke (*Point-to-point Protocol*)

Protokol od tačke do tačke je razvijen početkom 1990-tih i obično se koristio za dial-up linije sa kućnih računara. Dizajniran je da prenosi podatke preko telefonske linije ali sadrži i adresu tako da može da se koristi i na multipoint mrežama. Polja adresa i kontrola se koriste prilikom trajanja bilo koje konekcije (npr. telefonskog poziva). Polje protokol opisuje protokol na mrežnom nivou (TCP/IP, IPX/SPX). Poruka može da bude dužine i do 1500 bajtova. Protokol od tačke do tačke koristi CRC-16 za kontrolu greške.



Slika 7.x Okvir podataka kod PPP protokola

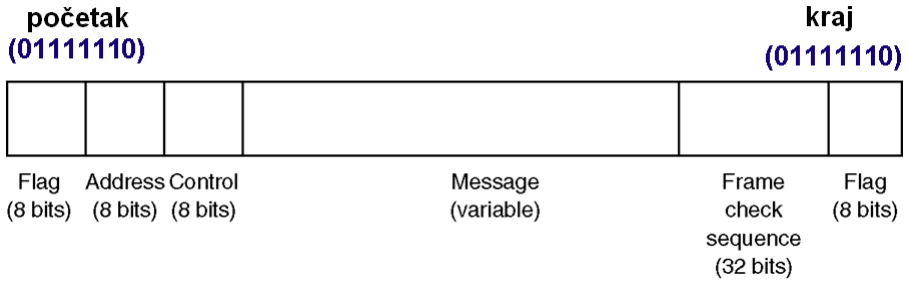
7.4.2.2. SDLC - *Synchronous Data Link Control*

Razvijen je 1972. godine i danas je u upotrebi. On je protokol orijentisan ka bitu zato što podaci u okvirima ne moraju da budu osmobitni. Tipični SDLC paket počinje i završava se sa specijalnim nizom bitova 01111110. Polje adrese utvrđuje odredište. Dužina polja adrese je obično 8 bita ali može da bude i 16 bita: svi računari na istoj mreži moraju da imaju istu dužinu bita. Polje kontrole identifikuje tip podatka koji se prenosi a podaci mogu biti:

- **podaci-informacije** (prenos podataka za krajnje korisnike) i
- **supervizorski** (prenosi potvrde (pozitivne i negativne).

Polje poruke je promenljive dužine. Kod za proveru paketa je 32-bitni CRC (neke starije verzije koriste 16-bitni CRC). SDLC ima problem transparentnosti gde korisni podaci mogu da sadrže isti niz bita koji postoje u flegu (01111110). Prijemnik bi mogao tada da ih interpretira kao kraj rama, i da ignoriše ostatak.

Rešenje se nalazi u zameni bita. Predajnik dodaje jednu nulu uvek kada detektuje pet jedinica i nastavlja sa prenosom. Svaki put kada prijemnik spazi pet uzastopnih jedinica testira sledeće bite koje prati nula (111110) automatski briše nulu i nastavlja započeti proces. Obrnuto, ako je jedan kraj rama (111111) moći će da prepozna drugu nulu kao početak sledećeg rama. Ako se slučajno desi da se ram završava sa 11, sigurno je došlo do greške jer ne može biti sedam jedinica.



Slika 7.x Okvir podataka kod SDLC protokola

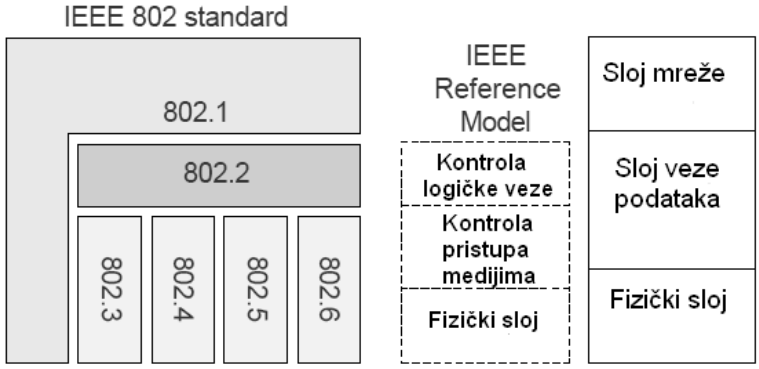
7.4.2.3. HDLC - *High-level Data Link Control*

Kontrola veze podataka visokog nivoa je praktično isti kao kontrola sinhrone veze podataka samo što ima duže adrese i kontrolna polja i ima veći klizeći prozor. Predstavlja osnovu za većinu drugih protokola na sloju veze kao što su:

1. **LAP-B** (*Link Accedes Protocol* – balansirani) - Koristi se u X.25 tehnologiji
2. **LAP-D** (*Link Accedes Protocol* – balansirani) - Koristi se kod ISDN-a
3. **LAP- F** - Koristi se kod *Frame Relay*-a

7.4.3. Ethernet

Eternet je najšire korišćen LAN protokol razvijen od strane Bob Metcalfe 1973. godine a koji su zajedno razvili Digital, Intel i Xerox 1970 godine. On je protokol orijentisan na brojanje bajtova (sadrži polje koje određuje dužinu poruke paketa). Za razliku od SDLC-a i HDLC-a nema problem transparentnosti. Svaki bit može biti prenesen zato što Eternet koristi polje koje sadrži broj bajtova. Primenjuje pristup medijumu na osnovu sadržaja.



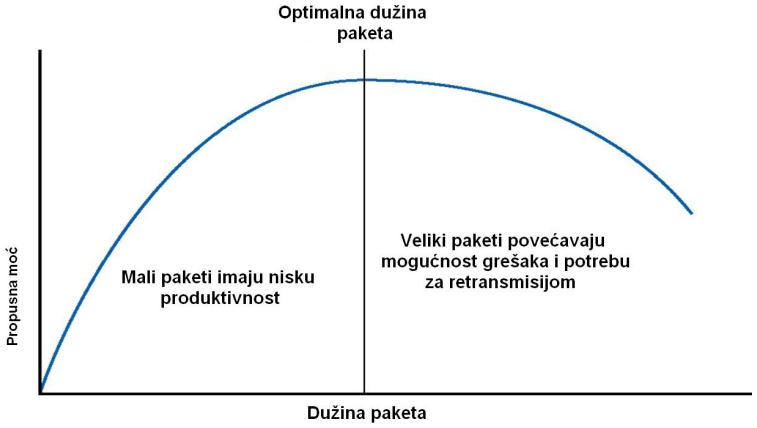
Slika 7.x Skup Ethernet protokola

Paket eterneta počinje sa uvodnim delom koji sadrži 7 bajtova i obično je oblika 10101010. Iza ovoga se nalazi bajt koji pokazuje početak paketa. Odredišna adresa određuje adresu primaoca, kao što početna adresa označava adresu pošaljioca. Dužina označava broj bajtova u poruci. VLAN se koristi se za virtualne LANove; ako nema vLAN-a, polje se izostavlja, a ako se koristi prva 2 bajta imaju vrednost: 24,832 (8100H). DSAP i SSAP se koriste za razmenu kontrolnih informacija, npr. tip protokola na mrežnom nivou (TCP/IP, IPX/SPX). Polje kontrola se koristi za prebrojavanje potvrda kao i negativnih potvrda. U većini slučajeva, kontrola je duga 1 bajt. Maksimalna dužina poruke je 1500 bajtova. Paket se završava sa CRC-32 za proveru paketa.

Slika 7.x Format Ethernet okvira

7.5. Efikasnost prenosa

Cilj kod računarskih mreža je da prenesu maksimalan broj tačnih informacija sa minimalnom greškom. Što je veći broj prnetih podataka, veća je efikasnost mreže. Svaki protokol ima informacione bite (informacija za korisnika) i dodatne bite(svrha je u proveravanju greške, formiranju okvira...). Efikasnost prenosa se definiše kao količnik ukupnog broja info bita za prenos i ukupnog broja korisnih bita za prenos. Pretpostavimo da koristimo 7-bitni ASCII, da imamo jedan bit za parnost i jedan početni kao i jedan krajnji bit. Efikasnost prenosa je 70%. Što je veća dužina poruke bolja je efikasnost mada veliki paketi mogu da imaju znatno više grešaka jer su verovatne retransmisije čime se slabi se efikasnost prenosa.



Slika 7.x Efikasnost prenosa

Propusna moć je ukupan broj primljenih infomacionih bita u jednoj sekundi. Manji paketi obezbeđuju veću propusnu moć za prenose sa više grešaka, a veći paketi obezbeđuju veću propusnu moć za prenose sa manje grešaka na mreži. Izračunavanje propusne moći zavisi od efikasnosti prenosa, nivoa greške i broja retransmisija.

7.6. Ethernet

Ethernet (IEEE 802.3 ili ISO 80802-2) predstavlja najčešće korišćeni standard kod savremenih LAN mreža. Ovaj standard je inicijalno razvijen kao *de facto* standard od strane kompanija DEC, Xerox i Intel a kasnije je formalizovan od strane IEEE kao IEEE 802.3.

7.6.1. Ethernet (IEEE 802.3)

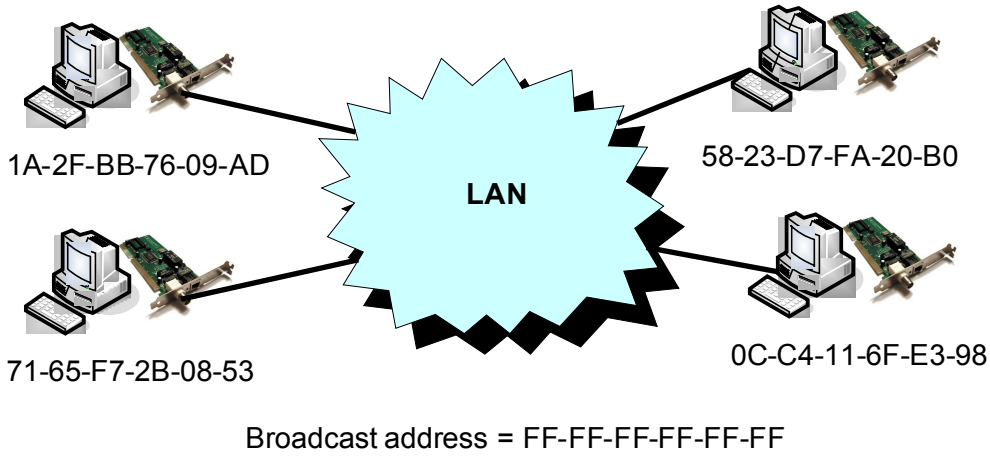
Ethernet je najpopularniji standard za umrežavanje računara u lokalne mreže. Široko je prihvaćen od strane proizvođača računarske mrežne opreme. Ethernet standard je prvi put objavljen 1985. formalnim nazivom IEEE 802.3 - *Carrier Sense Mutiple Access with Collision Detection* (CSMA/CD) *Access Method and Physical Layer Specifications*. Ovim standardom se definiše višestruki pristup prenosnom medijumu proverom nosioca signala metodom detekcije sudara. Hronološki se standard prvo odnosio na upotrebu koaksijalnih kablova (debeli i tanki) i za brzine prenosa od 10 Mb/s, a zatim je proširivan da bi podržao nove medije za prenos podataka (npr. UTP kablovi), kao i novi skup specifikacija koje podržavaju 100 Mb/s brzi Ethernet (*Fast Ethernet*), a kasnije i gigabitni Ethernet. Danas se standard 802.3 odnosi isključivo na fizički sloj i sloj veze podataka OSI modela.

Ethernet mreža je lokalna mreža koja prenosi podatke između Ethernet stanica. Adapter (interfejs) koji omogućava povezivanje računara ili nekog drugog uređaja na mrežu je mrežna kartica. Za mrežnu karticu postoji više naziva koji se u praksi ravnopravno koriste - Ethernet adapter, mrežni adapter, LAN adapter, LAN kontroler, komunikaciona kartica, *Network Interface Card* - NIC. Rad mrežne kartice kontroliše upravljački softver – drajver (*driver*) koji se izvršava u računaru. Svaki uređaj sa ugrađenim Ethernet adapterom koji učestvuje u mrežnom saobraćaju zove se Ethernet stanica. Ethernet stanice su povezane na zajednički (deljeni) komunikacioni medijum. Ethernet signali se kroz medijum šalju serijski, bit po bit. Svaka Ethernet stanica učestvuje u mrežnom saobraćaju samostalno - nezavisno od ostalih stanica na mreži.

Na sloju veze podataka OSI modela *Ethernet* koristi metod CSMA/CD. *Multiple Access* znači da su svi računari povezani na jedan zajednički medijum kome pristupa više računara. *Carrier Sense* označava da pre emitovanja podataka računar proverava - osluškuje medijum da bi utvrdio da li neki drugi računar već emituje podatke. Ako u medijumu vlada tišina (ne emituje neka druga stanica) tek onda računar počinje da šalje podatke. *Collision Detection* znači da u slučajevima kada dve stanice počnu istovremeno da emituju podatke i dođe do sudara (kolizije) postoje mehanizmi za otpočinjanje ponovnog slanja istih podataka.

Svaki Ethernet okvir mora da sadrži: zaglavlje, podatke koje prenosi i kontrolne podatke. Ethernet okvir je maksimalne dužine 1518 bajtova. Preambula je karakterističan niz 101010101010. koji označava početak okvira. Ethernet okvir sadrži (MAC) – fizičke adrese izvorišta i odredišta. Svaka Ethernet mrežna kartica ima fabrički određenu *Ethernet* (MAC) adresu koja se nikada ne može ponoviti, tj. ne postoje dve različite mrežne kartice sa istom MAC adresom. Polje rezervisano za adresu odredišta sadrži adresu primaoca; koja može biti i takozvana *multicast* adresa kada se podaci šalju za grupu računara ili *broadcast* adresa koja se koristi kada je potrebno da se paket prenese svim ostalim Ethernet stanicama u lokalnoj mreži. U normalnom radu Ethernet adapter prima samo pakete koji u polju adrese primaoca imaju njegovu vlastitu adresu ili adresu koja predstavlja *broadcast* ili *multicast* adresu. Sve ostale Ethernet pakete kartica osluškuje ali ih ne prima jer su namenjeni nekom drugom računaru koji se nalazi u istoj lokalnoj mreži. Ethernet adapter može biti setovan da prima sve pakete koji se pojavljuju u medijumu. Moguće je snimati saobraćaj u mreži i kasnije analizirati događaje sa ciljem da se utvrdi nepravilnost u radu neke kartice ili računara. Ova osobina može da se koristi i za prisluškivanje saobraćaja na mreži što treba uzeti u obzir kada je važna sigurnost podataka koji se prenose kroz mrežu.

Dva bajta nakon MAC adresa određuju dužinu podataka koji se prenose u Ethernet okviru ili to može biti tip protokola na višim slojevima. Maksimalna dužina podataka koji se prenose u Ethernet paketu je 1500 bajtova a sam sadržaj je prepušten mrežnom sloju. Na kraju Ethernet paketa su kontrolni podaci - CRC (*Cyclical Redundancy Check*). Kontrolni podaci služe za detekciju greške koja može da se javi u toku prenosa Ethernet paketa preko fizičkog sloja. Princip detekcije greške je zasnovan na matematičkoj operaciji koja se izvodi nad celim Ethernet paketom. Rezultat matematičke operacije predstavlja kontrolni podatak (CRC). Kada paket stigne na odredište, ista matematička operacija se izvrši ponovo pa ako rezultat nije identičan sa CRC podatkom upisanim na kraju Ethernet paketa - detektovana je greška u prenosu Ethernet paketa. Ethernet stanica koja primi paket i detektuje grešku u prenosu odbacuje paket. Problem izgubljenih podataka u mrežnom saobraćaju rešava transportni sloj (četvrti sloj po OSI modelu) ili sama aplikacija koja prima paket.



Slika 7.x Mrežna kartica sadrži jedinstvenu MAC adresu

Originalni Ethernet sistem radi na 10 Mbps i postoje četiri vrste medijuma za prenos signala definisanih Ethernet standardom:

- 10Base5 - debeli koaksijalni kabal,
- 10Base2 - tanki koaksijalini kabal,
- 10Base-T - upredene parice,
- 10Base-F – optički kabl.

Skraćenice predstavljaju trodelnu informaciju. Prvi deo - 10 - označava da sistem radi brzinom od 10 Mb/s. Reč Base znači *baseband* – tj., da se prenos vrši u osnovnom opsegu (a ne u nekom transformisanom). Treći deo oznake upućuje na vrstu segmenata ili njegovu maksimalnu dozvoljenu dužinu. Broj 5 označava, maximalnu dozvoljenu dužinu segmenta od 500m. Oznake T i F označavaju vrstu medijuma – "*twisted-pair"* i "*fiber optic"*.

Dopuna postojećeg standarda, gde je brzina prenosa povećana sa 10 na 100 Mb/s, je brzi Ethernet sa oznakom 802.3u, a njegovo originalno kabliranje je:

- 100Base-T4 – UTP kabl 3. kategorije za rastojanja do 100 m,
- 100Base-TX – UTP kabl 5. kategorije za rastojanja do 100 m,
- 100Base-FX – Optički kabl za rastojanja do 2000 m,

Standard za gigabitni Ethernet potiče iz 1998. godine sa oznakom 802.3z. Po ovom standardu gigabitni Ethernet se sastoji samo od dva međusobno povezana računara. Ako se povezivanje vrši preko switch-a, jedan računar predstavlja jedan

domen kolizije, tako da nije moguće sudaranje podataka. IEEE je 2002. godine standardisovao Ethernet za brzinu od 10 Gb/s – 802.3ae. Kabliranje gigabitnog Etherneta:

- 1000Base-SX – Optički kabl, multimodno vlakno, max 550 m,
- 1000Base-LX – Optički kabl, monomodno vlakno, max 5000 m,
- 1000Base-CX – STP kabl, dve parice, max 25 m,
- 1000Base-T – UTP kabl 5. kategorije, četiri parice, 100m.

7.6.2. Osnovni principi Ethernet-a

Osnovna logička topologija Ethernet mreže jeste topologija magistrale (iako je fizička topologija najšeće u obliku zvezde) što znači da su svi čvorovi mreže povezani putem half-duplex veze i da podaci upućeni od jednog čvora stižu do svih ostalih čvorova. Mrežni uređaj koji omogućava ovakvu logičku topologiju jeste *hub*.

Svi čvorovi prihvataju sve podatke sa mreže i utvrđuju da li su podaci njima namenjeni. Ukoliko jesu nastavlja se sa njihovim procesiranjem a ukoliko nisu podaci se odbacuju. Osim što ovakav način prosleđivanja podataka nepotrebno opterećuje članove kojima podaci nisu upućeni, on predstavlja i bezbednosnu pretnju s obzirom na to da omogućava jednostavno snimanje ukupnog saobraćaja u mreži.

7.6.3. Switched Ethernet

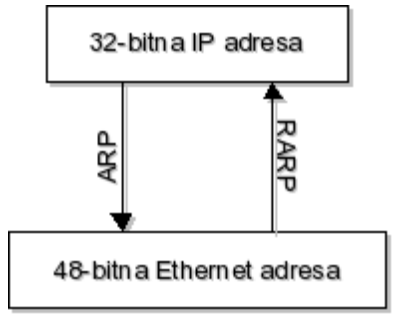
Ethernet mreže sa topologijom magistrale mogu imati loše performanse usled ograničenja broja konekcija u jednom trenutku, kolizija i opterećivanja svih članova mreže podacima upućenim samo jednom od njih. Iz tog razloga se došlo do nove varijante Etherneta - *Switched Ethernet*. Switched Ethernet koristi iste principe osnovne specifikacije sa tom razlikom što se umesto hub uređaja koriste switch uređaji.

Razlika između ova dva uređaja je u tome što hub primljeni paket prosleđuje svim članovima mreže dok switch pravi logičku vezu samo između pošiljaoca i primaoca. Na taj način je moguće istovremeno komuniciranje više parova, smanjuje se kolizija i povećava bezbednost. Logička topologija S*witched Ethernet-a* je zvezda.

7.7. Address Resolution Protocol (ARP)

Jedan od glavnih zadataka mrežnog sloja jeste adresiranje dok je sloj veze zadužen za prenos podataka. Međutim, adresiranje mrežnog sloja putem IP adresa nije moguće upotrebiti na nivou sloja veze a i na ovom sloju je u nekim situacijama neophodno obezbediti sistem adresiranja da bi se ostvarila veza sa određenim članom mreže. Na primer, pri korišćenju Ethernet tehnologije za direktno povezivanje dva računara ili za povezivanje više računara putem hab uređaja adresiranje na sloju veze nije neophodno jer u prvom slučaju ne postoje opcije a u drugom svi članovi mreže dobijaju sve poruke a zatim ih prihvataju ili odbacuju u zavisnosti od adrese mrežnog nivoa. Sa druge strane, u većim računarskim mrežama koje se npr. baziraju na svič uređajima potrebno je odrediti i adresiranje na sloju veze da bi se utvrdilo sa kojim uređajem u mreži treba uspostaviti vezu i dostaviti mu podatke. Određivanje uređaja se, naravno, vrši uskladu sa adresom mrežnom sloja. Za adresiranje na sloju veze zadužen je *Address Resolution Protocol* (ARP) koji je opisan u dokumentu RFC 826.

Address Resolution Protocol (ARP) je protokol zadužen za pronalaženje hardverske adrese odredišta putem njegove IP adrese. U slučaju Ethernet mreža, ARP se koristi za utvrđivanje MAC adrese putem IP adrese. ARP protokol obezbeđuje dinamičko prevođenje u smislu da se prevođenje odvija automatski bez potrebe za dodelom hardverskih adresa od strane korisnika.



Slika 7.x Konvertovanje adresa putem ARP i RARP protokola

Reverse Address Resolution Protocol (RARP) predstavlja inverzan protokol u odnosu na ARP. Ovaj protokol služi za određivanje adrese mrežnog sloja putem hardverske adrese uređaja.

7.8. Token Ring

Token Ring je tip lokalne računarske mreže koji je na tržište izbacio IBM. Nastao je na ideji da parira Ethernet-u. Token ring mreža ima logičku topologiju prstena, a fizičku topologiju zvezde. Brzine prenosa mogu biti 4 Mbps ili 16 Mbps. Osnovna ideja je sledeća: računari su prstenasto povezani. Od jednog do drugog računara se kroz mrežu kreće jedan skup bita koji se zove token (žeton). Računar koji želi da šalje svoju poruku nekom drugom u mreži prvo sačeka da token stigne do njega, a zatim ga ukloni iz mreže i počne da šalje svoju poruku. Ostali računari ne mogu u to vreme da šalju svoje podatke pošto to može samo računar koji drži token i koji na taj način samo za sebe rezerviše mrežu. Poruka ide po prstenu, računar kome je upućena je presnimi i na kraju se ponovo vraća računaru koji ju je poslao. Taj računar zatim ukloni poruku iz mreže, a token pusti dalje, tako da sad drugi računari, kada kod njih dođe token, mogu da šalju svoje poruke. Svaki računar u token ring mreži mora da ima odgovarajuću token ring adaptersku karticu.

U početku je IBM zajedno sa token ringom lansirao i poseban kablovski sistem za ovaj tip mreže. Međutim, tokom vremena, takav koncept je postepeno ustupio mesto sistemima strukturnog kabliranja. Ukoliko u mreži postoje adapterske kartice koje su prilagođene starom sistemu kabliranja, svakoj kartici se mora dodati odgovarajući adapter.

7.9. FDDI (Fiber Distributed Data Interface)

FDDI (*Fiber Distributed Data Interface*) je tip računarske mreže koji se uglavnom koristi u kičmama računarskih mreža. Razlog za to je velika brzina prenosa (100 Mbps) i velika ukupna dužina kablova (do 100 km) što je vrlo zgodno za povezivanje više zgrada. Mediji prenosa su uglavnom optički kablovi, ali se unutar zgrada često koriste bakarni parični kablovi, tako da to onda postaje CDDI.

Princip rada je veoma sličan token ringu, jedino što je kod FDDI i logička i fizička topologija prsten, odnosno dvostruki prsten. Prsteni provode signale u suprotnim smerovima i u slučaju da bilo gde dođe do prekida kabla, prsteni se automatski prespajaju i formiraju jedan veliki logički prsten. Prespajanje se vrši u odgovarajućim aktivnim uređajima (habovima, koncentratorima itd.). Pri formiranju FDDI mreže važno je voditi računa da se očuva logička topologija dvostrukog prstena.

7.10. 802.11(WiFi)

Bežične mreže se mogu klasifikovati u dve osnovne kategorije :

- Infrastrukturno zasnovane bežične mreže koje mogu biti:
    - celularne mobilne mreže (mobilna telefonija)
    - bežične računarske mreže - WLAN;
- Ad-hoc bežične mreže, kao mreže koje ne zahtevaju bilo kakvu infrastrukturu za rad, koje mogu biti:
    - mobilne ad hoc mreže,
    - senzorske ad hoc mreže (mreže autonomnih senzorskih uređaja).

Prema veličini prostora koji obuhvataju bežične računarske mreže mogu se još podeliti u tri osnovne grupe, a to su: bežične mreže na daljinu, lokalne bežične mreže i personalne ili lične mreže.

Bežične mreže na daljinu (*Wireless Wide Area Network* – WWAN), koje pokrivaju relativno velike geografske prostore i koriste radio i satelitske linkove. Obično se koriste za pokrivanje velikih univerzitetskih centara i gradova. U principu su fleksibilnije, jednostavnije za instaliranje i održavanje, i jeftinije po ceni priključka nego tradicionalne žične mreže.

Lokalne bežične mreže (*Wireless Local Area Network* – WLAN) omogućavaju da računari na jednoj geografskoj lokaciji dele informacije i zajedničke uređaje (štampači, baze podataka, itd.). U okviru ove mreže omogućeni su isti servisi kao i u žičnim mrežama, a imaju niz prednosti u odnosu na žični LAN – mobilnost, fleksibilnost, skalabilnost, brzina protoka, jednostavnost i smanjenje troškova instalacije. WLAN su neophodne u situacijama kada, zbog arhitektonskih, geografskih ili drugih razloga, nije moguće ostvariti druge načine formiranja mreže. U osnovi, bežične mreže zahtevaju određenu infrastrukturu: bežične PC kartice u umreženim računarima, pristupnu tačku (*Access point*), bežični PC adapter i mrežnu konekciju za pristupnu tačku. Potrebna je samo jedna pristupna tačka za jednu WLAN konekciju. Ograničavajući faktor primene je relativno kraći domet veze (30–300m) i frekvencijski opseg. Ako je potrebno premostiti veća rastojanja koriste se dodatne antene sa pojačivačima za podizanje nivoa signala.

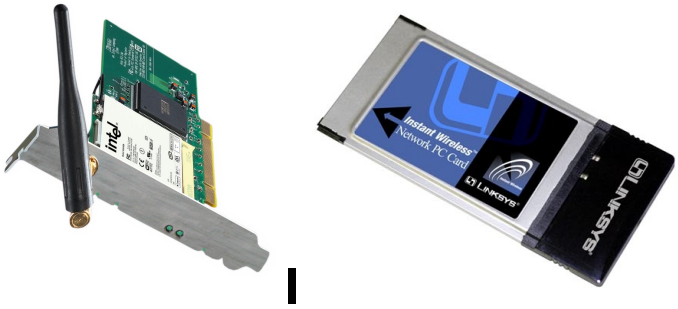
Personalne ili lične mreže (*Personal Area Network* – PAN) su mreže koje omogućavaju komunikaciju prvenstveno elektronskih uređaja unutar prostora od nekoliko metara i razmenu komunikacionih i sinhronizacionih informacija. To su pre svega mreže koje koriste infracrvene talase (*infrared*) za konekciju elektronskih uređaja na vrlo kratkim rastojanjima u okviru ograničene radne

prostorije i *bluetooth* mreže. Bluetooth komponente su našle široku primenu i u senzorskim mrežama.

7.10.1.Komponenete WLAN-a

Za formiranje bežične LAN mreže potrebni su bežične WLAN kartice i *Access Point* uređaji.

Bežične WLAN kartice se koriste umesto standardnih LAN kartica ili modema. Kartice koje se koriste imaju istu ulogu, koriste iste protokole i isto se ponašaju kao i kartice koje se koriste za standardnu mrežu s tim što za prenos podataka koriste radio talase a medijum za prenos je vazduh, a ne elektromagnetne signale kroz kablove. Na računar mogu biti spojeni preko jednog od sledećih interfejsa: PCI, USB ili PCMCIA.



Slika X - Bežične WLAN kartice

Access Point uređaj (pristupna tačka) se koristi umesto Dail-In servera ili Ethernet habova kod žičnih mreža (skup različitih uređaja koji se ponašaju kao čvorište, tj. razvodnik). Access Point je uređaj koji služi za međusobno povezivanje klijenata i predstavlja centralni deo jedne mreže. Takođe, može da se koristi i za spajanje wireless klijenata sa LAN-om ili sa izlazom na Internet. Access pointi igraju ulogu mostova (*bridges*) izmedu bežičnih stanica i resursa u žičnom LAN-u (serveri i ruteri za pristup internetu). Svaki access point ima integrisan konektor za antenu kao i konektor za LAN. Može da radi u nekoliko modova (čije prisustvo varira u zavisnosti od uređaja i proizvođača): *client* mod (pomoću njega se spaja na mrežu isto kao i pomoću obične kartice), *bridge* mod (koristi se za spajanje dve mreže ili više mreža u jednu celinu), *repeater* mod (repeater – ponavljač, koristi se ako je potrebno dodatno povećati domet mreže).

Slika X - Access point uređaji

Ukoliko postoji potreba da mreža pokriva veći prostor nego što to mogu gore navedeni uređaji svojim fabričkim antenama (100-400m u zavisnosti od prostora i prepreka) rešenje se traži u postavljanju jačih antena koje se uglavnom montiraju spolja, na krov. Na taj način mreža može da bude funkcionalna i par kilometara od access point-a. Antena koja se koristi na strani access pointa-a je omni-direkciona sto znači da pokriva prostor 360º oko sebe u horizontalnoj ravni. Na strani klijenta postavljaju se direkcione antene kojih ima raznih tipova i pojačanja (*helix*, *parabolic*, *biquad*, *panel* i druge).

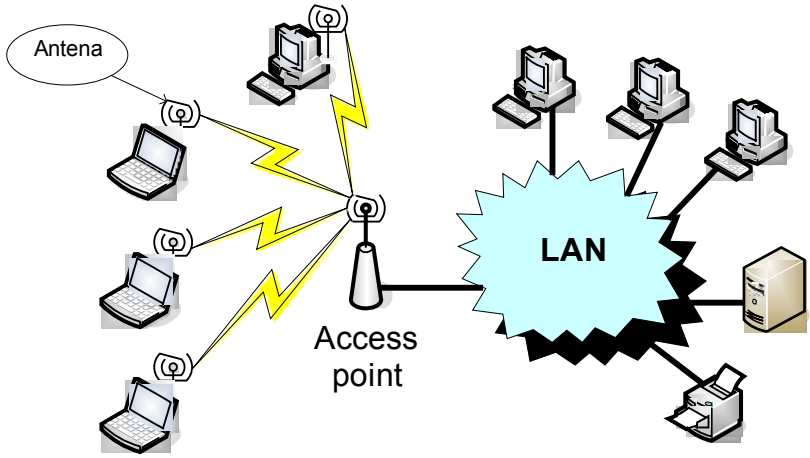
Omnidirekcionalna antena

Direkciona parabol antena

Slika 7.x Antene

7.10.2.Princip rada WLAN-a

Bežični LAN (WLAN) je fleksibilan komunikacioni sistem implementiran u početku kao dodatak ili kao alternativa žičnom LAN-u u zgradama, bolnicama, aerodromima itd. Bežični LAN-ovi koriste elektromagnetne talase za komunikaciju od jedne tačke do druge bez oslanjanja na bilo kakvu fizičku vezu.



Slika **7.x** Bežičan pristup LAN-u preko Access point uređaja

U tipičnoj WLAN konfiguraciji, odašiljač/prijemnik, koji se zove pristupna tačka (access point), povezuje se na žičnu mrežu sa fiksne lokacije koristeći standardan Ethernet kabl. Pristupna tačka prima, obrađuje i šalje podatke između WLAN-a i žične mrežne infrastrukture. Jedna pristupna tačka može podržati malu grupu korisnika i može funkcionisati unutar raspona od manje od tridesetak metara pa do preko stotinu metara. Krajnji korisnici pristupaju WLAN-u preko bežičnih LAN adaptera, koji su implementirani kao PC kartice u prenosnim računarima ili koriste PCI adaptere u desktop računarima.

Radio komunikacija kod WLAN-ova se obavlja u tzv. ISM (*Industrial, Scientific & Medical*) opsegu frekvencija koji je svuda u svetu prihvaćen kao opseg za čije korišćenje nije potrebna licenca - takozvani FTA (*free to air*) spektar. ISM čine tri opsega frekvencija: 902 - 928 MHz, 2400 - 2483,5 MHz i 5728 - 5750 MHz(slika 5). Od njih se, u ovom trenutku, najčešće koristi opseg oko 2.4 - 2.48 GHz. WLAN-ovi koriste *Spread Spectrum* tehniku prenosa (prenos u proširenom opsegu)

Renomirani proizvođači WLAN opreme, uključujući Nortel, Asus, Lucent, ZyXEL, Siemens, Cisco i dr. kao i specijalizovane kompanije kakva je Alvarion (Tel Aviv, Izrael), proizvode uređaje koji zadovoljavaju savremene WLAN standarde.

8. Mrežni sloj

Mrežni sloj predstavlja 3. sloj OSI i TCP/IP referentnih modela. Zadatak ovog sloja jeste da podacima dobijenim od transportnog sloja pridruži parametre na osnovu kojih će biti moguće određivanje jednog ili više mrežnih članova kojima pomenute podatke treba isporučiti. Drugim rečima, zadatak mrežnog sloja jeste da obezbedi sistem adresiranja članova mreže i pravila čijim će poštovanje biti moguća isporuka podataka na željenu adresu. Iako ovakav zadatak ne deluje komplikovano na nivou jednostavnih lokalnih mreža sa manjim brojem članova, značaj i problemi koji se stavljaju pred protokole mrežnog nivoa se mogu videti na nivou IP protokola koji omogućava univerzalno adresiranje preko četiri milijarde mogućih adresa na Internetu.

Jedan od najkompleksnijih zadataka koji se stavlja pred protokole mrežnog sloja jeste adresiranje koje omogućava povezivanje više različitih računarskih mreža. Na nivou jedne Ethernet mreže čiji su članovi povezani putem hab ili svič uređaja uloga protokola mrežnog nivoa je minimalna i uglavnom se odnosi na internu proveru da li je adresa primaoca lokalna adresa interfejsa. Međutim, na primeru kompleksne interne mreže koja se sastoji od više internih i međusobno povezanih segmenata i koja je dodatno povezana sa Internet mrežom mogu se uočiti problemi kao što su višestruke putanje, problem korišćenja istih mrežnih adresa u različitim internim mrežama i sl. Fokus protokola mrežnog sloja jeste rešavanje pomenutih problema sa konačnim ciljem omogućavanje univerzalnog i efikasnog sistema što većeg broja članova različitih, kompleksnih i međusobno povezanih računarskih mreža.

Protokolima mrežnog nivoa najčešće nedostaje funkcionalnost garantovanja isporuke podataka i otpornost na greške. Međutim, treba imati u vidu da se ove osobine najčešće nadomeštaju u protokolima transportnog sloja i njhovo uvođenje u protokole mrežnog nivoa bi znatno iskomplikovalo njihovu definiciju i dovelo do redundantnosti.

Jedan od najpopularnijih protokola mrežnog sloja jeste IP protokol verzije 4 koji je ujedno i podrazumevani protokol mrežnog sloja kod TCP/IP referentnog modela. Glavni atributi ovog protokola su jednostavnost i univerzalnost. Takođe, postoje i proširenja ovog protokola koja nude mogućnost dodatne kontrole prenosa (protokol ICMP) kao i rešenja koja korišćenjem IP protokola na mrežnom nivou omogućavaju kontrolu greške, tajnost putem šifrovanja podataka i utvrđivanje autentičnosti pošiljaoca (protokol IPsec).

Kod aktivnih mrežnih uređaja sa podrškom za protokole mrežnog sloja prvenstveno treba identifikovati ruter s tim da postoje i posebni svič uređaji koji nude dodatnu funkcionalnost (npr. VLAN segmentaciju) kroz razumevanje protokola mrežnog nivoa.

8.1. Internet Protocol (IP)

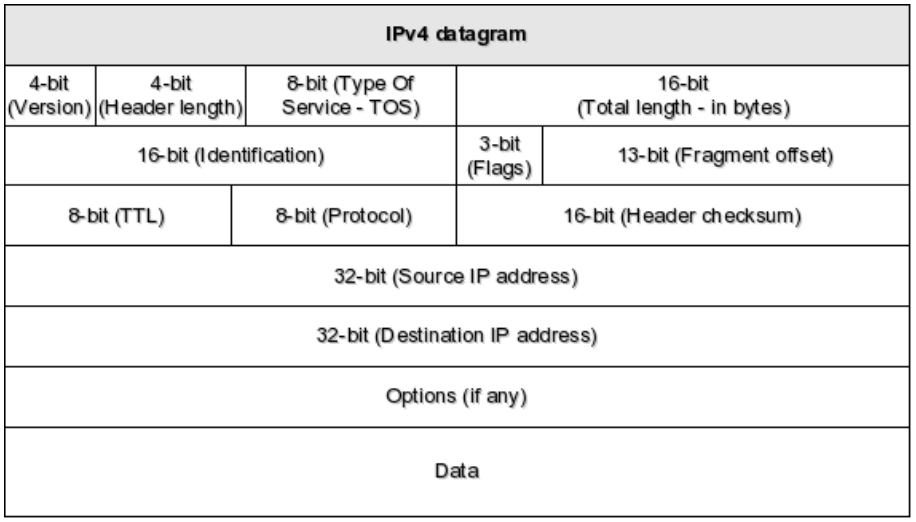
Internet Protokol (IP) je protokol koji se koristi za prenos podataka u i između "packet switched" mreža. Ovaj protokol se odnosi na mrežni sloj OSI i TCP/IP modela. To znači da ovaj protokol u sebe enkapsulira podatke viših slojeva (aplikativnog i transportnog) i u okviru paketa se podaci ovog protokola enkapsuliraju kao podaci za protokole nižeg sloja, sloja veze.

Glavna uloga IP protokola je obezbedi jedinstven sistem za globalno adresiranje računara i time obezbedi jedinstvenu identifikaciju svakog od njih. Protokoli nižih nivoa (protokoli sloja veze) imaju sopstvene načine adresiranja a za pronalaženje njihove adrese preko IP adrese zadužen je Address Resolution Protocol.

Internet Protokol ne garantuje dostavu paketa. Takođe, ovaj protokol ne garantuje ispravnost podataka (npr. da li je sadržaj paketa oštećen pri transportu), dozvoljava dupliranje paketa, prenos paketa u izmenjenom redosledu. Nedostatak ovih funkcionalnosti omogućava veću jednostavnost i performanse a one su izmeštene u protokole višeg nivoa.

8.1.1. Internet Protocol verzije 4 (IPv4)

Predstavlja 4. verziju Internet Protokola (IP) i to je ujedno prva verzija ovog protokola koja je široko prihvaćena za korišćenje. Izuzimajući IPv6 ovo je jedini protokol za adresiranje na mrežnom nivou koji se koristi na Internetu.



Slika X - Struktura IPv4 datagrama

IPv4 koristi 32-bitne (4 puta 8 bita) adrese i time nudi 2^{32} ($2^8 * 2^8 * 2^8 * 2^8$) ili 4,294,967,296 jedinstvenih adresa. Ipak, neke od ovih adresa (približno 18

miliona) su rezervisane za privatne mreže. Broj od preko 4 milijarde se u trenutku projektovanja IPv4 (1981. godina) činio sasvim dovoljnim za sve buduće potrebe ali se svakoga dana sve više uviđa njegovo ograničenje.

IPv4 adrese se mogu predstaviti u različitim formatima (heksadecimalno, decimalno, oktalno, binarno - sa i bez tačke) ali se najčešće koristi decimalna reprezentacija sa tačkom. Primer:

```
212.062.045.222
```

Binarno predstavljanje pomenute adrese bi izgledalo ovako:

```
11010100.00111110.00101101.11011110
```

Konvertovanje binarnog zapisa u decimalni zapis se vrši na sledeći način:

$$1*2^7 + 1*2^6 + 0*2^5 + 1*2^4 + 0*2^3 + 1*2^2 + 0*2^1 + 0*2^0 =$$
$$1*128 + 1*64 + 0*32 + 1*16 + 0*8 + 1*4 + 0*2 + 0*1 = 212$$

$$0*2^7 + 0*2^6 + 1*2^5 + 1*2^4 + 1*2^3 + 1*2^2 + 1*2^1 + 0*2^0 =$$
$$0*128 + 0*64 + 1*32 + 1*16 + 1*8 + 1*4 + 1*2 + 0*1 = 62$$

$$0*2^7 + 0*2^6 + 1*2^5 + 0*2^4 + 1*2^3 + 1*2^2 + 0*2^1 + 1*2^0 =$$
$$0*128 + 0*64 + 1*32 + 0*16 + 1*8 + 1*4 + 0*2 + 1*1 = 45$$

$$1*2^7 + 1*2^6 + 0*2^5 + 1*2^4 + 1*2^3 + 1*2^2 + 1*2^1 + 0*2^0 =$$
$$1*128 + 1*64 + 0*32 + 1*16 + 1*8 + 1*4 + 1*2 + 0*1 = 222$$

IPv4 adrese se ponekad nazivaju i *simboličkim adresama* jer su stvarne adrese čvorova na mreži u stvari hardverske MAC adrese. Promenom IP adrese uređaja se ne menja njegova MAC adresa.

8.1.2. Mreže i klase mreža

Pod IPv4 svaki uređaj na mreži ima jedinstvenu *kompletnu mrežnu adresu*. Razlog zašto se ova adresa označava kao *kompletna* je to što se ona sastoji iz dva dela:

- mrežne adrese (koja je zajednička za sve uređaje na istoj fizičkoj mreži
- adrese čvora (koja je jedinstvena za svaki uređaj/čvor na toj mreži)

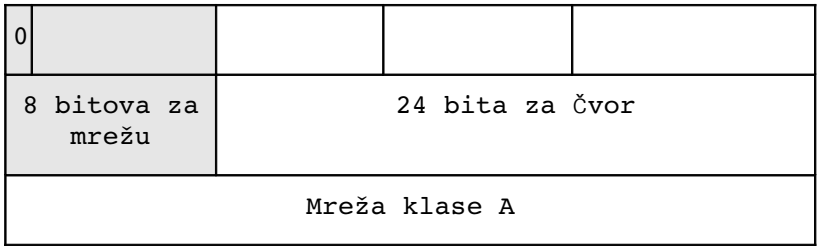
U originalu, IPv4 adrese su podeljene na sledeći način:

- adresa mreže (prvih 8 bitova)
- adresa čvora (preostala 24 bita)

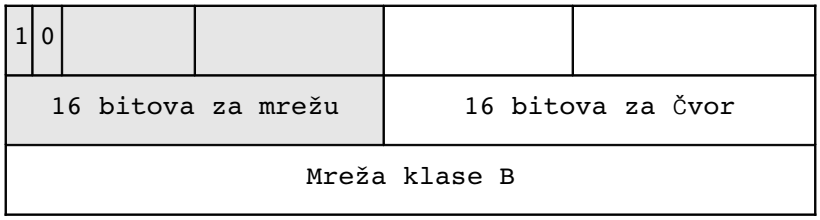
Ovakva podela je dovela do ograničenja od 256 (tačnije, 254) mreža što je dovelo do nastanka klasa mreža. Postoje 4 klase mreža - A, B, C, D i E. Klase A, B i C predstavljaju mreže sa različitom dužinom mrežnog broja dok klasa D služi za

multicast adrese a klasa E je rezervisana.

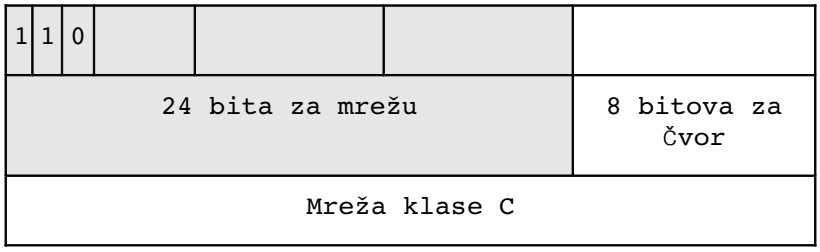
Kod mreža klase A se prvih 8 bitova koristi za određivanje mreže a ostala 24 za određivanje čvora s tim da je prvi bit fiksiran na 0 što znači da postoji 127 mreža klase A od kojih svaka može imati preko 16.777.214 članova. Opseg klase A je 0.0.0.0-127.255.255.255.



Kod mreža klase B se prvih 16 bitova koristi za određivanje mreže a ostalih 16 za određivanje čvora s tim da je prva dva bita fiksirana na 10 što znači da postoji 16.384 mreža klase B od kojih svaka može imati 65534 člana. Opseg klase B je 128.0.0.0-191.255.255.255.



Kod mreža klase C se prva 24 bita koristi za određivanje mreže a ostalih 8 za određivanje čvora s tim da je prva tri bita fiksirana na 110 što znači da postoji 2.097.152 mreža klase C od kojih svaka može imati 254 člana. Opseg klase C je 192.0.0.0-223.255.255.255.



Klasa D je rezervisana za *multicast* (isporuku informacija grupi primalaca, simultano) i kod nje su prva četiri bita fiksirana na 1110 a njen opseg je 224.0.0.0-239.255.255.255.255.

Klasa E je rezervisana i kod nje su prva četiri bita fiksirana na 1111 a njen opseg je 240.0.0.0-255.255.255.255.

8.1.3. Specijalni opsezi adresa

U cilju korišćenja IP adresa u lokalnim mrežama sa mogućnošću povezivanja tih mreža na Internet, određeni opsezi adresa su rezervisani za privatne mreže. Takođe, određeni opsezi su rezervisani i za specijalne namene.

Opseg	CIDR Ekvivalent	Svrha	Br. adresa
0.0.0.0 - 0.255.255.255	0.0.0.0/8	Zero Addresses	16.777.216
10.0.0.0 - 10.255.255.255	10.0.0.0/8	Privatne IP adrese	16.777.216
127.0.0.0 - 127.255.255.255	127.0.0.0/8	Localhost Loopback Address	16.777.216
169.254.0.0 - 169.254.255.255	169.254.0.0/16	Zeroconf / APIPA	65.536
172.16.0.0 - 172.31.255.255	172.16.0.0/12	Privatne IP adrese	1.048.576
192.0.2.0 - 192.0.2.255	192.0.2.0/24	Dokumentacija i primer	256
192.88.99.0 - 192.88.99.255	192.88.99.0/24	IPv6 ka IPv4 rilej anycast	256
192.168.0.0 - 192.168.255.255	192.168.0.0/16	Privatne IP adrese	65.536
198.18.0.0 - 198.19.255.255	198.18.0.0/15	Network Device Benchmark	131.07
224.0.0.0 - 239.255.255.255	224.0.0.0/4	Multicast	268.435.456
240.0.0.0 - 255.255.255.255	240.0.0.0/4	Rezervisano	268.435.456
Rezervisani opsezi IPv4 adresa			

8.1.4. CIDR (Classless Inter-Domain Routing)

1993. godine je predstavljen CIDR (Classless Inter-Domain Routing). CIDR je ujedno i poslednja dorada načina korišćenja IP adresa tj. zamena *klasa mreža*. CIDR nudi veću fleksibilnost pri podeli IP adresa na opsege ili pod-mreže. CIDR omogućava:

- efikasnije iskorišćavanje IPv4 adresa
- bolju hijerarhiju pri dodeli adresa (tzv. *agregacija prefiksa*)

CIDR se omogućava prefikse bazirane na bitovima (dok se klase mreža baziraju na grupama od 8 bitova tj. bajtovima).

CIDR blokovi IPv4 adresa se označavaju sličnom sintaksom ko i same IPv4 adrese: četiri grupe decimalnih brojeva (odvojene tačkom) sa dodatkom kose crte (/) i broja između 0 i 32 - A.B.C.D/N. Broj N (0-32) predstavlja broj bitova adrese, počev od 1 bita sa leve strane, koji ulaze u prefix. Veća dužina prefiksa (N) znači veći broj opsega (2^N) sa manjim brojem adresa (broj adresa se dobija po formuli 2^{32-N}) i obratno.

Na osnovu sopstvene adrese i dužine prefiksa, računari mogu da odrede da li se čvor sa određenom adresom nalazi u istom bloku (mreži) i da li je neposredna komunikacija moguća ili ne.

CIDR se koristi i kod IPv6 protokola na isti način s tom razlikom što dužina prefiksa može biti od 0 do 128 usled razlike u formatu IPv6 adresa (pogledati deo *"IPv6"*).

8.1.5. Maska pod-mreže

U delu "IPv4 / Mreže i klase mreža" je objašnjeno kako se početni bitovi (od 8. do 24.) IP adrese mogu koristiti za određivanje mreže kojoj čvor pripada. Ova informacija se takođe naziva i maska podmreže a reprezentuje se u vidu kontinualnog niza jedinica (čiji je broj jednak broju bitova koji ulaze u adresu mreže) praćenog nizom nula (čiji je broj jednak broju bitovakoji ulaze u adresu čvora).

A	11111111	00000000	00000000	00000000
B	11111111	11111111	00000000	00000000
C	11111111	11111111	11111111	00000000

Podmaske mreža klase A, B i C (binarna reprezentacija)

Decimalna reprezentacija ovih maski bi izgledala:

A	255	0	0	0
B	255	255	0	0
C	255	255	255	0

Podmaske mreža klase A, B i C (decimalna reprezentacija)

Klase A, B i C ne omogućavaju precizniju podelu mreže jer njihove makse koriste isključivo sve bitove ili ni jedan iz svake grupe od 8 bitova. CIDR omogućava dodatnu i precizniju podelu opsega adresa na mreže korišćenjem sva 32 bita u kreiranju maske podmreže.

Uzmimo kao primer mrežu klase C. Adresni opseg te mreže se kreće u intervalu od 192.168.1.0 do 192.168.1.255 a maska te mreže je 255.255.255.0 i u nju ulaze prva 24 bita u obliku jedinica:

C	11111111	11111111	11111111	00000000

Ukoliko želimo da ovu mrežu podelimo na dve manje mreže, u mrežnu masku ćemo uključiti i 25. bit:

C+	11111111	11111111	11111111	1	0000000

tako da se ona decimalno može predstaviti:

C+	255	255	255	128

Na ovaj način smo, krenuvši od identifikatora mreže (sa 24 bita):

C	192	168	1	0
	11000000	10101000	00000001	00000000

došli do dve mreže čiji identifikatori uključuju prvih 25 bitova:

CM1	192	168	1	0	
	11000000	10101000	00000001	0	0000000
CM2	192	168	1	128	
	11000000	10101000	00000001	1	0000000

Na ovaj način smo kreirali dve mreže sa manjim adresnim opsegom od početne mreže (mreža klase C ima 256 adresnih mesta dok novokreirane mreže imaju po 128 adresnih mesta). Prva od ove dve mreže ima adresni opseg od 192.168.1.0-192.168.127 a druga od 192.168.1.128-192.168.1.255.

Još jednu stvar je bitno zapaziti:

- prvi broj opsega predstavlja identifikator mreže
- poslednji broj opsega predstavlja *Broadcast*
- ove dve adrese se ne mogu koristiti za adresiranje uređaja

Iz ovoga proizilazi da u mreži klase C imamo svega 2/256 (0,8%) gubitaka tj. adresa koje ne možemo koristiti za adresiranje čvorova. Međutim, podelom mreže klase C na dve manje mreže, opseg od 256 adresa je podeljen na dva opsega od 128 adresa a svaki od ovih opsega ima svoj mrežni broj i *Broadcast* tako da su u ovom slučaju gubici (2*2)/256 (1,6%). Iz ovoga proizilazi da ukoliko želimo da mrežu klase C podelimo na 64 podmreže (u čiju će masku ući prvih 30 bitova), dobićemo 64 mreže sa po 4 adresna mesta od koji prvo predstavlja broj mreže a četvrto *Broadcast* tako da ostaju svega dva adresna mesta za adresiranje čvorova po mreži a broj gubitaka iznosi (64*2)/256 ili 50%.

Maska mreže i IP adresa su osnovni mrežni parametri svakog uređaja (čvora) u mreži. U slučaju da mreža ima mogućnost komunikacije sa drugim mrežama (tj. ima gateway), adresa gateway uređaja je treći konfiguracioni mrežni parametar

svih uređaja. Na osnovu svoje IP adrese i mrežne maske, članovi mreže određuju da li je određenu komunikaciju moguće ostvariti direktno (tj. da li se odredište nalazi u istoj mreži kao i sam uređaj) ili je neophodno komunikaciju obaviti posredstvom gateway-a (tj. odredište se nalazi u van lokalne mreže).

Uzmimo za primer računar sa sledećim mrežnim parametrima:

adresa: 192.168.1.100

maska: 255.255.255.0 (CIDR: 192.168.1.100/24)

gateway: 192.168.1.1

Ukoliko ovaj računar želi da komunicira sa računarom čija je adresa 192.168.1.200 on će pomoću informacije iz mrežne maske uporediti prva 24 bita svoje adrese sa prva 24 bita odredišne adrese. Pošto se ovi bitovi poklapaju (192.168.1 = 192.168.1) računar shvata da se odredište nalazi u istoj mreži kao i on sam, i odredištu će se obratiti direktno tj. bez posredstva gateway-a.

U sledećem primeru uzmimo računar sa mrežnim parametrima:

adresa: 192.168.1.100

maska: 255.255.255.128 (CIDR: 192.168.1.100/25)

gateway: 192.168.1.1

Ukoliko ovaj računar želi da komunicira sa računarom čija je adresa 192.168.1.200 on će pomoću informacije iz mrežne maske uporediti prvih 25 bitova svoje adrese sa prvih 25 bitova odredišne adrese. Pošto se ovi bitovi razlikuju (konkretno, 25. bit izvorišnog računara je 0 a odredišnog 1) računar shvata da se odredište ne nalazi u lokalnoj mreži i obraća mu se posredstvom gateway-a.

8.1.6. Primer podele mreže klase C na podmreže

maska podmreže CIDR	br. mreža	opseg adresa	br. adr.	ID mreže	Broadcast
255.255.255.0 x.x.x.ID/24	1	x.x.x.1- x.x.x.254	254	x.x.x.0	x.x.x.255
255.255.255.128 x.x.x.ID/25	2	x.x.x.1- x.x.x.126 x.x.x.129- x.x.x.254	126	x.x.x.0 x.x.x.128	x.x.x.127 x.x.x.255
255.255.255.192 x.x.x.ID/26	4	x.x.x.1 - x.x.x.62 x.x.x.65 - x.x.x.126 x.x.x.129 - x.x.x.190 x.x.x.193 - x.x.x.254	62	x.x.x.0 x.x.x.64 x.x.x.128 x.x.x.192	x.x.x.63 x.x.x.127 x.x.x.192 x.x.x.255
255.255.255.224 x.x.x.ID/27	8	x.x.x.1 - x.x.x.30 x.x.x.33 - x.x.x.62 x.x.x.65 - x.x.x.94 x.x.x.97 - x.x.x.126 x.x.x.129 - x.x.x.158 x.x.x.161 - x.x.x.190 x.x.x.193 - x.x.x.222 x.x.x.225 -	30	x.x.x.0 x.x.x.32 x.x.x.64 x.x.x.96 x.x.x.128 x.x.x.160 x.x.x.192 x.x.x.224	x.x.x.31 x.x.x.63 x.x.x.95 x.x.x.127 x.x.x.159 x.x.x.191 x.x.x.223 x.x.x.255

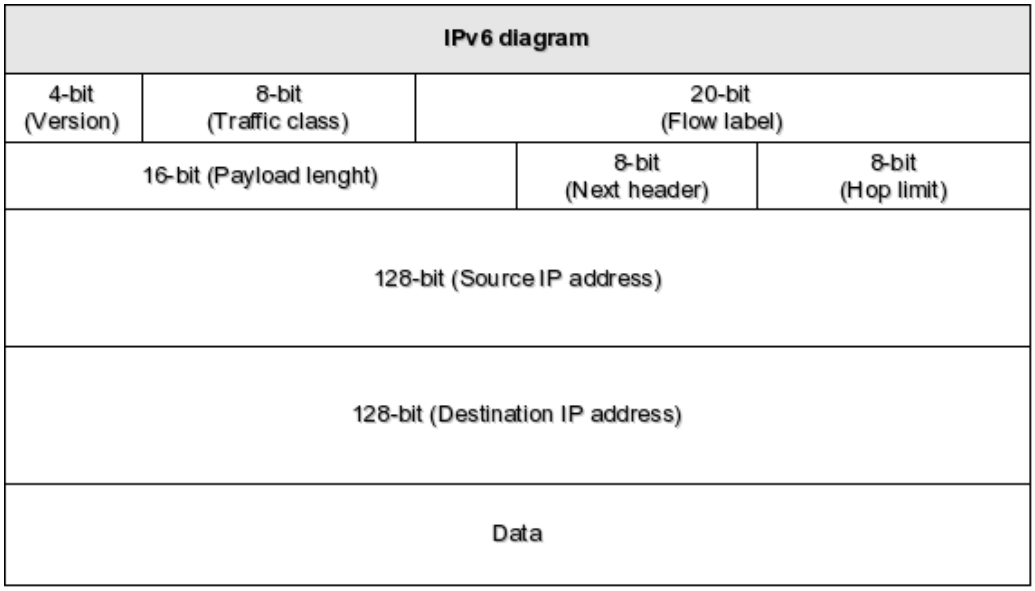
		x.x.x.254			
255.255.255.240 x.x.x.ID/28	16	x.x.x.1 - x.x.x.14 x.x.x.17 - x.x.x.30 x.x.x.33 - x.x.x.46 x.x.x.49 - x.x.x.62 x.x.x.65 - x.x.x.78 x.x.x.81 - x.x.x.94 x.x.x.97 - x.x.x.110 x.x.x.113 - x.x.x.126 x.x.x.129 - x.x.x.142 x.x.x.145 - x.x.x.158 x.x.x.161 - x.x.x.174 x.x.x.177 - x.x.x.190 x.x.x.193 - x.x.x.206 x.x.x.209 - x.x.x.222 x.x.x.225 - x.x.x.238 x.x.x.241 - x.x.x.254	14	x.x.x.0 x.x.x.16 x.x.x.32 x.x.x.48 x.x.x.64 x.x.x.80 x.x.x.96 x.x.x.112 x.x.x.128 x.x.x.144 x.x.x.160 x.x.x.176 x.x.x.192 x.x.x.208 x.x.x.224 x.x.x.240	x.x.x.15 x.x.x.31 x.x.x.47 x.x.x.63 x.x.x.79 x.x.x.95 x.x.x.111 x.x.x.127 x.x.x.143 x.x.x.159 x.x.x.175 x.x.x.191 x.x.x.207 x.x.x.223 x.x.x.239 x.x.x.255
255.255.255.248 x.x.x.ID/29	32	x.x.x.1 - x.x.x.6 x.x.x.9 - x.x.x.14	6	x.x.x.0 x.x.x.8 ...	x.x.x.7 x.x.x.15 ...

		... x.x.x.241 – x.x.x.246 x.x.x.249 – x.x.x.254		x.x.x.240 x.x.x.248	x.x.x.247 x.x.x.255
255.255.255.252 x.x.x.ID/30	64	x.x.x.1 – x.x.x.2 x.x.x.5 – x.x.x.6 ... x.x.x.249 – x.x.x.250 x.x.x.253 – x.x.x.254	2	x.x.x.0 x.x.x.4 ... x.x.x.248 x.x.x.252	x.x.x.3 x.x.x.7 ... x.x.x.251 x.x.x.255

8.2. Internet Protocol verzije 6 (IPv6)

Internet protocol datira još sa kraja 60-tih godina prošlog veka i počeo ja da pokazuje neke znake "starenja". Jedan problem je trošenje adresa, tj. nedovoljan broj adresa za opsluživanje globalnih zahteva. Pošto su Internet adrese 32-bitne, postoji konačan broj raspoloživih adresa. IPv6 je naslednik tekuće verzije Intrnet protokola (IPv4).

8.2.1. Zaglavlje IPv6 paketa



Slika X – struktura IPv6 paketa

Polje *Version* je dužine 4 bita i identifikuje verziju IP-ja koju ovaj paket predstavlja (vrednost 4 za tekuću verziju IP-ja, a 6 za novu).

Polje *Priority* takođe ima 4 bita i izuzetno je korisno za kontrolu zagušenja. Koncept prioriteta je jednostavan: više vrednosti ukazuju na značenje paketa. Bitno je kako se prioriteti koriste. IPv6 prepoznaje da su kašenjenja u nekim aplikacijama, kao što je email, često i neprimetne, dok kašnjenja u nekim drugim aplikacijama, kao što su multimedijalne, čine gledanje skoro nemogućim. Trik je u tome da se identifikuje koji paketi odgovaraju kojim aplikacijama. Sajt sa koga se šalju IP paketi može da iskoristi ovo polje za definisanje značaja paketa u odnosu na ostale pakete koji se šalju sa istog mesta. Vrednosti prioriteta se nalaze između 0 i 7, i odgovaraju paketima koji se mogu zadržavati malo duže radi rešavanja zagušenja. IPv6 preporučuje vrednosti u zavisnosti od aplikacije, email ima prioritet 2, FTP i HTTP 4, Telnet 6, a SNMP 7. vrednosti iznad 7 odgovaraju real-time, ili multimedijalnim aplikacijama, slučajevima kada kašnjenja mogu da

budu veoma neprikladna.

24-bitno polje *Flow Label* koristi se zajedno sa poljem Priority. Ideja je da se identifikuju paketi koji zahtevaju "specijalni tretman" u ruterima. Normalno rukovanje zahteva od rutera da pretraže svoje tabele rutirana pre nego što proslede pakete. Pošto se te tabele menjaju vremenom, paketi sa istim odredištem mogu da "putuju" preko različitih ruta. IPv6 definiše tok (flow) kao sekvencu paketa koji se šalju od izvora do jednog odredišta, kao odziv na neku aplikaciju. Ako su ti paketi dizajnirani za prikazivanje u realnom vremenu na odredištu, specijalni tretman može da podrazumeva njihovo rutiranje na isti način kako bi se garantovao dolazak u ispravnom redosledu.

16-bitno polje *Payload Length* predstavlja broj bajtova u paketu minus 40. Pošto je zaglavlje dugačko 40 bajtova, ovo polje definiše koliko značajnih bitova sledi iza njega.

Polje *Hop Limit* u suštini ima istu funkciju kao i polje Time to live kod IPv4 paketa.

8-bitno polje *Next Header* predstavlja značajnu razliku u poređenju sa IPv4 paketima. Tekuće zaglavlje IPv4 paketa sadrži polja Options i Protocol, pomoću kojih se naznačava kada ruter treba da predume određeni akcije. Pošto se u polje sa tim nazivom ugrađuju različite opcije svaki ruter mora da pasira zaglavlje paketa (specijalno polje Option) kako bi utvrdio da li postoje opcije koje mogu da utiču na njegove odluke. To zahteva dodatnu logiku i vreme koje ruter mora da izdvoji, što usporava ceo proces rutiranja.

Da bi se omogućilo navođenje različitih opcija, IPv6 ima *zaglavlje proširenja (extension header)*. Svako dodatno zaglavlje ima i polje Next Header, koje definiše tip dodatnog zaglavlja koje sledi (ako postoji). Ovo omogućava nekoliko zaglavlja proširenja koja se postavljaju između originalnog zaglavlja i korisnih informacija paketa; svako od njih ukazuje na različitu opciju. Ako nema zaglavlja proširenja, onda, poput polja Protocol u IPv4 zaglavlju, polje Next Header definiše transportni protokol koga IPv6 koristi. Najznačajnijim aspektom ovog uređenja može se smatrati to što će neka dodatna zaglavlja ruteri ignorisati. Tako će ruteri moći brže da prosledjuju pakete.

Sadržaj i forma svakog dodanog zaglavlja zavisi od njegovog tipa:

- **Destination options header** (Zaglavlje sa opcijama za odredište) Ovo zaglavlje obezbeđuje informacije za odredište. Ne koristi se za vreme rutiranja.
- **Fragmentation headrer** (Zaglavlje fragmentacije) Ovo zaglavlje obezbeđuje informacije za slučaj da je neophodno ponovo sastaviti fragmente paketa. Kao takvo, ono sadrži stavke kao što su ofset

fragmenta, bit Last Fragment i identifikator koji je jedinstven za originalni paket.

Prelazni IPv4 ruteri su mogli da fragmentuju dolazeće pakete ako su bili suviše veliki. IPv6 ne dopušta fragmentiranje paketa u prelaznim ruterima. Ovo je značajno zbog toga što uprošćava logiku u ruteru i doprinosi efikasnijem i bržem rutiranju. Ako ruter dobije paket koji je suviše veliki da bi bio poslat preko mreže, on jednostavno odbacuje pakt i šalje poruku (preko ICMP-a) nazad do izvora. Ta poruka ukazuje da je paket bio suviše veliki i naznačava se maksimalna dopuštena veličina. Izvor će nakon toga fragmentirati paket i poslati fragmente, koji sadrže zaglavlje fragmentacije. Fragmenti se ponovo sastavljaju na odredištu.

- **Hop-by-hop header** (Zaglavlje za pojedinačne skokove) Ovo zaglavlje, ako postoji, mora da se prouči u svakom ruteru. Ideja je da se navedu sve informacije koje moraju da imaju svi ruteri. Postoji nekoliko mogućih opcija. Pošto je dužina polja Payload Length 16 bitova, maksimalna veličina paketa je 64 KB. Ovo zaglavlje dopušta *džambo pakete*, pakete veće od 64 KB što je korisno prilikom prenosa velikih količina podataka, kao u slučaju video zapisa. Sledeđa opcija je olakšavanje RSVP protokola,gde paketi sadrže informacije o rezervisanom propusnom opsegu koji mora da se obezbedi u svakom ruteru.
- **Routing header** (Zaglavlje za rutiranje) Ovo zaglavlje obezbeđuje dodatne informacije o rutiranju. Sadrži 128-bitne adrese rutera preko koji paket mora da prođe.
- **Security header** (Bezbednosno zaglavlje) Ovo zaglavlje ukazuje na činjenicu da su korisne informacije paketa šifrovane.
- **Authentication header** (Zaglavlje autentifikacije) Ovo zaglavlje suži za autentifikaciju paketa koja se koristi sa IPSec , bezbednosnim protokolom na nivou paketa.

8.2.2. IPv6 adresiranje

Najočiglednija razlika u odnosu na IPv4 je to što su IPv6 adrese 128- bitne, četiri puta duže od IPv4 adresa. Teorijski je omogućeno 2^{128} različitih adresa.

Adrese se svrstavaju u tri opšte kategorije: unicast, anycast i mulicast. *Unicast adresa* definiše jedinstveni interfejs. *Anycast adresa* definiše grupu interfejsa. Paket sa anycast odredišnom adresom može da se isporuči jednom interfejsu u bilo kojoj grupi. *Multicast adresa* definiše grupu, ali u ovom slučaju paket prolazi kroz svaki interfejs u grupi.

Notacija 128-bitnih adresa se razlikuje od one koja se koristi za IPv4. Korišćenje tekuće notacije u kojoj se tačkama razdvajaju brojevi dalo bi notaciju koja sadrži 16 trocifrenih brojeva razdvojenih tačkama. Umesto toga, tačke se menjaju dvotačkama i svakih 16 bitova u adresi predstavlja heksadecimalnu notaciju četvorocifrenog broja. Primer IPv6 adres ima sledeći oblik:

```
7477:0000:0000:0000:0000:0AFF:1BDF:7FFF
```

Za adrese koje sadrže mnogo nula koristi se skraćena notacija. U suštini, nule se ne navode, već se na njihovo prisustvo ukazuje sa dve dvotačke (::). Stvarni broj nula koje nedostaju izračunava se oduzimanjem broja heksadecimalnih cifara u notaciji od 32, broj heksadecimalnih cifara koje su potrebne za punu 128-bitnu reprezentaciju. Primer:

```
7477::0AFF:1BDF:7FFF
```

Trenutno postoje 22 različita tipa adresa; svaki ima jedinstven prefiks. Prefiksi mogu da sadrže od tri do deset bitova.

8.2.3. Kompatibilnost sa IPv4

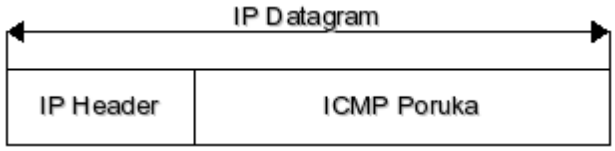
IPv4 i IPv6 ruteri moraju da koegzistiraju i da održavaju sve neophodne konekcije. IPv6 protokol je dizajniran tako da prepozna IPv4 protokol. Sa druge strane, IPv4 protokol dizajnirani pre IPv6 i ne znaju ništa o njemu.

Ukoliko IPv6 paket mora da prođe preko IPv4 ruter paket se ugrađuje u IPv4 paket. IPv4 protokoli rade ono što je neophodno da se prakt prosledi do sledeće tačke, gde se IPv6 paket izvlači iz IPv4 paketa. Ovakav sistem se naziva tunelovanje.

Kompatibilnost IP verzije 6 sa verzijom 4 predstavlja dodatno opterećenje definicije protokola koje je nepotrebno u mrežama baziranim isključivo na protokolu verzije 6. Međutim, nepostojanje ovakvog sistema kompatibilnosti bi znatno usporilo prihvatanje verzije 6 kao opšteg standarda jer bi ogroman broj korisnika Interneta morao da istovremeno izvede prelazak što u praksi ne bi bilo izvodljivo. Takođe, većina aktivne mrežne opreme koja se koristi u mrežama koje rade pod IP protokolom verzije 4 bi postala neupotrebljiva i zamena opreme bi predstavljala ogroman finasijski izdatak. Dodatno, LAN mreže koje imaju pristup Internetu bi takođe morale i interno da se prevedu na verziju 6 IP protokola.

8.3. Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP) se često smatra delom IP protokola. Ovaj protokol u stvari predstavlja proširenje IP protokola. Osnovma uloga ICMP-a jeste podnošenje izveštaja o greškama i stanju IP mreže. Korišćenje ICMP protokola može inicirati sam mrežni sloj ili aplikacije/protokoli viših slojeva. Zvanična specifikacija ICMP protokola se nalazi u RFC dokumentu 792.



Slika X - Enkapsulacija ICMP poruke u okviru IP datagrama

ICMP protokol koristi kontrolne poruke koje se prenose u okviru IP datagrama. ICMP poruke se sastoje od zaglavlja dužine 32 bita i sadržaja.

Slika X - Struktura ICMP

S obzirom na to da je uloga ICMP protokola nadomeštanje nedostajućih funkcija za kontrolu u IP protokolu, ICMP poruke se uglavnom odnose na ispitivanje stanja mreže i u sebi sadrže upite i njima odgovarajće odgovore. Jedan od najčešće korišćenih korisničkih alata za upotrebu ICMP protokola jeste *ping* alat.

```
bash-3.1$ ping www.google.com
PING www.l.google.com (209.85.135.104) 56(84) bytes of data.
64 bytes from f14.google.com (209.85.135.104): icmp_seq=1 ttl=241 time=37.0 ms
64 bytes from f14.google.com (209.85.135.104): icmp_seq=2 ttl=241 time=35.8 ms
64 bytes from f14.google.com (209.85.135.104): icmp_seq=3 ttl=240 time=35.8 ms
--- www.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 35.851/36.268/37.094/0.584 ms
bash-3.1$
```

Listing X - primer korišćenja ping alata

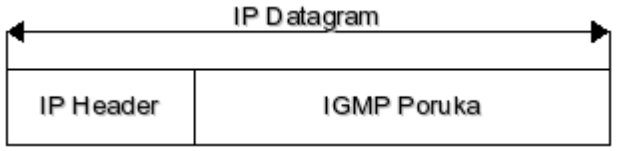
Ovaj alat se koristi za proveru da dostupnosti IP odredišta i brzine komunikacije.

Kontrolna poruka	Opis
Destination Unreachable	Odredište možda ne postoji, ili je trenutno nefunkcionalno, pošiljalac je možda postavio zahtev za rutom koju je možda nemoguće izvesti, ili je paket sa postavljenim flegom Do Not Fragment isuviše veliki da bi bio enkapsuliran u okvir. U takvim situacijama ruter detektuje grešku i šalje ICMP paket do originalnog pošiljaoca
Echo Request	ICMP koristi ovaj paket kako bi utvrdio da li je određeno odredište dostupno.
Echo Reply	Šalje se kao odgovor na Echo Request paket.
Parameter Problem	Ukoliko IP paket sadrži grešku, ili nedozvoljenu vrednost u nekom polju zaglavlja, ruter otkriva grešku i šalje Parameter Problem paket nazad do izvora. Ovaj paket sadrži problematično zaglavlje i pokazivač na polje zaglavlja u kome postoji greška
Redirect	Ako host stanica šalje paket do rutera koji zna da paket može da se brže isporuči preko nekog drugog rutera, da bi olakšao buduće rutiranje, ruter šalje Redirect paket nazad do hosta. On obaveštava host stanicu gde se drugi ruter nalazi i da bi ubuduće sve pakete do istog odredišta trebalo slati njemu. Ovako je omogućeno dinamičko ažuriranje tabela rutiranja i na taj način je moguće povoljno iskoristiti neke primene uslova na mreži. Redirect paket se ne koristi za ažuriranje rute, jer IP paket sadrži izvornu adresu, a ne adresu rutera koji je prethodno imao paket.
Source Quench	Ako ruter primi i suviše veliki broj paketa od hosta, može da pošalje poruku kojom zahteva redukovanje učestalosti kojom se paketi šalju.
Time Exceeded	Time Exceeded paket se šalje kada je vrednost polja Time to Live u IP paketu dostigla o, ili kada je tajmer za ponovno slanje paketa istekao. U svakom slučaju paket, ili neki nesastavljeni fregment se odbacuju sa mreže. Ruer koji je kriv za njihovo odbacivanje šalje Time Exceeded do odredišta kako bi se ukazalo da paketi nisu isporučeni.
Timestamp Request Timestamp Reply	Vremenska oznaka paketa (timestamp) omogućava hostu da proceni koliko je vremena potrebno za krug do drugog hosta i nazad.

Address Mask Request and Reply	Host može da pošalje Address Mask Request and Reply paket do rutera da bi utvrdio masku adrese za mrežu na koju je priključen. Ruter može da pošalje odgovor.

8.4. Internet Group Management Protocol (IGMP)

Kao i ICMP, Internet Group Management Protocol (IGMP) se često smatra delom IP protokola. Ovaj protokol se koristi kod članova mreže koji podržavaju *multicasting* i služi za dobijanje informacija koji članovi mreže se trenutno nalaze u kojim *multicast* grupama. Ova informacija je neohpodna ruterima koji podržavaju multicast iz tog razloga da bi znali na koje interfejse treba proslediti multicast saobraćaj. Specifikacija IGMP protokola je data u RFC 1112 dokumentu.



Slika X - Enkapsulacija IGMP poruke u okviru IP datagrama

Bitska dužina IGMP poruke je 64 bita. Ova poruka sadrži polje koje označava verziju IGMP protokola (ova vrednost je za sada uvek 1), polje koje označava tip IGMP poruke (1 predstavlja IGMP upit a 2 IGMP odgovor), polja koje sadrži vrednost kontrolne sume poruke i polje u kome se nalazi IP adresa klase D (vrednost svih bitova adrese je 0 kod IGMP poruka sa tipom 1).

IGMP poruka			
4-bita (IGMP verzija)	4-bita (IGMP tip)	8-bita (Nije u upotrebi)	16-bita (Kontrolna suma)
32-bita (Grupa adresa – IP adresa klase D)			

Slika X - Struktura IGMP poruke

Za korišćenje IGMP protokola je potrebno u mreži imati ruter koji podržava IGMP protokol. Sledeća četiri pravila definišu način rada mreže sa podrškom za IGMP:

1. Član mreže šalje IGMP poruku čim se prvi proces na njemu priključi nekoj multicast grupi. Za naredne procese koji se priključuju istoj multicast grupi se ne šalju dodatne IGMP poruke.
2. Član mreže ne šalje IGMP poruke o tome da se neki od lokalnih procesa isključi sa multicast grupe. Poruka se takođe ne šalje čak ni kada poslednji proces napusti multicast grupu. Član mreže jedino vodi evidenciju o tome da li za neku od multicast grupa ima procese koji su joj pridruženi ili ne.
3. Ruter sa podrškom za multicast u određenim vremenskim intervalima

šalje IGMP upite za proveru da li neki od članova lokalne mreže ima procese pridrušene nekoj od multicast grupa koje se obraćaju ruteru.

4. Članovi mreže odgovaraju na IGMP upite rutera šaljući odgovore za svaku od multicast grupa kojoj su lokalni procesi pridruženi.

Na osnovu opisanih IGMP upita i odgovora ruter održava internu tabelu na osnovu koje određuje na koje će interfejse propustiti pristigle multicast datagrame.

8.5. Internetwork Packet Exchange (IPX)

Internetwork Packet Exchange (IPX) je protokol mrežnog nivoa OSI modela i koristi se u kombinaciji sa SPX protokolom transportnog sloja. Ovaj protokol je razvijen od strane Novell kompanije na osnovu IDP protokola kompanije Xerox a za potrebe Novel NetWare mrežnih operativnih sistema. S obzirom na popularnost operativnih sistema kompanije Novell početkom 90-ih godina 20. veka, IPX/SPX kombinacija protokola je u tom periodu predstavljala jedno od najpopularnijih rešenja za lokalne mreže. Danas, međutim, TCP/IP stek protokola predstavlja univerzalno i daleko češće korišćeno rešenje. Čak i NetWare operativni sistemi počev od verzije 5 podržavaju i komunikaciju putem TCP/IP protokola.

IPX protokol poseduje određene sličnosti sa IP protokolom ali i razlike koje ova dva protokola čine nekompatibilnim. Dok IP protokol univerzalno koristi 32-bitno adresiranje IPX protokol adresira logičke mreže preko 32-bitnih adresa (predstavljenih heksadecimalno) a članove mreža putem 48-bitnih adresa inicijalno postavljenih na vrednost hardverskih adresa interfejsa (MAC). Ovakvo adresiranje članova eliminiše potrebu za ARP protokolom koji je neophodan kod IP protokola. Rutiranje se kod IPX protokola odvija slično kao i kod IP protokola, pomoću tabela za rutiranje. Kao i IP protokol, IPX protokol prenosi podatke bez prethodnog ostvarivanja veze. Jedinica za prenos podataka je takođe datagram.

IPX protokol podržava četiri tipa enkapsulacije u frejmove nižih slojeva (npr. Ethernet-a):

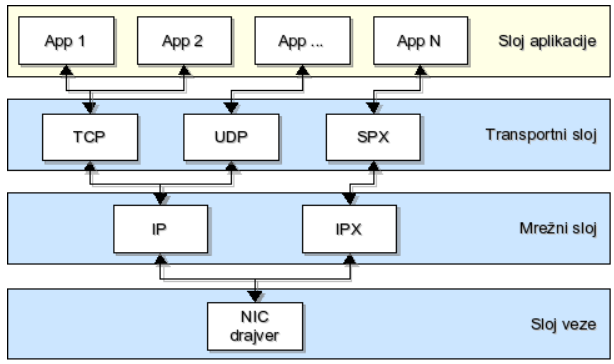
1. Novell Proprietary - koristi IEEE 802.3 *lenght* polje ali ne sadrži IEEE 802.2 *LLC* zaglavlje. Zaglavlje IPX protokola počinje odmah nakon *lenght* bitova. Naziva se i Novell Ethernet_802.3 ili sirovi 802.3.
2. 802.3 - koristi standardni IEEE 802.3 format frejma.
3. Ethernet II - podaci IPX datagrama počinju nakon standardnog Ethernet II zaglavlja.
4. SNAP - koristi standardni IEEE 802.3 format frejma sa dodatkom SNAP zaglavlja pre početka IPX datagrama.

8.6. IPsec

Jedan od čestih nedostataka protokola transportnog i nižih slojeva jeste prenos podataka u izvornom obliku - obliku u kom su dobijeni od aplikacije. Dobra strana ovakvog pristupa jeste minimalan uticaj nosećih protokola na podatke koje entiteti aplikativnog nivoa razmenjuju. Nedostatak ovakvog pristupa jeste mogućnost pregleda i izmena podataka od strane članova mreže kojima podaci nisu namenjeni i koji nisu nadležni za njihovu izmenu. U takvoj situaciji mogućnost pregleda podataka imaju svi članovi mreže do kojih podaci dođu (npr. svi članovi Ethernet mreže povezani putem hub uređaja) a mogućnost izmene svi članovi koji su zaduženi za prosleđivanje podataka do odredišta (npr. ruteri i ostala čvorišta).

Drugi ozbiljan nedostatak, pre svega protokola mrežnog nivoa, jeste mogućnost falsifikovanja ili preotimanja izvorišne adrese i slanje podataka sa izvorišta koje se smatra pouzdanim. Ovaj nedostatak se pre svega odnosi na mreže kod kojih se privilegije pristupa dodeljuju na osnovu parametara protokola mrežnog sloja umesto na osnovu parametara aplikativnog sloja.

Rešavanje pomenutih problema se najčešće sreće na aplikativnom sloju tj. unutar samih aplikacija. Nedostatak ovakvog pristupa je potreba da se svaka aplikacija nadograđuje funkcijama za šifrovanje/dešifrovanje i proveru autentičnosti druge strane tj. strane sa kojom se ostvaruje komunikacija. Određene aplikacije već imaju ugrađene ove funkcionalnosti ali kod aplikacija koje te funkcionalnosti nemaju naknadno ugrađivanje može zahtevati znatne finansijske, ljudske i vremenske resurse a najčešće i nije moguće usled nedostupnosti izvornog koda.



Slika X - "Slivanje" slojeva

Idealno rešenje u ovakvoj situaciji jeste rešavanje problema pregleda/izmene podataka i provera autentičnosti na što nižem sloju i na taj način obuhvatanje svih podataka dostavljenih od gornjih slojeva. Međutim, rešavanje na fizičkom sloju bi uslovljavalo dizajn hardvera, znatno uticalo na cenu i otežalo unapređivanje rešenje i ispravljanje eventualni nedostataka. Rešavanje problema na sloju veze

bi uslovilo format prenosa podataka i uslovilo prilagođavanje formata na svim nosećim komunikacionim kanalima. Mrežni sloj se kod pomenutog problema ističe kao ciljni sloj na kome rešenje treba realizovati.

Jedno od najpopularnijih rešenja za šifrovanje na mrežnom nivou je svakako IPsec (IP Security) koje je ujedno i standard za obezbeđivanje Internet Protokola (IP). IPsec je set kriptografskih protokola za obezbeđivanje protoka paketa i razmenu ključeva:

- ESP (Encapsulating Security Payload) - omogućuje autentičnost, poverljivost podataka i integritet poruke.
- AH (Authentication Header) - obezbeđuje autentičnost i integritet poruke ali ne i poverljivost).
- IKE (Internet Key Exchange) - komponenta zadužena za upravljanje ključevima.

Princip rada IPsec-a je takav da podatke dobijene od transportnog sloja šifruje i/ili potpisuje u skladu sa odabranim algoritmom i ključevima. U zavisnosti od načina pridruživanja IP zaglavlja dobijenom šifratu i/ili digitalno potpisanim podacima IPsec omogućava dva režima rada:

1. Transportni režim rada
2. Tunelski režim rada

Kod transportnog režima rada standardno IP zaglavlje se pridružuje šifrovanim podacima dobijenim od transportnog sloja. To znači da je na datagrame transportnog režima rada primenljivo standardno rutiranje. Međutim, NAT (*Network Address Translation*) operacija nad ovakvim datagramima nije moguća jer se prevođenjem IP adrese sadržaj datagrama menja i kontrolna suma datagrama prestaje da se poklapa sa sadržajem. Iz tog razloga je transportni režim rada moguće koristiti samo za zaštitu direktnih komunikacija.

Kod tunelskog režima rada se podacima dobijenim od transportnog sloja pridružuje standardno IP zaglavlje a operacija šifrovanja se izvršava nad celim datagramom. Od dobijenog šifrata se pravi novi datagram dodavnjem novog IP zaglavlja. Nad IP datagramima kreiranim kod tunelskog režima rada je moguće izvršiti NAT operaciju jer se kontrolna suma IPsec protokola odnosi samo na deo datagrama na koji NAT operacija nema uticaj.

IPsec sistem zaštite predstavlja jedno od najefikasnijih rešenja za zaštitu podataka koji se prenose komunikacionim kanalima nebezbednih računarskih mreža (npr. Internet). Ovaj sistem omogućava visok stepen zaštite a brojna rešenja za korišćenje IPsec protokola čine njegovu upotrebu jednostavnom.

9. Transportni sloj

Transportni sloj OSI i TCP/IP referentih modela predstalja sloj između sloja aplikacije (tj. aplikativnog sloja sesije kod OSI modela) i mrežnog sloja. Opšta uloga ovog sloja, kao i ostalih slojeva jeste da omogući komunikaciju sloja iznad i sloja ispod (u ovom slučaju sloja aplikacije sa slojem mreže). Konkretna uloga ovog sloja jeste da prihvati podatke aplikacije izvorišta i dostavi ih aplikaciji odredišta starajući se o prenosu, kontroli i ispravljanju grešaka pri prenosu i garantovanjem isporuke. Podrška za transportni sloj je uglavnom realizovana na nivou operativnih sistema računara s tim da sam transportni sloj nije eksplicitno definisan već se realizje kroz podršku za protokole tog sloja.

Prihvatanjem podataka od aplikativnog sloja transportni sloj ima zadatak da podatke prevede u oblik pogodan za transport. Znatno kompleksnija funkcija ovog sloja jeste da podatke prenese korišćenjem nižih slojeva kojima često nedostaju pomenute funkcionalnosti vezane za garantovanje isporuke i kontrolu grešaka. Funkcionalnosti koje se uglavnom adresiraju na ovom sloju su:

- Ostvarivanje virtuelne veze za prenos podataka.
- Prevođenje podataka u (uglavnom binarni) format pogodan za prenos.
- Segmentacija podataka radi efikasnijeg iskorišćenja komunikacionog kanala.
- Isporuka podataka u identičnom obliku u kom su poslati.
- Omoućavanje optimalne brzine prenosa podataka u skladu sa propusnom moći i učestalošću grešaka na komunikacionom kanalu i prihvatnoj moći primaoca.

Iako je adresiranje glavna uloga mrežnog sloja, transportni sloj poseduje interni sistem adresiranja čija je adresna jedinica *port*. Port je određen 16-bitnim numeričkim parametrom i njegova je uloga da adresira izvorni/odredišni entitet aplikativnog sloja (aplikaciju) od koga potiču podaci tj. kome treba isporučiti podatke.

Portovi se mogu podeliti na privilegovane, registrovane i dinamičke (ili kratkotrajne) portove. Privilegovani portovi su portovi u opsegu 0-1023 i pravo na njihovo otvaranje uglavnom ima samo operativni sistem. Na ovim portovima se nalaze najčešće korišćeni servisi (FTP, SSH, Telnet, DNS i sl.). Registrovani portovi se kreću u opsegu od 1024 do 49151 i na njima se zvanično koriste servisi novijeg datuma. Dinamički ili kratkotrajni portovi se kreću u opsegu od 49152 do 65535 i njih nije moguće registrovati a uglavnom služe za klijentske komponente klijent/server softvera.

Entitete aplikativnog sloja je moguće adresirati putem portova po sopstvenom

izboru s tim da je za standardizaciju u ovoj oblasti zadužena organizacija IANA (Internet Assigned Numbers Authority). Ovo telo na zahtev proizvođača softvera analizira opravdanost za zvaničnim dodeljivanjem slobodnih portova (u skladu sa rasprostranjenošću servisa za koji se port zahteva) i dodeljuje zahtevani port ukoliko je dostupan. Pre zvaničnog dodeljivanja porta servisu potrebno je ostvariti određenu opštost (tj. masovnost) servisa. Ovakav način može dovesti do konfliktnih situacija kod kojih se dva ili više servisa koriste u različitim mrežama na istom portu i ostvare određenu grupu korisnika pre zvaničnog zahteva za određenim portom. Primer ovakve situacije jeste port 465 koji se bez zvaničnog odobrenja koristi za SMTP protokol zaštićen SSL-om kao i od strane Cisco kompanije.

Port	Servis
20	FTP prenos podataka
21	FTP kontrolne poruke
22	SSH - Secure Shell
23	Telnet
25	SMTP - Simple Mail Transfer Protocol
53	DNS - Domain Name System
80	HTTP - Hyper Text Transfer Protocol
110	POP3 - Post Office Protocol verzije 3
123	NTP - Network Time Protocol
143	IMAP4 - Internet Message Access Protocol 4
161	SNMP - Simple Network Management Protocol
389	LDAP - Lightweight Directory Access Protocol
443	HTTPS - HTTP obezbeđen putem TLS/SSL
860	iSCSI - Internet SCSI

631	IPP - Internet Printing Protocol
989	FTP prenos podataka obezbeđen putem TLS/SSL
990	FTP kontrolne poruke obezbeđen putem TLS/SSL

Tabela X - Često korišćeni portovi

Kompozitna adresna jedinica transportnog i mrežnog sloja jeste *socket.* Socket (nekada se naziva i mrežni socket ili samo socket) je sačinjen od sledećih komponenti:

- IP adresa izvorišta
- Port izvorišta
- Protokol transportnog sloja
- Port odredišta
- IP adresa odredišta

Podrška za socket-e se u operativnim sistemima najčešće realiuje pomoću gotovih sistemskih biblioteka. Neke od najpopularnijih socket biblioteka su Berkeley socket za Unix operativne sisteme i Winsock za MS Windows operativne sisteme. Osim upotrebe u računarskim mrežama socket-i se mogu koristiti i kod aplikacija koje se izvršavaju na lokalnom računaru. Npr. X Window System grafički sistem na Unix platformi zahteva socket da bi funkcionisao.

Iako referenti modeli OSI i TCP/IP omogućavaju razvoj različitih transportnih protokola danas su u upotrebi (i na Internetu i kod lokalnih mreža) najčešće Transmision Control Protocol (TCP) i User Datagram Protokol (UDP). TCP protokol omogućava pouzdan prenos podataka putem ostvarivanja virtuelne veze, kontrole grešaka, kontrole redosleda segmenata i prilagođavanje brzine slanja podataka prijemnoj moći odredišta dok UDP protokol ne poseduje ove funkcionalnosti. TCP protokol se koristi kod servisa kod kojih je neophodna tačnost na račun performansi a UDP protokol u obrnutim situacijama.

9.1. Transmission Control Protocol (TCP)

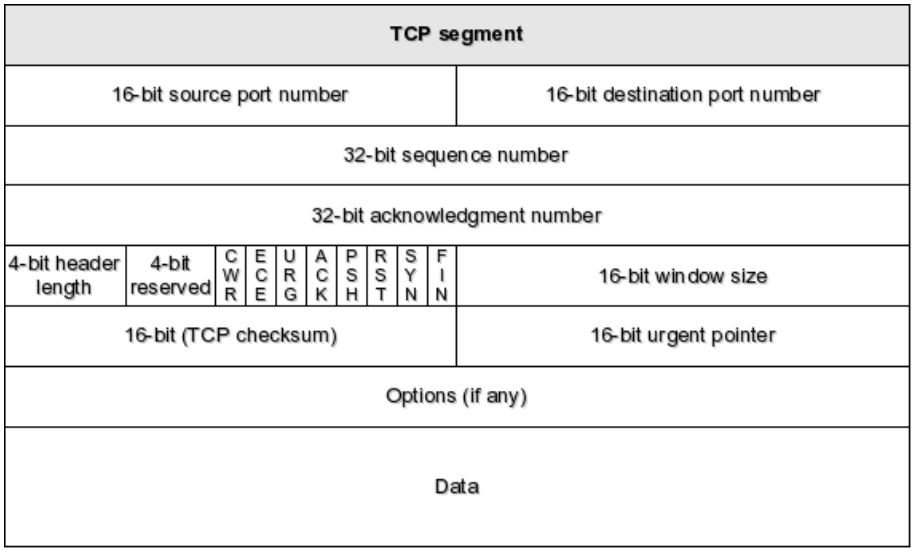
Transmission Control Protocol (protokol za upravljanje prenosom) je protokol zadužen za rad sa podacima u transportnom sloju. TCP je protokol sa uspostavom veze dizajniran da za podatke koristi nizove bajtova i obezbedi pouzdan prenos podataka u oba smera (full-duplex). Ovaj protokol je pogodan za rad na komunikacionim kanalima visoke pouzdanosti (npr. UTP i optički kablovi) a pokazuje slabije performanse na komunikacionim kanalima sa čestim oštećenjem podataka pri prenosu (npr. bežična komunikacija).

TCP protokol je jedan od najčešće korišćenih protokola na transportnom nivou kada je su u pitanju Internet i klasične lokalne mreže. Ovaj protokol je već godinama u upotrebi i razlog tome je pre svega optimalan rad na Ethernet tehnologiji. TCP protokol je inicijalno definisan u dokumentu RFC793 a kasnije je njegova specifikacija nekoliko puta menjana u skladu sa novim potrebama i mogućnostima računarskih mreža. Neki parametri TCP protokola su određeni u skladu sa ograničenjima komunikacionih kanala (npr. MTU parametar je ograničen na 536 bajtova za veze sa stranama koje nisu u lokalnoj mreži) ali su se vremenom pokazali neadekvatnim usled značajnih unapređenja brzina i pouzdanosti komunikacionih kanala.

Savremena okruženja za razvoj distribuiranih aplikacija najčešće imaju razvijenu podršku za korišćenje TCP protokola i/ili protokola višeg nivoa koji koriste usluge TCP protokola. To znači da ovaj protokol predstavlja *de facto* standard za razvoj distribuiranog softvera koji zahteva pouzdan prenos podataka. Neki od najpopularnijih servisa interneta (Web, e-mail, FTP itd) se baziraju na TCP protokolu.

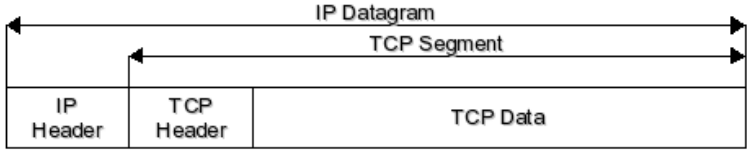
9.1.1. TCP segmenti

Osnovna jedinica prenosa podataka kod TCP protokola je segment. Segment se sastoji od zaglavlja (koje generiše i interpretira sam protokol) i aplikativnih podataka (koje generiše/preuzima aplikativni sloj). Aplikativni podaci nisu obavezan deo segmenta i izostavljeni su kod kontrolnih segmenata (npr. segmenata zaduženih za uspostavljanje i prekid veze).



Slika X - Struktura TCP segmenta

Zaglavlje TCP segmenta se sastoji od polja fiksne dužine koja sadrže informacije vezane za protokol. Bitska dužina zaglavlja je 5x32 bita ukoliko nisu uključene opcije. Bitska dužina celokupnog segmenta je jednaka bitskoj dužini zaglavlja (ukoliko se segmentom ne prenose podaci aplikacije) ili zbiru bitske dužine zaglavlja i bitske dužine podataka dobijenih od sloja aplikacije.



Slika X - Odnos IP datagrama i TCP segmenta

Osim osnovnog dela zaglavlja ono može sadržati i dodatne opcije vezane za protokol. Svaka opcija zaglavlju dodaje reč od 32 bita. Ukoliko opcija ne sadrži dovoljno podataka da ispuni 32 bita, preostali bitovi se dopunjavaju nulama. Neke od najvažnijih opcija TCP protokola su MSS (*Maximum Segment Size*), WSOPT (*Window Scale Option*), SACK (*Selective ACK*) i SACK Permitted. Sadržaj opcija takođe ulazi u kontrolnu sumu segmenta (*TCP checksum*).

Polje	Bita	Opis
Source port number	16	Port preko koga se komunikacija vrši na strani koja šalje segment. Na osnovu porta sistem određuje kojoj aplikaciji treba proslediti podatke iz segmenta. Broj porta u kombinaciji IP adresom se naziva *socket*.
Destination port number	16	Port preko koga se komunikacija vrši na strani koja prima segment.
Sequence number	32	Broj koji označava redni broj prvog bajta podataka u segmentu u odnosu na celokupan niz podataka koji se prenosi. U slučaju segmenta sa SYN indikatorom kada se određuje inicijalna vrednost (ISN - Initial Sequence Number).
Acknowledgment number	32	Broj koji služi za utvrđivanje koji paketi su regularno isporučeni na odredište.
Header length	4	Broj reči dužine 32 bita koje se nalaze u zaglavlju (podrazumevana vrednost je 5). Ovaj parametar pomnožen sa 32 označava poslednji bit zaglavlja.
Reserved	4	Bitovi rezervisani za buduće proširenje protokola.
Indikatori	8	**CWR -** *Congestion Window Reduced*
		ECE - *Explicit Congestion Notification*
		URG - urgentan segment (eng. *urgent*)
		ACK - potvrda prijema (eng. *acknowledge*).
		PSH - (eng. *push*).
		RST - označava segment koji inicira prekid i ponovno uspostavljanje veze.
		SYN - označava segment koji inicira uspostavljanje veze (uz sinhronizaciju sekvencijalnih brojeva).
		FIN - označava segment koji inicira prekid veze.
Window size	16	Veličina okvira tj. broj bajtova koje odredište može da prihvati preko segmenata koji su potvrđeni.
TCP checksum	16	Kontrolna suma koja se odnosi na zaglavlje i potatke i koristi se za proveru da li je segment izmenjen tokom

		transporta.
Urgent pointer	16	Koristi se u sprezi sa URG indikatorom i upućuje na poslednji bajt urgentnih podataka.

9.1.2. Uspostavljanje i prekid veze

Pri korišćenju TCP protokola dve strane moraju da uspostave vezu između sebe kao preduslov za dalju razmenu podataka. Uspostavljanje veze se vrši putem sledećih koraka:

1. Klijent serveru šalje segment sa SYN indikatorom koji sadrži broj porta servera na koji klijent želi da se poveže i ISN klijenta.
2. Server odgovara na SYN zahtev klijenta segmentom koji sadrži ACK indikator sa ISN-om klijenta uvećanim za jedan. Segment takođe sadrži SYN indikator servera sa njegovim ISN.
3. Klijent odgovara na SYN zahtev servera šaljući segment sa ACK indikatorom koji sadrži ISN servera uvećan za jedan.

Ova tri koraka se nazivaju "rukovanje" (eng. *handshake*) i ukoliko ne dođe do greške u njima, veza je uspostavljena. Strana koja inicira uspostavljanje veze izvršava *aktivno uspostavljanje veze* (eng. *active open*) dok strana koja prihvata uspostavljanje veze izvršava *pasivno uspostavljanje veze* (eng. *passive open*).

Jednom uspostavljena veza ostaje aktivna dok god se ne zahteva njen prekid ili dok se jedna od strana ne izgubi evidenciju o njoj (npr. resetovanjem računara). To znači da su u periodima kada se veza ne koristi za prenos podataka mogući prekidi na svim nižim slojevima (uključujući i fizički).

Kod prekida uspostavljene veze potrebno je da obe strane dobiju informaciju da je veza prekinuta i da dalji prenos podataka nije moguć. Prekid veze može inicirati svaka od strana, bez obzira na to koja strana je inicirala uspostavljanje veze. Za prekid veze se koriste FIN indikatori u TCP zaglavlju a redosled segmenata je sledeći:

1. Strana koja inicira prekid šalje TCP segment sa uključenim FIN indikatorom.
2. Primalac odgovara segmentom sa uključenim ACK indikatorom.
3. Za potpuni prekid veze primalac šalje segment sa uključenim FIN indikatorom.
4. Inicijator prekida šalje odgovor u vidu segmenta sa uključenim ACK indikatorom.

Strana koja inicira prekid veze izvršava *aktivan prekid veze* (eng. *active close*) dok strana koja prihvata prekid veze izvršava *pasivan prekid veze* (eng. *passive close*). Ukoliko jedna strana inicira prekid veze (pošalje segment sa FIN indikatorom i primi segment sa ACK indikatorom) a druga zadrži vezu uspostavljenom takva veza se naziva polu-zatvorenom (eng. *half-close*) i njome se nadalje mogu slati samo podaci u jednom smeru.

9.1.3. Pouzdanost i performanse

Performanse TCP protokola su uglavnom znatno slabije u poređenju sa protokolima koji rade bez uspostavljanja veze (npr. UDP protokolom). Takođe, TCP protokol ne podržava broadcasting i multicasting već omogućava komunikaciju između isključivo dve strane. Međutim, glavna karakteristika TCP protokola je pouzdanost. S obzirom na to da IP protokol (protokol mrežnog sloja) ne garantuje pozdan prenos podataka, pouzdanost TCP protokola se ostvaruje putem sledećih pravila:

- Podatke koje aplikacija dostavlja transportnom sloju TCP deli u segmente koje šalje pojedinačno. Na taj način se smanjuje jedinica nad kojom se vrši kontrola i na taj način smanjuje mogućnost i cena ispravljanja greške.
- TCP zahteva potvrdu da je svaki od poslatih segmenata isporučen. Podaci se nakon slanja čuvaju u izlaznom baferu do dobijanja potvrde o prijemu. Ukoliko potvrda o isporučivanju ne stigne u određenom vremenskom roku, segment se šalje ponovo.
- TCP eliminiše iste segmente koje je mrežni sloj greškom dostavio dva ili više puta.
- TCP reorganizuje primljene segmente po izvornom redosledu bez obzira na redosled kojim ih mrežni sloj dostavlja.
- TCP prilikom slanja segmenta generiše kontrolne parametre vezane za zaglavlje i sadržaj. Ukoliko prilikom prenosa segmenta dođe do izmena zaglavlja ili sadržaja ove sume ukazuju na njih i zahteva se ponovno slanje segmenta.
- TCP prilagođava frekvenciju slanja segmenata prihvatnoj moći primaoca čime sprečava odbacivanje segmenata (i nepotrebno opterećenje komunikacionog kanala) i smanjuje mogućnost greške.

Dobijene korisničke podatke (tj. podatke koje dostavlja aplikativni sloj) TCP protokol tretira kao niz bajtova. Ukoliko dobijeni niz bajtova prelazi najveću dozvoljenu veličinu segmenta (MSS, Maximum Segment Size), niz se deli i šalje sa više segmenata.

MSS (Maximum Segment Size) opcija

Parametar MSS svaka strana dostavlja suprotnoj u okviru segmenta sa SYN indikatorom (pri upostavljanju veze) a, ukoliko ta opcija segmenta nije data eksplicitno, koristi se podrazumevana sistemska vrednost od 536 bajtova. Ukupna veličina TCP segmenta (uključujući zaglavlje i podatke) sa MSS-om od 536 bajtova iznosi 556 bajtova veličina IP datagram ovakvog paketa bi iznosila 576 bajtova (556 bajtova TCP segmenta + 20 bajtova IP zaglavlja). Dakle, IP datagram sa ovakvom veličinom MSS-a sadrži 536 bajtova

(93%) korisničkih podataka i 40 bajtova (7%) podataka vezanih za TCP i IP protokole. To znači da je u ovakvom slučaju komunikacionim kanalom propusne moći 100Mb/s u jednoj sekundi moguće preneti 93Mb korisničkih podataka.

Ukoliko vrednost MSS-a povećamo na 3960 bajtova ukupna veličina IP datagrama bi iznosila 4000 bajtova (veličine TCP i IP zaglavlja ostaju iste po segmetnu i datagramu). U tom slučaju bi odnos korisničkih podataka i podataka vezanih za protokole iznosio 99:1. Takva vrednost MSS-a bi na komunikacionom kanalu propusne moći 100Mb/s omogućila prenos 99Mb korisničkih podatak u sekundi.

Iz ovoga bi se moglo zaključiti da veća vrednost MSS-a omogućava veće brzine prenosa tj. efikasnije korišćenje komunikacionog kanala. Međutim, ovakav zaključak je tačan samo u slučaju kada komunikacioni kanal i interfejsi ka njemu omogućavaju prenos podataka bez grešaka. U slučajevima kada se javljaju greške pri prenosu (što zahteva ponovno slanje oštećenih segmenata) visoke vrednosti MSS-a mogu imati suprotan efekat ili čak u potpunosti onemogućiti komunikaciju.

Opcija MSS stoji u bliskoj vezi sa performansama TCP protokola. Negativan uticaj na performanse ovog protokola može imati i potreba da se za svaki dostavljeni segment zasebno dostavi potvrda o isporuci.

SACK (Selective ACK) i SACK Permitted opcije

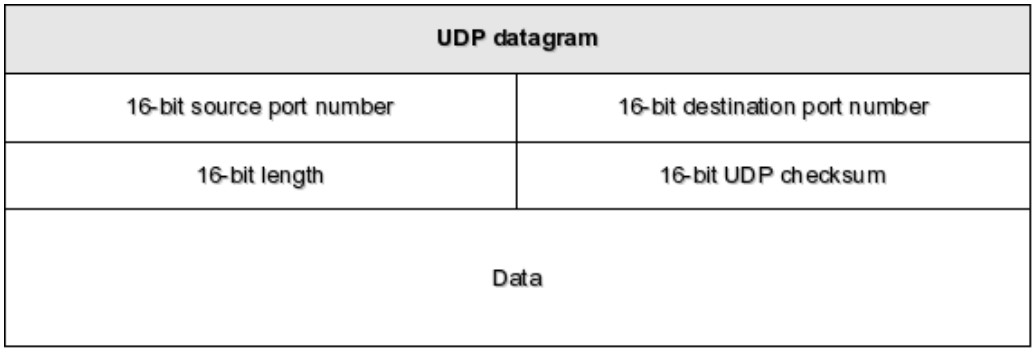
Slanje ACK segmenta za svaki uspešno primljeni segment u određenim slučajevima može predstavljati nepotrebno opterećenje komunikacionog kanala. Međutim, pošiljalac može slanjem paketa sa SACK permitted opcijom ovlastiti klijenta za periodično slanje segmenta sa SACK opcijom - segmenta koji sadrži obaveštenje o više uspešno primljenih segmenata. Na taj način se rasterećuje komunikacioni kanal na račun izlaznog bafera pošiljaoca.

Osnovna potvrda o isporuci se šalje u vidu segmenta sa uključenim ACK indikatorom. Pomoću opcije SACK (Selective ACK) moguće je poslati potvrdu za više primljenih paketa u okviru jednog segmenta. Za ovu opciju je potrebno da i druga strana dozvoli njeno korišćenje slanjem paketa sa SACK Permitted opcijom.

9.2. User Datagram Protocol (UDP)

User Datagram Protocol (UDP) pored TCP protokola predstavlja jedan od najčešće korišćenih transportnih protokola Interneta i lokalnih računarskih mreža. Nasuprot TCP protokolu UDP protokol ne omogućava pouzdan prenos podataka putem ostvarivanja virtuelne veze, kontrole grešaka, kontrole redosleda segmenata i ne prilagođava brzinu slanja podataka prijemnoj moći odredišta. Nedostatak ovih funkcionalnosti čini UDP protokol jednostavnijim protokolom od TCP protokola i protokolom koji ne garantuje pouzdan prenos podataka. Međutim, namena UDP protokola nije pouzdan prenos podataka već prenos sa što manjim vremenskim neslaganjima između generisanja podataka na strani izvorišta i prijema podataka na odredištu. Glavne primene UDP-a su kod protočnog prenosa glasa i video materijala (Internet telefonija, video konferencije, računarske igrice i sl.). Prednost UDP protokola u odnosu na TCP jeste mogućnost *broadcast* slanja podataka tj. istovremenog slanja podataka svim članovima mreže.

Jedinica za prenos podataka UDP protokola je datagram. Struktura UDP datagrama je znatno jednostavnija od strukture TCP segmenata jer je izostavljena većina kontrolnih informacija.



Slika X - Struktura UDP datagrama

Međutim, nedostatak kontrolnih informacija čini UDP protokol znatno efikasnijim u smislu manjeg opterećenja komunikacionog kanala kontrolnim podacima i manjeg opterećenja primaoca datagrama u smislu jednostavnijeg procesiranja datagrama.

Polje	Bita	Opis
Source port number	16	Port preko koga se komunikacija vrši na strani pošiljaoca.
Destination port number	16	Port preko koga se komunikacija vrši na strani primaca.

Length	16	Broj bitske dužine podataka koje datagram nosi.
Checksum	16	Kontrolna suma zaglavlja i paketa.

Neotpornost UDP protokola na greške pri prenosu, višestruko dostavljanje istih datagrama ili gubitka podataka, dostavljanje podataka u izmenjenom redosledu i sl. moguće je nadomestiti funkcionalnostima u aplikativnom sloju. Neke aplikacije koje koriste UDP protokol primenjuju ovakav pristup (npr. TFTP servis). Međutim, korišćenjem UDP protokola aplikacije ugavnom očekuju maksimalne performanse prenosa bez obzira na greške i dodatni sistemi za ispravljanje grešaka bi ugrozili normalan rad pomenutih aplikacija.

9.3. Stream Control Transmission Protocol (SCTP)

Stream Control Transmission Protocol (SCTP) je protokol koji ima sličnos i sa TCP i sa UDP protokolom. Kao i TCP protokol SCTP omogućava pouzdan prenos podataka brzinom koja je prilagođena prihvatnoj moći odredišta. Takođe, kao i UDP protokol SCTP omogućava isporuku podataka na više odredišta istovremeno.

Izvod iz RFC 2960 dokumenta

SCTP is designed to transport PSTN signaling messages over IP networks, but is capable of broader applications.

SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. It offers the following services to its users:

- acknowledged error-free non-duplicated transfer of user data,
- data fragmentation to conform to discovered path MTU size,
- sequenced delivery of user messages within multiple streams, with an option for order-of-arrival delivery of individual user messages,
- optional bundling of multiple user messages into a single SCTP packet, and
- network-level fault tolerance through supporting of multi-homing at either or both ends of an association.

The design of SCTP includes appropriate congestion avoidance behavior and resistance to flooding and masquerade attacks.

SCTP je relativno mlad protokol tako da se danas retko sreće u upotrebi. Takođe, i podrška za ovaj protokol u operativnim sistemima je uglavnom u eksperimentalnoj fazi. Međutim, ovaj protokol je pomenut zbog svoje važnosti kao protokol koji u budućnosti može objediniti prednosti TCP i UDP protokola.

9.4. Sequenced Packet Exchange (SPX) protokol

Sequenced Packet Exchange (SPX) protokol je protokol transportnog sloja koji se koristi kao podrazumevani transportni protokol kod Novell NetWare operativnih sistema. Ovaj protokol se koristi u kombinaciji sa IPX protokolom mrežnog nivoa. SPX protokol omogućava pouzdan prenos podataka sa ostvarivanjem veze i najbliže se može uporediti sa TCP protokolom. SPX protokol je razvijen na osnovu Sequenced Packed Protocol (SPP) rešenja kompanije Xerox.

S obzirom na popularnost operativnih sistema kompanije Novell početkom 90-ih godina 20. veka, IPX/SPX kombinacija protokola je u tom periodu predstavljala jedno od najpopularnijih rešenja za lokalne mreže. Danas, međutim, TCP/IP stek protokola predstavlja univerzalno i daleko češće korišćeno rešenje. Čak i NetWare operativni sistemi počev od verzije 5 podržavaju i komunikaciju putem TCP/IP protokola.

9.5. Internet SCSI (iSCSI)

Small Computer System Interface (SCSI) predstavlja skup standarda koji omogućavaju fizičko povezivanje i prenos podataka između računara i računarskih periferija. Najčešće korišćeni uređaj na SCSI interfejsu jesu SCSI hard-diskovi. Osim hard-diskova preko SCSI interfejsa je moguće povezati i uređaje za skladištenje podataka na magnetnoj traci, optički uređaji, skeneri i štampači. Jedna od glavnih prednosti SCSI uređaja jeste platformska nezavisnost tako da računari koji imaju SCSI interfejs poseduju SCSI kontrolere sa mikro-procesorima koji omogućavaju nezavistan rad periferija od centralnog procesora. Međutim, ovakav pristup podrazumeva visoku cenu SCSI rešenja tako da su ona danas u upotrebi samo kod skupih serverskih rešenja a na personalnim računarima se koristi znatno jeftiniji Integrated Drive Electronics (IDE) standard.

iSCSI (Internet SCSI) je mrežni protokol koji omogućava korišćenje SCSI protokola u računarskim mrežama baziranim na IP protokolu. Ovaj protokol se ulgavnom koristi u brzim računarskim mrežama (npr. Gigabit Ethernet) za pridruživanje velike količine eksterne memorije serverima. Ovakve mreže se nazivaju Storage Area Network (SAN).

iSCSI protokol nije značajan u pogledu prenošenja podataka između velikog broja članova mreže. Međutim, namena iSCSI protokola je potpuno drugačija i ovaj protokol prikazuje tendenciju distribuiranja računarskih servisa koji su nekad bili čvrsto vezani za interne magistrale računara.

10. Sloj aplikacije

Sloj aplikacije predstavlja najviši sloj OSI i TCP/IP referentih modela i kao takav ovaj sloj se nalazi najbliže korisniku. Elemente na ovom sloju čine korisničke aplikacije koje koriste mrežne resurse i komunikaciju. Elementi aplikativnog sloja se kod OSI modela obraćaju sloju prezentacije dok je prvi sloj ispod sloja aplikacije kod TCP/IP modela transportni sloj. Postoje i slučajevi kod kojih se aplikacija direktno obraća nižem sloju od transportnog (npr. korisnički alat *ping* koristi direktno usluge ICMP protokola).

10.1. Telnet

Osnovna uloga telnet servisa jeste da omogući rad korisnika na udaljenim računarima (najčešće pod UNIX operativnim sistemom). Ovaj servis je izgrađen na klijent-server arhitekturi što znači da zahteva od korisnika posedovanje klijentske aplikacije i da na računaru na koji korisnik želi da se poveže bude instalirana serverska komponenta servisa. Nakon uspostavljanja inicijalne veze telnet protokola ovaj servis poprima karakteristike host-based arhitekture. To znači da svaka operacija od strane klijenta (npr. pritisak tastera na tastaturi) se istovremeno prosleđuje serveru. Na taj način korisnik može obavljati operacije na udaljenom računaru na isti način kao da sedi direktno ispred računara i koristi lokalnu tastaturu i monitor.

Jedan od glavnih razloga zašto se danas telnet retko koristi za udaljeni pristup računarima jeste pojava grafičkog korisničkog interfejsa (eng. GUI) za koji ovaj protokol nije dizaniran. Dodatni razlog pada popularnosti ovog servisa jeste bezbednost. Telnet protokol sve akcije korisnika (uključujući i slanje korisničkog imena i lozinke) i rezultate instrukcija šalje u izvornom obliku što ga čini nebezbednim za korišćenje na mrežama čije je kanale moguće prisluškivati.

Bez obzira na sve ređu upotrebu telnet servisa za rad na udaljenim računarima većina modernih operativnih sistema danas se isporučuje sa uključenom klijentskom komponentom. Razlog ovome jeste mogućnost korišćenja telnet klijenta za pristup serverskim komponentama ostalih servisa.

```
bash-3.1$ telnet mail.singidunum.ac.yu 110
Trying 212.62.48.42...
Connected to mail.singidunum.ac.yu.
Escape character is '^]'.
+OK
user korisnik
+OK
pass lozinka
+OK
stat
+OK 1 870
quit
+OK
Connection closed by foreign host.
bash-3.1$
```

Slika X - Pristup POP3 serveru putem telnet klijenta

Formalna specifikacija telnet protokola je data u RFC 2355 i RFC 854 dokumentima dostupnim na Web sajtu IETF-a (www.ietf.org). Podrazumevani port telnet servisa je 23 a transportni protokol TCP. Za naslednike telnet protokola mogu se smatrati SSH (Secure Shell, obezbeđuje sigurnost putem šifrovanja podataka) na UNIX i Remote Desktop (omogućava grafički korisnički interfejs) na MS Windows platformi.

10.1.1.Secure Shell (SSH)

Osnovna uloga SSH servisa jeste da omogući bezbedan pristup i rad na udanjenom računaru. Ovaj servis je nasledio većinu osobina Telnet servisa s tom razlikom što SSH podatke prenosi u šifrovanom obliku.

```
bash-3.1$ ssh korisnik@server
korisnik@server's password:
Last login: Thu Mar  1 15:40:53 2007 from 192.168.1.10 Linux 2.6.18
korisnik@server:~$ ls -la
total 4
drwxr-xr-x  5 korisnik users  144 2007-02-28 12:44 .
drwx--x--x 68 korisnik users 4192 2007-03-02 13:22 ..
drwxr-xr-x  4 korisnik users  152 2006-12-16 09:28 2006-12-16-10
drwxr-xr-x  4 korisnik users  152 2006-12-16 10:43 2006-12-16-11
drwxr-xr-x  4 korisnik users  152 2006-12-16 13:00 2006-12-16-13
korisnik@server:~$ exit
logout
Connection to server closed.
bash-3.1$
```

Slika X - Primer korišćenja SSH servisa

SSH servis se uglavnom koristi za udaljeni rad na Unix računarima s tim da postoji i veći broj klijenata za ostale platforme. Osim rada na udaljenim računarima SSH protokol se može iskoristiti i kao podloga za FTP protokol tj. siguran prenos fajlova.

10.1.2.Remote Desktop

Zadatak *Remote Desktop* servisa jeste da omogući pristup i rad na udaljenim računarima na kojima je instaliran MS Windows i uključen *Microsoft Terminal Services*.

Slika X - Primer klijentske aplikacije Remote Desktop servisa

Prednost SSH i Telnet servisa u odnosu na Remote Desktop jeste prenos manje količine podataka. Zbog prenosa grafičkih elemenata korisničkog interfejsa Remote Desktop može pokazati lošije performanse na sporijim vezama.

10.2. Domain Name System (DNS)

Domain Name System (DNS) je sistem koji čuva informacije vezane za *imena domena* u vidu distribuirane baze podataka na mrežama (npr. Internetu) a realizovan je kao klijent-server servis. Najvažnija funkcionalnost DNS-a je prevođenje IP adresa u ime domena i obrnuto. Većina ostalih mrežnih servisa (Web, E-mail, FTP...) koristi ili ima mogućnost da koristi DNS servis. Na primer, jedna od funkcionalnosti DNS-a je i obezbeđivanje informacije o tome koji serveri su zaduženi za razmenu elektronske pošte za određeni domen. Bez ove funkcionalnosti DNS-a, servis za razmenu elektronske pošte ne bi mogao da funkcioniše.

10.2.1.Istorijat problema i rešenja

DNS se javio usled porasta veličine računarskih mreža, porasta broja računarskih mreža (i pojave Interneta) i potrebe za jednostavnijim adresiranjem računara na mreži. Pod jednostavnijim adresiranjem se u stvari podrazumeva prilagođavanje mrežnog adresiranja karakteristici ljudi da lakše pamte simbolička imena od brojeva (npr. lakše je zapamtiti "www.singidunum.ac.yu" od "212.62.45.222"). Problem je u početku bio rešen putem *hosts* fajlova na svakom od računara na mreži. Međutim, porastom broja računara u računarskim mrežama, nedostaci ovakvog rešenja su postali ozbiljan problem:

1. Uzmimo za primer računarsku mrežu od N članova.
2. N računara čuva informaciju o N članova te mreže u lokalnim *hosts* fajlovima:
    1. 192.168.1.1 računar1.lokalna-mreža
    2. 192.168.1.2 računar2.lokalna-mreža
    3. 192.168.1.N računarN.lokalna-mreža
3. Problem 1: dodavanjem novog računara u mrežu potrebno je:
    1. na N računara dodati novi zapis u *hosts* fajl
    2. na novom računaru uneti kompletan *hosts* fajl
4. Problem 2: izmenom postojećeg računara u mreži potrebno je:
    1. na N računara izmeniti postojeći zapis u *hosts* fajlu
5. Problem 3: uklanjanjem postojećeg računara iz mreže potrebno je:
    1. na N-1 računara dodati ukloniti zapis iz *hosts* fajla

Iz navedenog se jasno vidi da kod malih mreža *hosts* fajlovi mogu biti jednostavnije rešenje od DNS-a (jer nema potrebe za postavljanjem DNS servera) dok se kod velikih mreža administracija znatno otežava jer se pri svakoj izmeni mreže ona odnosi na sve računare u mreži.

Prvi korak ka rešavanju problema je bio distribuirani *hosts* fajl (jedan *hosts* fajl u mreži kome mogu da pristupaju svi članovi mreže) a problem je u potpunosti rešen 1983. godine kada je Pol Mokapetris izumeo DNS (RFC dokumenti 882, 883 a zatim i 1034, 1035).

10.2.2.Hosts fajlovi

Pojavljivanje DNS-a nije u potpunosti eliminisao korišćenje *hosts* fajlova. Ovi fajlovi postoje i u modernim operativnim sistemima (Linux, Unix, MS Windows XP...) i najčešće se koriste kod veoma malih mreža (najviše nekoliko desetina računara). Podrazumevani sadržaj *hosts* fajla je "127.0.0.1 localhost".

```
#
# hosts         This file describes a number of hostname-to-address
#               mappings for the TCP/IP subsystem.  It is mostly
#               used at boot time, when no name servers are running.
#               On small systems, this file can be used instead of a
#               "named" name server.  Just add the names, addresses
#               and any aliases to this file...
#
# By the way, Arnt Gulbrandsen <agulbra@nvg.unit.no> says that 127.0.0.1
# should NEVER be named with the name of the machine.
# It causes  problems
# for some (stupid) programs, irc and reputedly talk. :^)
#

# For loopbacking.
127.0.0.1               localhost
192.168.1.1             tool.local tool

# End of hosts.
```

Tabela 9.2.1-1 Primer /etc/hosts fajla na Linux sistemu

Hosts fajlovi se mogu koristiti u kombinaciji sa DNS-om. U tom slučaju oni imaju prioritet nad DNS-om tj. pri razrešavanju nekog imena prvo se proverava sadržaj *hosts* fajla a tek ukoliko on ne sadrži informaciju o traženom imenu upit se šalje DNS serveru. Ovakav redosled u razrešavanju imena ima svoje dobre strane:

- Moguće je "zaobići" DNS tj. moguće je zameniti adresu nekog računara pri lokalnom razrešavanju imena - unosom zapisa "0.0.0.0 ad.doubleclick.net" u hosts fajl lokalnog računara on neće biti u mogućnosti da pristupi stvarnoj adresi "ad.doubleclick.net". Posledica ovoga je da pri surfovanju Internetom nijedan sadržaj sa pomenute adrese neće biti dostupan. Međutim, kako sa pomenute adrese najčešće dolaze samo reklame, one neće biti dosupne tako da će se to odraziti kao veća

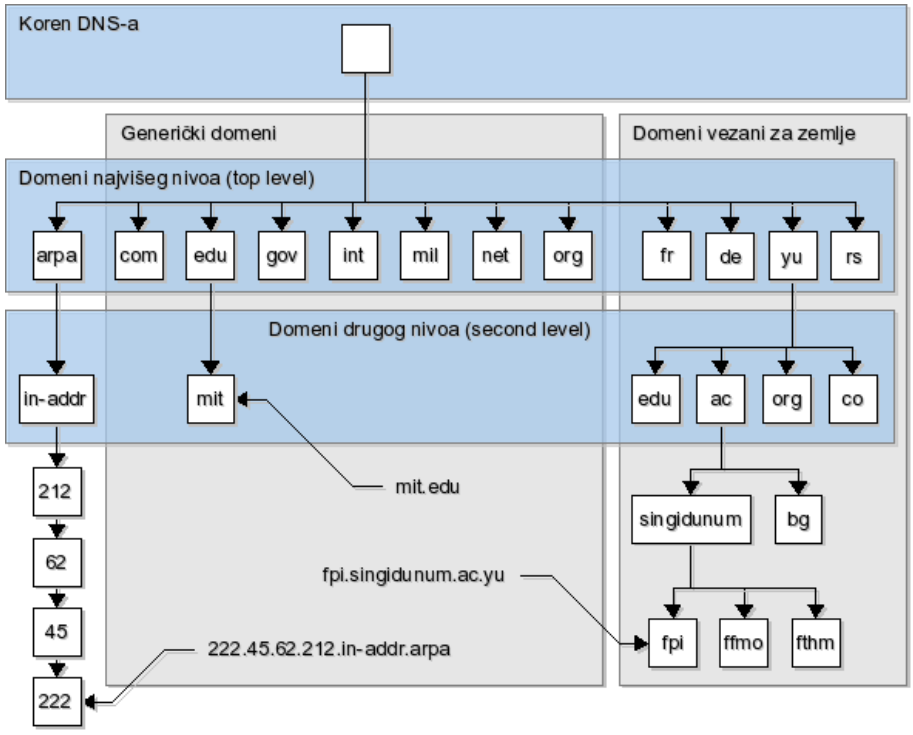
brzina učitavanja ostalih lokacija koje pored osnovnog sadržaja imaju i pomenute reklame.

ali i nedostatke:

- Zaobilaženje DNS-a je moguće je moguće kao posledica inficiranja sistema nekim trojancem/crvom. Primer:
  - Napadač kreira web stranicu na sopstvenoj IP adresi X.X.X.X koja je različita od IP adrese na kojoj se nalazi "www.google.com" - Y.Y.Y.Y
  - Web stranica na adresi X.X.X.X je takva da vizuelno u potpunosti odgovara originalnoj stranici na "www.google.com" ali su logika i baza podataka pretraživača koji stoji iza te stranice potpuno drugačije od onih na stvarnoj adresi pretraživača "www.google.com"
  - Lažni "www.google.com" na adresi Y.Y.Y.Y je namenjen za promociju klijenata koji napadaču za uzvrat daju novčanu nadoknadu
  - Napadač zatim kreira trojanca/crva koji se širi putem Interneta i u *hosts* fajl zaraženih računara unosi zapis: "X.X.X.X www.google.com"
  - Na ovaj način, svaki od zaraženih računara pri zahtevu za stranicom "www.google.com" pristupa lažnoj adresi X.X.X.X umesto Y.Y.Y.Y a korisnici dobijaju pogrešne informacije u korist napadača

10.2.3.Teorija rada DNS-a

Prostor domenskih imena je stablo za čiji svaki čvor postoji zapis u DNS-u nadležnom za tu zonu. U nadležnom DNS serveru (eng. *authoritative DNS nameserver*) je moguće za određenu zonu deklarisati pod-zone putem deklarisanja odgovarajućih DNS pod-servera.



Slika X - Hijerarhijska organizacija DNS-a

Za razumevanje DNS sistema i načina njegovog funkcionisanja potrebno je razumeti strukturu naziva domena (naziva domena, eng. *domain name*). Naziv domena se sastoji od dva ili više delova razdvojenih tačkom (tačkama). Uzmimo za primer domen `fpi.singidunum.ac.yu`:

- Prva oznaka sa desne strane predstavlja *top-level* domen (u ovom slučaju: yu).
- Svaka naredna oznaka gledano sa desne strane predstavlja pod-domen (u ovom slučaju: ac, singidunum i fpi). Maksimalan broj pod-podela je 127 a svaki od članova može imati maksimalnu dužinu od 63 karaktera s tim da celokupna dužina naziva (uključujući sve pod-domene i tačke kojim su

razdvojeni) ne sme preći 255 karaktera.

- Domen može imati jedan ili više *hostname*-ova kojima su pridružene realne IP adrese. (U našem slučaju, domen je fpi.singidunum.ac.yu a *hostname* bi mogao da bude www.fpi.singidunum.ac.yu sa odgovajućom IP adresom 212.62.45.222).

Kao što je rečeno, DNS čine hijerarhijski povezani DNS serveri. Za svaki od domena mora da postoji deklarisan jedan ili više nadležnih DNS servera koji su zaduženi za čuvanje i davanje informacija o navedenom domenu. Jedan DNS server može biti zadužen i za veći broj potpuno nezavisnih domena. U korenu stabla postoje specijalni DNS serveri koji se zovu *root serveri* i oni su zadužene za *top level domene* tj. domene na samom korenu stabla. Bez pomenutih *root servera* rad Interneta ne bi bio moguć jer oni čine osnovu svakog domenskog imenovanja na njemu. Trenutno postoji 13 *root servera* i njihova imena su A-M.root-servers.net.

Top-level domeni su prva s desna oznaka u svakom imenu domena (u pomenutom slučaju .yu domen). Postoje tri kategorije top-level domena:

- **top-level domeni vezani za zemlje**: domen dužine dva slova vezan za zemlju ili određeni geografski prostor (.yu - Jugoslavija, .jp - Japan, .ru - Rusija i sl.)
- **generički top-level domeni**: domen koji se koristi za određenu klasu organizacija (.com - commercial, .org - neprofitne organizacije, .net - network, .mil - military i sl.)
- **infrastrukturni top-level domeni**: jedini u ovoj grupi je .arpa domen.

Klijentske komponente DNS sistema su *resolver-i* tj. komponente na klijentskoj strani koje se obraćaju DNS serveru da bi od njih dobili IP adresu određenog domena. Resolver je sistemska komponenta koja se koristi posredno tj. putem programa koja je ova usluga potrebna. Resolver koristi sistemske mrežne parametre koji najčešće sadrže IP adresu jednog ili dva DNS servera. Primer korišćenja DNS usluge:

1. Aplikacija (npr. web browser) dobija URI adresu:
   http://www.fpi.singidunum.ac.yu/index.php
   od strane korisnika i raščlanjuje je na:
2. protokol (http)
3. hostname (www.fpi.singidunum.ac.yu)
4. adresu dokumenta (/index.php)

5. Aplikacija se obraća resolveru za dobijanje IP adrese hosta www.fpi.singidunum.ac.yu
6. resolver se obraća DNS serveru iz mrežne konfiguracije računara sa pitanjem:
   "Da li znaš na kojoj je IP adresi www.fpi.singidunum.ac.yu ?"
7. Ukoliko DNS kome se resolver obratio nije nadležan za domen "fpi.singidunum.ac.yu" on se obraća jednom od *root servera* sa pitanjem:
   "Koji je DNS server nadležan za `yu` domen?"
8. *Root server* šalje odgovor:
   "147.91.8.6"
9. DNS server se obraća serveru 147.91.8.6 sa pitanjem:
   "Koji je DNS server nadležan za ac.yu domen?"
10. Server 147.91.8.6 šalje odgovor:
    "147.91.8.6"
11. DNS server se obraća serveru 147.91.8.6 sa pitanjem:
    "Koji je DNS server nadležan za domen singidunum.ac.yu?"
12. Server 147.91.8.6 šalje odgovor:
    "212.62.48.42"
    "212.62.45.222"
13. DNS server se obraća serveru 212.62.48.42 sapitanjem:
    "Koji je DNS server nadležan za domen fpi.singidunum.ac.yu?"
14. Server 212.62.48.42 šalje odgovor:
    "212.62.48.42"
    "212.62.45.222"
15. DNS server se obraća serveru 212.62.48.42 sapitanjem:
    "Koja je adresa host-a www.fpi.singidunum.ac.yu?"
16. Server 212.62.48.42 šalje odgovor:
    "212.62.45.222"
17. DNS server vraća odgovor računaru čiji mu se *resolver* obratio:
    "IP adresa host-a www.fpi.singidunum.ac.yuje 212.62.45.222"
18. Na ovaj način aplikacija sa klijentskog računara dobija IP adresu HTTP servera i putem te adrese prosleđuje zahtev za web stranicom /index.php.

Ovaj primer objašnjava rekurziju u radu DNS-a. Takođe, iz primera se može

videti da jedan DNS server može čuvati informacije o više različitih domena kao i da više DNS servera mogu čuvati informaciju o jednom domenu (server 147.91.8.6 je nadležan za domene .yu i .ac.yu a serveri 212.62.48.42 i 212.62.45.222 su nadležni za domene singidunum.ac.yu i fpi.singidunum.ac.yu).

10.2.4.Keširanje kod DNS-a

U primeru rekurzivnog DNS razrešavanja datog u "Teorija rada DNS-a" prikazan je skup koraka koji je teoretski neophodno proći da bi klijent dobio informaciju od servera. U praksi, međutim, ovakav način rada kod svakog DNS upita za svaki Internet domen bi stvorio veliko opterećenje svih DNS servera koji učestvuju u razrešavanju određenog domena. Ovo se pre svega odnosi na *root* DNS servere i DNS servere kojima klijent direktno pristupa. Da bi se izbeglo pomenuto opterećenje uvedeno je keširanje upita.

Keširanje kod DNS-a ima za cilj da omogući svakom od DNS servera smanjenje broja upita koje on postavlja ostalim DNS serverima pri razrešavanju upita vezanog za domen iz zone za koju pomenuti server nije nadležan. Ukoliko je keširanje uključeno na DNS serveru on u internoj bazi čuva rezultate svih uspešno obavljenih razrešavanja tako da, ukoliko se isti upit ponovi, server ne mora da traži ponovo sve informacije od ostalih DNS servera već koristi potojeću informaciju iz baze.

Ovakav način rada štedi vreme i kapacitet mrežnog linka DNS servera ali otvara i novo pitanje:

- Ukoliko DNS server, putem skladištenja dobijenih informacija u svojoj bazi, nudi informacije klijentima o domenu za koji nije direkno nadležan, šta se dešava sa autoritetom DNS servera koji je nadležan za pomenuti domen? I, ukoliko se informacija o domenu na nadležnom DNS serveru izmeni, kako će se to odraziti na klijente koji vrše upit za taj domen posredstvom drugih servera koji u svojoj bazi imaju zabeleženu prethodnu informaciju?

Odgovor na ovo pitanje leži u TTL (time to live) parametru vezanom za domen. Ovaj parametar određuje nakon kog vremena će posrednički DNS serveri obnoviti informaciju u svojoj bazi vezanu za taj domen. TTL vreme se izražava u sekundama i najčešće je postavljeno na 86400 sekundi (10 dana). Ovo u praksi znači da je maksimalno vreme (nakon izmene domena na nadležnom DNS serveru) tokom koga će klijenti dobijati pogrešnu informaciju od posredničkih DNS servera, u ovom slučaju, 10 dana.

Ostali sistemski parametri svakog domena su i:

- Serial: serijski broj zone, uvećava se pri svakoj izmeni podataka, služi ostalim serverima za utvrđivanje da li se informacija izmenila na glavnom serveru.
- Refresh: broj sekundi nakon koga će *slave* i *secondary* serveri osvežiti svoje podatke za zonu.

- Retry: broj sekundi nakon koga će *slave* i *secondary* serveri ponovo pokušati osvežavanje podataka sa *master* servera ukoliko prethodni pokušaj ne uspe.
- Expire: broj sekundi nakon koga će *slave* i *i secondary* serveri odustati od pokušaja da osveže svoju bazu sa *master* servera ukoliko prethodni pokušaji ne uspeju.

10.3. File Transfer Protocol (FTP)

FTP (File Transfer Protokol) je protokol namenjen razmeni fajlova između računara koji imaju podršku za TCP/IP protokol. FTP je klijent-server protokol što znači da se njegova primena vrši putem serverskog programa na serveru i klijentske aplikacije na klijentu. Postoji veliki broj serverskih i klijentskih realizacija za različite operativne sisteme i uglavnom su besplatne.

10.3.1.Ciljevi i mane

Osnovni ciljevi FTP protokola su:

- omogućavanje razmene fajlova između računara
- omogućavanje indirektnog korišćenja udaljenih računara
- zaštita korisnika od različitih varijacija kod skladištenja fajlova na različitim sistemima
- pouzdan i efikasan prenos fajlova

Osnovne mane FTP protokola su:

- Pristupne lozinke i sadržaj fajlova se mrežom prenosi u izvornom obliku što ga čini nebezbednim.
- Za svaku operaciju (povezivanje, preuzimanje fajlova, listanje sadržaja, postavljanje fajlova) se koristi zasebna TCP/IP konekcija što može izazvati probleme ukoliko se prenos obavlja posredstvom računara sa firewall-om.
- Postoji mogućnost "uznemiravanja" 3. računara pri određenim zahtevima preko proxy servera.
- FTP je veoma latentan protokol usled velikog broja komandi potrebnih za iniciranje transfera.
- Ne postoji ugrađena mogućnost provere integriteta prenešenog fajla tako da se ovo najčešće obavlja zasebno preko md5 fajla.

10.3.2.Sigurni FTP

Glavni bezbednosni nedostaci FTP protokola su:

1. Korisničko ime i lozinka se preko mreže prenose u izvornom obliku.
2. Podaci koji se prenose protokolom prenose se u izvornom obliku.

Ovi nedostaci ne predstavljaju problem kod lokalnih mreža čiji se komunikacioni kanali najčešće smatraju bezbednim. Međutim, korišćenje FTP protokola putem mreže čije je kanale moguće prisluškivati (npr. Internet) otvara sledeće bezbednosne rizike:

1. Napadač može utvrditi koje operacije je korisnik izveo na serveru.
2. Napadač može utvrditi sadržaj fajlova koji su prenešeni FTP prokotokolom (u oba smera).
3. Napadač može utvrditi korisničko ime i lozinku korisnika.

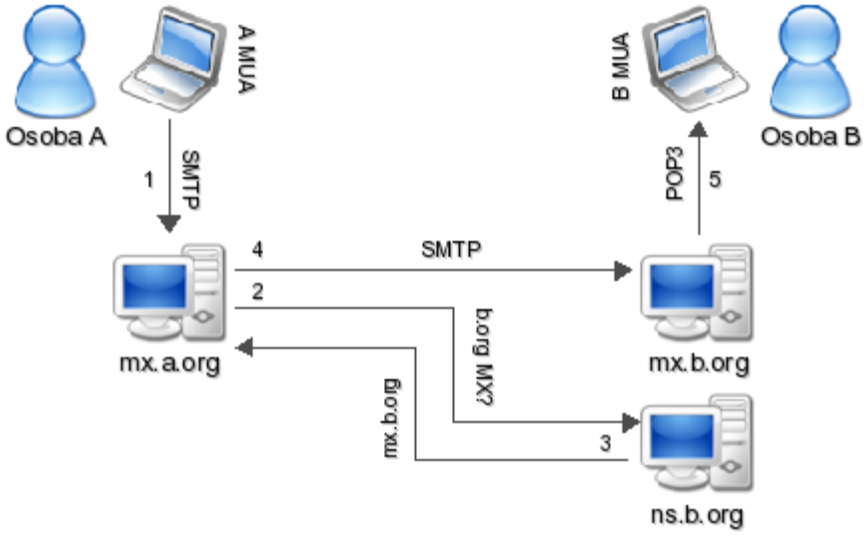
Usled pomenutih bezbednosnih rizika pri korišćenju FTP-a, pojavile su se dve različite implementacije sigurnog FTP-a:

8. SFTP (*SSH File Transfer Protocol*) - FTP baziran na SSH (*Secure SHell*) protokolu.
9. FTPS (*File Transfer Protocol over SSL*) - FTP sa korišćenjem SSL ili TLS enkripcije.

10.4. Elektronska pošta (E-mail)

E-mail servis je jedan od najčešće korišćenih servisa na Internetu. Ovaj servis postoji duže od samog Interneta. Prvi put je predstavljen 1965. godine za međusobnu komunikaciju korisnika na mainframe računarima. Ubrzo je dobio mogućnost rada i u mrežama tj. mogućnost razmene poruka između korisnika na različitim računarima. 1969. godine se pojavljuje simbol "@" za razdvajanje korisnika od mašine (korisnik@računar.mreža).

10.4.1.Principi rada e-mail servisa



Slika X - Princip rada e-mail servisa

Dijagram iznad prikazuje tipične korake koji se prolaze kada osoba A šalje osobi B poruku:

1. Osoba A sastavlja poruku koristeći e-mail klijentski program (*mail user agent* - MUA). U zaglavlje poruke ona unosi e-mail adresu primaoca (b@b.org). Nakon pisanja poruke ona zadaje komandu da se poruka pošalje.

2. MUA osobe A formatira u skladu sa Internet e-mail formatom, koristi internu informaciju za određivanje servera (u ovom slučaju: mx.a.org) za slanje e-mail poruka (*mail transfer agent* - MTA) i prosleđuje mu poruku koristeći *Simple Mail Transfer Protokol* (SMTP).

3. MTA mx.a.org nakon prijema poruke analizira odredišnu adresu (u ovom slučaju: b@b.org). Pošto deo nakon znaka @ određuje domen u kome se

korisnik nalazi, MTA posredstvom DNS servisa utvrđuje koji me mail server zadužen za prihvatanje e-mail poruka za taj domen.

4. DNS server zadužen za domen čijem je korisniku upućena poruka vraća informaciju ka MTA o tome koji je server zadužen za e-mail poruke za taj domen (u ovom slučaju: mx.b.org).
5. MTA smtp.a.org šalje poruku ka MTA mx.b.org korišćenjem SMTP protokola.
6. MTA mx.b.org nakon prijema poruke smešta poruku u lokalni mail box korisnika kome je namenjena (u ovom slučaju osoba B).
7. Server pod imenom mx.b.org je takođe dostupan i pod imenom pop3.b.org. Osoba B, koristeći svoj MTA pristupa serveru pop3.b.org korišćenjem POP3 (*Post Office Protocol* verzije 3) i sa njega preuzima sve novopristigle poruke (među njima i poruku od osobe A).

Pomenuti redosled koraka je primenjiv na većinu korisnika e-mail servisa. Ipak, moguće su sledeće alternative:

- Osoba A i osoba B ne moraju koristiti sopstveni MUA već u tu svrhu mogu iskoristiti Webmail uslugu.
- Računar osobe A može imati na sebi instaliran MTA tako da može preskočiti 2. korak.
- Osoba B ne mora pristupati pošti putem POP3 protokola već u tu svrhu može iskoristiti *Internet Message Access Protokol* (IMAP), može se na drugi način povezati na server i pročitati poruku direktno ili može koristiti WebMail uslugu.
- Domeni najčešće imaju više od jednog servera za prijem pošte tako da u slučaju da jedan otkaže jedan od ostalih preuzima ulogu.

10.4.2.Protokoli e-mail servisa

SMTP protokol predstavlja osnovni protokol za prenos elektronske pošte u računarskim mrežama i na Internetu. S obzirom na to da je ovo jedini opšte prihvaćeni protokol za prenos elektronske pošte podrazumeva se njegova podrška kod svih MTA softvera (Sendmail, MS Exchange, Postfix...).

```
FROM: "Adam Jones" <adam@jones.xyz>
TO: "Danny Carrey" <danny@carrey.zxy>
DATE: Fri 18 Feb 2005 16:27:01 GMT
SUBJECT: New song
Message-ID: 000a01c76701$b2a25600$f601f0d5@server
DATA
Danny, I believe that two notes would be enugh for entire song.
```

Listing X - Primer elektronske pošte u SMTP formatu

SMTP protokol se koristi za prenos pošte između e-mail servera, MTA (Mail Transfer Agent). Korisnici e-mail servisa koriste SMTP protokol samo za slanje elektronske pošte (prenos pošte od njhovog e-mail klijenta – MUA, Mail User Agent – do lokalnog SMTP servera). Za pristup e-mail porukama koje je server prihvatio u njihovo poštansko sanduče (eng. *Mailbox*) korisnici koriste POP3 ili IMAP protokole.

POP3 protokol predstavlja jednostavniji protokol koji pristup porukama obavlja putem sledećih akcija:

- povezivanje na server
- preuzimanje i uklanjajne poruka
- raskidanje veze sa serverom

IMAP kao noviji protokol nudi naprednije mogućnosti u radu korisnika sa elektronskom poštom. Ovaj protokol podrazumeva trajnije čuvanje poruka na serveru uz eventualno preuzimanje lokalnih kopija. Pomoću IMAP protokola je moguć i pristup više korisnika istom mailbox-u istovoremeno. IMAP protokol nudi više funkcionalnosti što zahteva više sistemskih resursa te je ovaj protokol ređe podržan od strane Internet provajdera koji imaju veliki broj korisnika.

10.5. SMB/CIFS

SMB (Server Messages Block) je protokol aplikativnog sloja OSI modela i najčešće se koristi za razmenu fajlova, štampača i serijskih portova između računara na mreži. Uglavnom se koristi na računarima pod MS Windows operativnim sistemima.

SMB je originalno predstavljen od strane IBM-a sa ciljem da od DOS-ovog "Interupt 33" lokalnog pristupa fajlovima napravi mrežni fajl sistem. Međutim, opšte rasprostranjena varijanta SMB-a je prilično izmenjena od strane Microsoft-a. 1998. godine je Microsoft lansirao inicijativu za promenu imena SMB-a u CIFS (*Common Internet File System*) jer je u SMB dodato mnoštvo novih mogućnosti: simbolički i tvrdi linkovi, veća veličina fajlova i pokušaj da se komunikacija ostvaruje direktno, bez korišćenja NetBios-a.

SMB je originalno dizajniran da radi na NetBios protokolu (koji radi na NetBEUI, IPX/SPX ili NBT protokolu) a od MS Windows 2000 operativnog sistema SMB može da radi i na TCP/IP protokolu. Usled neophodnosti za komunikacijom sa sistemima pod MS Windows operativnim sistemima, SMB je portovan i na Unix operativne sisteme u okviru Samba projekta. Takođe, postoje i druge, manje popularne, implementacije SMB protokola namenjene različitim operativnim sistemima.

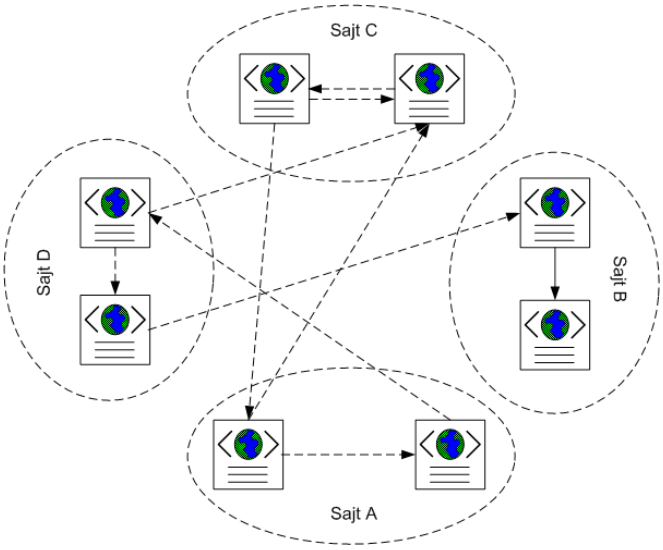
CIFS (Common Internet File System) predstavlja noviju verziju SMB-a koja podržava meko i tvrdo linkovanje, nudi funkcionalnosti koje nisu dostupne u SMB-u i radi na TCP/IP umesto NetBios protokolu. Kompanija Microsoft je 1996. godine nakon uvođenja pomenutih novina u SMB protokol pokrenula inicijativu za preimenovanje SMB protokola u CIFS. Specifikacija 1.0 verzije CIFS protokola je dostavljena IETF grupi za standardizaciju a Microsoft takođe sarađuje na primeni ovog protokola i sa ostalim zainteresovanim stranama.

Prevođenje sa NetBios na TCP/IP protokol omogućava CIFS protokolu rad na Internet mreži uz korišćenje DNS sistema za adresiranje članova. U mrežama sa više klijenata CIFS rešava problem konkurentnog pristupa fajlovima internim sistemima zaključavanja pristupa već otvorenim fajlovima.

10.6. HTTP, WWW i Web 2.0

10.6.1.Nastanak i uloga Web servisa

World Wide Web je najpristupačniji i najzastupljeniji Internet servis. Nastao je na osnovu idejnog projekta koji je napravio Tim Berners-Lee iz CERN-a, laboratorije za atomsku fiziku u Švajcarskoj. Tema projekta bila je sistem za hipertekst, odnosno metoda pronalaženja dokumenata na Internetu pomoću hiperveza (eng. hyperlink) koje upućuju na mesta gde se dokumenti nalaze.



Slika X - Princip povezivanja dokumenata na Web-u putem hiperveza.

Hiperveze se u HTML dokumentima realizuju putem označavanja dela dokumenta sa navođenjem ciljnog resursa. Ove veze mogu upućivati na određeni deo dokumenta u kome se nalaze, na neki drugi dokument na istom sajtu ili na dokument koji se nalazi bilo gde na Web-u (Internetu). Osim HTML dokumenata, hiperveze mogu upućivati i na ostale tipove dokumenata (slika, fajl...) dostupne na Web-u kao i na resurse ostalih servisa (e-mail, ftp...). Ukoliko hiperveza upućuje na nepostojeći dokument/resurs (što nije redak slučaj s obzirom na dinamičnost Web-a), takva hiperveza se naziva prekinutom (eng. broken link). Ovakvo povezivanje dokumenata predstavlja izuzetnu pogodnost za autore dokumenata jer mogu veoma lako da referenciraju druge dokumente. Danas postoje i sistemi koji sadrže baze podataka sa terminima i pridruženim referencama i koji automatski terminima u dokumentu pridružuju odgovarajuću hipervezu.

Osnovna namena hiperveza bila je jednostavno povezivanje dokumenata na Web-u. Razvojem tehnologija na kojima se zasniva Web hiperveze su postale nosilac

korisničke interakcije sa Web aplikacijama.

Trenutno nadležna organizacija za razvoj ovog servisa (i većine pratećih tehnologija) je World Wide Web Consortium (W3C). Na čelu ove organizacije se nalazi Tim Berners-Lee. W3C svoj uticaj na trazvoj Web-a vrši preko preporuka standarda. Takođe uticajna organizacija je i IETF (Internet Engineering Task Force). Ostale organizacije mogu same odrediti u kojoj meri će ispoštovati propisane standarde. Pre potpunog usvajanja, W3C preporuke prolaze kroz sledeće nivoe zrelosti:

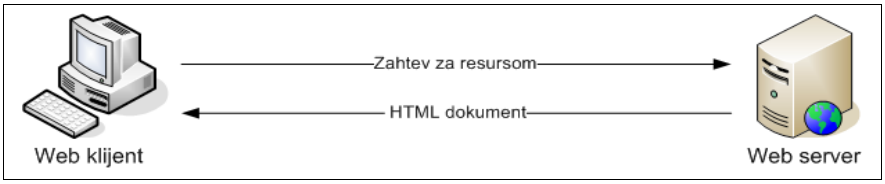
- Working Draft (WD)
- Last Call Working Draft
- Candidate Recommendation (CR)
- Proposed Recommendation (PR)
- W3C Recommendation (REC)

Napomena: World Wide Web servis se često skraćeno naziva Web servis. Razvojem Web-a pojavila se nova pod-tehnologija sa nazivom: Web servisi (eng. Web services). U daljem tekstu se pod nazivom Web servis podrazumeva celokupan World Wide Web servis dok god nije naznačeno drugačije.

10.6.2.Noseće komponente Web servisa

Web servis svoju popularnost u velikoj meri duguje svom modularnom i otvorenom dizajnu. Modularnost ovog servisa se ogleda u razdvajanju jedne relativno kompleksne arhitekture na jednostavnije komponente. Osnovne komponente Web-a su:

1. protokol kojim se servis distribuira (HTTP)
2. format dokumenata kojima se sadržaj servisa distribuira (HTML
3. server (Web server ili HTTP server)
4. klijent (Web čitač)
5. adresa dokumenta/resursa (URI/URL)



Slika X - Princip rada Web servisa.

Otvorenost ovog servisa znači da je specifikacija protokola i formata sadržaja javno dostupna tako da svaka zainteresovana strana može razvijati sopstvene serverske/klijentske komponente. To u praksi znači da postoji više različitih Web čitača kao i biblioteka pomoću kojih se sopstvenim programima mogu ugraditi Web funkcionalnosti.

Napomena: Iako otvorenost standarda sa jedne strane predstavlja razvojnu pogodnost, nekontrolisan razvoj (pre svega klijentskih) komponenti je doveo do određenih nekompatibilnosti različitih realizacija. Naime, čitači Web-a različitih proizvođača mogu različito prikazivati određene HTML dokumente (uglavnom samo određene HTML elemente). Ovaj problem je u ranoj fazi doveo i do degradacije HTML jezika jer su proizvođači ubacivali sopstvene, nestandardizovane elemente u sam HTML jezik. Problem je poznat pod nazivom "Browser War". Iako je sam HTML jezik "očišćen" od pomenutih ubačenih elemenata jačanjem autoriteta W3C-a i propisivanjem novih standarda (npr. XHTML), problem različite interpretacije HTML jezika još uvek postoji. Takođe, problem su nasledile i prateće Web tehnologije (npr. CSS).

10.6.3.HyperText Transfer Protokol (HTTP)

HyperText Transfer Protokol (HTTP) je osnovni protokol za distribuciju sadržaja na Web-u. Osnovna funkcionalnost ovog protokola je prenos zahteva za HTML dokumentima (od strane klijenta ka serveru) i prenost sadržaja HTML dokumenata (od strane servera ka klijentu). HTTP je protokol aplikativnog nivoa. Podrazumevani transportni protokol je TCP a port 80.

HTTP je protokol koji ne definiše stanje konekcije (eng. stateless). To u praksi znači da server ne čuva informacije o klijentu nakon obrade klijentskog zahteva tj. da se za svaki novi zahtev (od strane istog klijenta ka istom serveru, čak i istom resursu) ostvaruje potpuno nova veza. Problem je delimično rešen uvođenjem tzv. kolačića (eng. cookie) a postoje i alternativni načini rešavanja kod dinamičkih stranica. Drugi glavni problem kod HTTP protokola je ne posedovanje nikakvih sistema zaštite podataka koji se njime prenose. Ovaj problem je rešen uvođenjem HTTPS protokola (Secured HTTP).

10.6.4. Format dokumenata (HTML)

HTML (Hyper Text Markup Language) je jezik iz porodice jezika za označavanje (Markup Language). Jezici za označavanje se ponekad svrstavaju u programske jezike što je pogrešno. Uloga jezika za označavanje je da označe delove dokumenta. Na primer:

```
Ovo je <u>jezik za označavanje</u>.
```

predstavlja deo HTML dokumenta i u njemu je označeno da se reči uokvirene <u> i </u> oznakama (eng. tag) prikažu podvučene. Za sam prikaz je zadužen klijent (Web čitač). HTML dokumenti nisu predviđeni da sadrže binarne podatke (mada je moguće zaobilaženje ovog ograničenja) ali mogu imati reference prema binarnim resursima (npr. slici).

Klasičan HTML dokument se sastoji od dve celine: zaglavlja i tela dokumenta. Podaci u zaglavlju su namenjeni Web čitaču i sadrže informacije o naslovu dokumenta, ključnim rečima, datumu isticanja i sl. Telo dokumenta je deo koji je namenjen za prezentovanje (koje može biti prikaz na ekranu ali i zvučni izlaz) korisnicima.

```
<html>
   <head>
      <title>Naslov Dokumenta</title>
   </head>
   <body>
      Ovo je 1. red.<br />
      Ovo je 2. red.<br />
      Ovo je 3. red.<br />
      Ovo je <a href="http://www.singidunum.ac.yu">link</a>.
   </body>
</html>
```

Listing X - Primer HTML dokumenta.

Pregled svih HTML oznaka i njihovih atributa i vrednosti izlazi iz okvira ove knjige. Na zvaničnom sajtu W3C-a javno je dostupna puna specifikacija HTML standarda a postoji i veliki broj javno dostupnih materijala koji se bave HTML-om. Takođe postoji i veliki broj tekstualnih i grafičkih (tzv. WYSIWYG - What You See Is What You Get) editora koji olakšavaju rad sa HTML dokumentima. Najpoznatiji grafički editor je Dreamweaver, proizvod kompanije Macromedia koju je kupila kompanija Adobe.

10.6.5.Server (Web/HTTP server)

Osnovna uloga Web servera (nekad se naziva i HTTP serverom) je da osluškuje na portu 80 (podrazumevani port za HTTP protokol), na dobijeni zahtev pronađe traženi dokument u lokalnom skladištu dokumenata i njegov sadržaj pošalje klijentu ili, u slučaju da traženi dokument ne postoji, klijentu pošalje poruku o grešci. Ipak, ovakav scenario opisuje samo osnovnu funkcionalnost Web servera. Savremeni Web serveri imaju mnoge dodatne funkcionalnosti o kojima će više reči biti u delu *9.6.3.1 - Razvoj serverskog dela*.

Trenutno najpopularniji softver ovog tipa je Apache HTTP server čiji je autor Apache Foundation. U trenutku pisanja ove knjige (oktobar 2006.) pomenuti softver je (prema podacima kompanije Netcraft) opsluživao 61,44% svih sajtova na Internetu. Sledeći najzastupljeniji softver je IIS, proizvod kompanije Microsoft, sa 31,35% tržišta.

10.6.6.Klijent (Web čitač)

Osnovna uloga Web čitača (eng. Web browser, User Agent) je da korisničke zahteve za HTML dokumentima (i ostalim resursima) prevodi u instrukcije HTTP protokola, šalje HTTP zahteve, prihvata HTML dokumente i prezentuje ih korisnicima. Pre samog slanja HTTP zahteva Web čitač ima zadatak da dekomponuje URL i u skladu sa rezultatom formira zahtev. Ipak, ovakav scenario opisuje samo osnovnu funkcionalnost Web čitača. Savremeni Web čitači imaju veliki broj dodatnih funkcionalnosti o kojima će više reči biti u delu *9.6.3.2 - Razvoj klijentskog dela*.

Slika X - Prikaz HTML dokumenta (9.6.2.2-1) u Mozilla Firefox Web čitaču.

Utvrđivanje zastupljenosti Web čitača na Internetu nije jednostavan zadatak i statistike različitih izvora variraju i do 30%. Prosečna statistika u trenutku pisanja ove knjige pokazuje oko 80% zastupljenosti Internet Explorer-a (Microsoft), 15% zastupljenosti Mozilla Firefox-a (Mozilla Foundation), 3% zastupljenosti Safari-ja (Apple) i 2% ostalih Web čitača (Opera, Netscape Navigator...). Takođe, zastupljenost varira i od područja tako da u Velikoj Britaniji odnos između Microsoft Internet Explorer-a i Mozilla Firefox-a je 88/10 procenata a u Nemačkoj 60/33 procenata.

Odabir Web čitača može biti uslovljen i platformom na kojoj će se on koristiti jer su određeni Web čitači dostupni samo na određenim platformama: Internet Explorer na Microsoft Windows operativnim sistemima (uz izuzetak starijih verzija koje imaju podršku za Mac OS), Safari samo na Mac OS... Neki od kriterijuma za odabir ovog softvera su:

- podrška za različite platforme,
- upravljanje beleškama (eng. Bookmark management),
- podrška za evidentiranje izvršenih akcija (eng. History list)
- upravljanje preuzimanjem fajlova (eng. Download managemenet),
- upravljanje lozinkama na sajtovima sa proverom autentičnosti,
- upravljanje formularima,

- podrška za Web pretraživače u vidu ugrađene komponente,
- podrška za tabove (podprozore u okviru jednog prozora),
- blokada/filtriranje Pop-Up reklama,
- mogućnost internog pretraživanja dokumenta,
- mogućnost uveličanja stranice (eng. zooming),
- podrška za audio interpretaciju sadržaja i navigaciju glasom,
- podrška za moderne Web tehnologije (CSS, Frames, XHTML, Java, XForms, Web Forms 2.0, RSS, Atom, MathML, SVG...),
- nivo podrške za JavaScript (JavaScript, ECMAScript 3, DOM1, DOM2, DOM3, XPath, DHTML, Ajax),
- kompatibilnost sa HTTP protokolom,
- podrška za SSL (Secure Socket Layer),
- podrška za ostale protokole (FTP, Gopher, BitTorent...),
- podrška za format slika (JPEG, GIF, PNG, TIFF, SVG...),
- podrška za PlugIn-ove (Flash, PDF, QuickTime...),
- mogućnost povezivanja sa okruženjem,
- podrška za lokalni jezik,
- broj grešaka/kritičnih grešaka i vreme potrebno proizvođaču za otklanjanje

10.6.7.Adresa dokumenta/resursa (URI/URL)

Uniform Resource Identifier (URI) predstavlja skup karaktera (slova, brojeva i specijalnih znakova) koji služi za identifikovanje resursa. Cilj identifikovanja je mogućnost pristupa svakom od resursa na mreži.

Uniform Resource Locator (URL) je podskup URI-a i njegov zadatak je, osim identifikovanja, opis akcije koju treba izvršiti nad resursom. URI/URL se sastoji od više delova. Na primer:

http://adamjones:46and2@www.singidunum.ac.yu:80/nastava/doc?naziv=studije#phd

čine sledeći delovi:

1. šema: http
2. korisnik: adamjones
3. lozinka: 46and2
4. host: www.singidunum.ac.yu
5. port: 80
6. putanja: nastava/dokument
7. upit: naziv=studije
8. fragment: phd

Pomenuti primer predstavlja URL sa svim komponentama. U praksi, korisnici najčešće ručno unose samo osnovni URL (npr. www.singidunum.ac.yu) a komplikovanijim URL-ovima pristupaju putem hiperveza sadržanih u HTML dokumentima.

10.6.8.Evolucija Web servisa

Ranije pomenuta modularnost Web servisa omogućila je nezavistan razvoj svake od njegovih komponenti. Naravno, određene izmene jedne komponente zahtevale su izmene ne ostalim komponentama ili su stvarale mogućnost unapređenja ostalih komponenti. Takođe, planirani i prateći efekti razvoja Web-a doveli su do novih servisa, pristupa i tehnologija vezanih za ovaj servis. Na primer, omasovljenje javno dostupnih dokumenata na Web-u uslovilo je pojavljivanje Web direktorijuma a kasnije i pretraživača, servisa za filtriranje po određenom kriterijumu itd.

Web servis (pored E-mail servisa) predstavlja najpopularniji servis Interneta. Takođe, on predstavlja i servis koji je najviše evoluirao od svog nastanka. Međutim, bez obzira na broj uvedenih funkcionalnosti, tehnologije na kojima se Web zasniva su još uvek u fokusu različitih razvojnih timova jer se u nekim krugovima smatra da one predstavljaju primarnu platformu za rad i razvoj aplikativnog softvera u budućnosti. Ciljevi Web-a 2.0 su usmereni ka korisničkim aplikacijama i mogu se porediti sa efektima Web-a prve generacije na korisničke dokumente.

10.6.9.Razvoj serverskog dela Web-a

Formalni zadatak u razvoju Web servera (i tehnologija na kojima su oni izgrađeni) jeste praćenje razvoja HTTP protokola i garantovanje kompatibilnosti sa njim. Ovaj zadatak je uspešno obavljan od većine proizvođača Web servera usled svega jedne ozbiljnije izmene HTTP protokola - prelazak sa verzije 1.0 na trenutno aktuelnu verziju 1.1. Ipak, fokus u razvoju Web servera je postavljen na:

- uvođenje tehnologija koje omogućavaju dinamičko kreiranje Web dokumenata
- garantovanje bezbednosti na različitim nivoima korišćenja Web servisa
- povećavanje vremena dostupnosti servisa

Uvođenje tehnologija koje omogućavaju dinamičko kreiranje Web dokumenata predstavlja most Web-a ka ostatku informacionog okruženja. Tehnologije za dinamičko kreiranje Web dokumenata su svoje postojanje započele više kao dekorativni element HTML stranica (npr. uključivanje trenutnog datuma/vremena u sadržaj dokumenta, primitivne personalizacije i sl.) a danas predstavljaju osnovu Web-a 2.0 i imaju tendenciju da putem Web aplikacija smanje ili čak izbace iz upotrebe standardne korisničke aplikacije. Jedna od osnovnih uloga tehnologija za dinamičko kreiranje Web dokumenata je korišćenje podataka kroz DBMS (DataBase Management System). Sistemi koji koriste dinamičko kreiranje dokumenata radi lakše organizacije sadržaja se nazivaju Sistemi za Upravljanje Sadržajem (eng. Content Management Systems - CMS).

Postoji više različitih tehnologija za kreiranje dinamičnih Web dokumenata na Web serveru (eng. server-side). Tri trenutno najpopularnije tehnologije su:

- Microsoft: Active Server Pages (ASP)
- Sun Microsystem: Java Server Pages (JSP)
- The PHP Group: PHP Hypertext Preprocessor (PHP)

Active Server Pages (ASP) predstavlja tehnologiju kompanije Microsoft i dostupna je samo u okviru IIS (Internet Information Server) Web servera (takođe proizvod kompanije Microsoft). Poslednje verzije ASP podrške omogućavaju korišćenje .NET tehnologije. Većina ASP stranica je napisana u VBScript programskom jeziku ali je moguće koristiti i bilo koji drugi ActiveScripting jezik.

Java Server Pages (JSP) tehnologija se bazira na Javi. Odnosi se na ugnježdavanje java koda u HTML dokumente preko posebnih JSP tagova. Ovaj kod se izvršava na serverskoj strani dinamički neposredno pre isporuke stranice

klijentu. U novije vreme razvijeno su čitave biblioteke JSP tagova koje omogućavaju veću produktivnost u izradi Web aplikacija.

JSP predstavlja nastavak servlet tehnologije i njeno je proširenje. Prednost JSP-a je što je to u potpunosti objektno orijentisana tehnologija koja omogućava korišćenje svih funkcionalnosti Java jezika. Za korišćenje JSP-a koristi se aplikacioni serveri od kojih su najpoznatiji Tomcat, Sun Application Server, JBoss itd.

PHP Hypertext Preprocessor (PHP) je programski jezik orijentisan ka Web-u ali se danas, usled svoje popularnosti, može sresti i u grafičkim desktop aplikacijama, Unix skriptovima i sl. Prva verzija ovog jezika se pojavila 1994. godine a trenutno aktuelna verzija 5 datira iz 2005. godine. PHP se može koristiti na različitim platformama ali se najčešće sreće kod Apache Web servera na Linux operativnom sistemu. Korišćenje PHP-a je slobodno s obzirom na to da je njegov izvorni kod javno dostupan a njegova licenca ne podrazumeva plaćanje korišćenja.

Prednost JSP-a i PHP naspram ASP tehnologije je platformska nezavisnost. Java programski jezik je poznat po svom revolucionarnom konceptu vrituelne mašine (koja omogućava izvršavanje istog programa na različitim platformama) dok PHP predstavlja interpretirani programski jezik čiji je interpreter dostupan za različite platforme. Nasuprot tome, ASP tehnologija je usko vezana za Microsoft platformu što predstavlja značajno ograničenje.

Bezbednost. Uvođenjem aktivnih tehnologija u Web servere stvorene su i određene mogućnosti zloupotrebe propusta u procedurama samog Web servera kao i procedurama za dinamičko kreiranje dokumenata. Na primer, rane verzije Microsoft IIS-a su u sebi sadržale propust koji je napadaču omogućavao pristup svim sadržajima sa hard-diska servera unošenjem određene adrese dokumenta. Takođe, greške u procedurama kreiranja dinamičkih dokumenata mogu dovesti do sličnih problema.

Dodatni problem vezan za bezbednost jeste i držanje više sajtova na jednom Web serveru. S obzirom na to da broj sajtova po serveru u nekim slučajevima dostiže i nekoliko desetina hiljada a uglavnom se radi o sajtovima čiji se sadržaj (i procedure za generisanje dokumenata) ne kontroliše, to predstavlja dodatni izazov koji se stavlja pred proizvođače.

Povećavanje vremena dostupnosti servisa, performansi i otpornosti na greške je očekivan zahtev koji se stavlja pred tehnologije koje ulaze u privredu ili čak vojnu upotrebu. Svaka konekcija oduzima određenu količinu (konačnih) resursa na serveru a nije redak slučaj da istom resursu na Internetu u svega nekoliko sekundi pristupi više desetina hiljada korisnika. Takođe, određeni tipovi napada

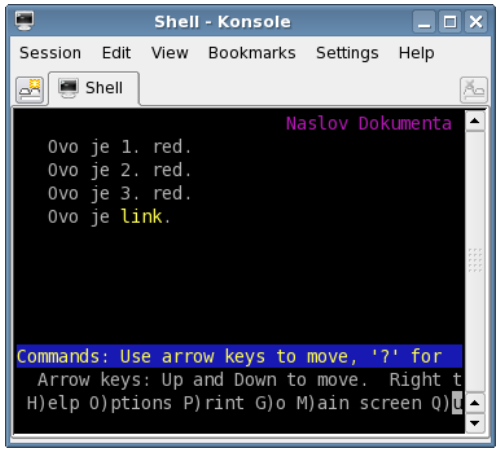
mogu namenski otvoriti veliki broj konekcija sa ciljem da server izvedu iz normalnog funkcionisanja ili onemoguće pristup ostalim korisnicima Interneta. Sa druge strane, kreiranje dinamičkih stranica na serveru je takođe proces koji zahteva određene resurse a u sebi može sadržati i procedure sa greškom (najčešće usled ljudskog faktora) što opet može dovesti do prestanka normalnog funkcionisanja servera. Prestanak normalnog funkcionisanja servera je situacija koja može imati negativne ekonomsko/bezbednosne posledice. Odgovori na pomenute probleme leže u skalabilnosti i robusnosti.

Skalabilnost predstavlja mogućnost povećanja performansi i dostupnosti (u skladu sa rastom zahteva) putem dodavanja hardverskih resursa. Skalabilnost može biti vertikalna - dodavanje resursa (procesora, memorije, spoljne memorije...) serveru koji je zadužen za servis - ili horizontalna - dodavanje većeg broja servera zaduženih za isti servis. Vertikalna skalabilnost je trenutno znatno ograničenija od horizontalne ali i zahteva manje (ili nikakve) izmene na softveru. Primer horizontalne skalabilnosti je klaster Web servera (grupa servera zadužena za isporuku sadržaja jednog Web sajta) a takav pristup zahteva i odgovarajući softver (npr. potreban je jedan server sa softverom koji omogućava deljenje sesije).

Robusnot predstavlja osobinu normalnog funkcionisanja u nepredviđenim uslovima. Ova osobina se može obezbediti određenim dizajnom softvera ili spoljnim tehnikama kao što je virtualizacija. Kao što je ranije pomenuto, jedan Web server može biti zadužen za više Web sajtova. Iako ovakav pristup smanjuje troškove (hardverske, mrežne, prostorne) njime se pojavljuje mogućnost da potpuno ispravan Web sajt bude nedostupan usled obaranja servera neispravnom procedurom za dinamičko kreiranje stranica ostalih sajtova. Karakteristika profesionalnih Web server softvera je lokalizovo područje (vremensko, procesno i memorijsko) eventualnih grešaka kao i mogućnost praćenja preko tzv. Log fajlova.

10.6.10.Razvoj klijentskog dela Web-a

Web klijenti (eng. Web browser) su prešli ogroman razvojni put od svog nastanka. Prvi popularni Web klijent je bio Mosaic, razvijen od strane NCSA (National Center for Supercomputing Applications) 1992/1993. godine. Jedna od glavnih karakteristika ovog softvera je bila podrška za različite operativne sisteme (Unix, MS Windows, Mac OS). Razvoj Mosaic-a je prekinut početkom 1997. godine.



Slika X - primer konzolnog Web klijena, Lynx-a.

Današnji Web klijenti predstavljaju ne samo interpretere HTML dokumenata već kompletan klijentski deo HTTP platforme distribuiranih aplikacija. Korišćenje različitih funkcionalnosti savremenih Web klijenata omogućava programerima da razvijaju samo određene delove klijentskog dela distribuiranih aplikacija a za ostatak iskoriste postojeće funkcionalnosti Web klijenata.

Jedna od prvih značajnih novina je bila uvođenje podrške za formulare (eng. form) u HTML jezik, HTTP protokol, Web klijente i Web servere. Značaj formulara ogleda se u tome što uvodi mogućnost dvosmerne komunikacije između klijenta i servera tj. omogućava korisnicima da serveru pošalju podatke određene formularom.

Sledeća značajna novina jeste uvođenje podrške za JavaScript programski jezik. Podrška za JavaScript omogućava proširivanje funkcionalnosti klijentskog dela putem uključivanja skriptova u HTMLdokumente.

Proširivanje funkcionalnosti Web klijenata je moguće i putem plug-in komponenti za koje klijent ima podršku. Neki od najpopularnijih tipova plug-in komponenti su Java, Flash, QuickTime i ActiveX. Java plug-in omogućava izvršavanje kompletnih Java apleta (eng. applet) na klijentskoj strani, Flash plug-

in je orijentisan ka grafičkim apletima sa animacijama, QuickTime omogućava prikaz video klipova a ActiveX tehnologija je vezana za Microsoft platformu i omogućava komunikaciju Web klijenta sa sistemskim resursima.

Proširivanje funkcionalnosti Web klijenata postavlja sledeće zahteve pred proizvođače i programere:

1. očuvanje kompatibilnosti sa W3C standardima
2. zaštita korisnika od zlonamernih resursa na Web-u.

Problem očuvanja kompatibilnosti sa W3C standardima utiče i na klijente i na autore Web sajtova. Naime, nepodržavanje W3C specifikacije dovodi do različite interpretacije istih dokumenata kod različitih Web klijenata. Razlike u interpretaciji mogu biti od čisto estetske prirode do potpune nefunkcionalnosti dokumenta/sajta. Sa druge strane, autori pokušavaju da putem određenih dodatnih direktiva izglade nekompatibilnosti (što dovodi do oštećenja strukture dokumenta ili, u najmanju ruku, nepotrebnog opterećivanja dokumenta). Autori koji ne uspeju da stvore dokumente koji će se identično interpretirati u različitim klijentima najčešće se odlučuju za podršku samo jednog od najpopularnijih Web klijenata (i to naznače u dokumentu porukom: "Sajt je prilagođen Web klijentu X"). Na ovaj problem se oglasio i sam Tim Berners - Lee:

"Svako ko na svoj sajt postavi etiketu 'ovaj sajt je prilagođen klijentu X' izgleda da čezne za lošim starim danima, pre Web-a, kada su postojale veoma male šanse za čitanje dokumenta kreiranog na drugom računaru, u drugom tekstualnom editoru ili na drugoj mreži"

Tim Berners - Lee, Technology Review, Jul 1996.

S obzirom na to da nekompatibilnost Web čitača predstavlja ozbiljnu prepreku za razvoj Web-a, postoji više inicijativa koje imaju za cilj da proizvođače nateraju na potpuno poštovanje W3C standarda. Najpoznatija inicijativa "AnyBrowser" se nalazi na adresi: http://www.anybrowser.org/campaign/.

Dodavanje novih funkcionalnosti postavlja pred autore Web klijenata dodatni zahtev - očuvanje bezbednosti i privatnosti korisnika. Podržavanje aktivnih tehnologija na klijentskoj strani može dovesti do ubacivanja zlonamernog koda u računare korisnika i na taj način do neovlašćenog pristupa privatnim podacima korisnika. Ovakvi propusti su česti a proporcionalno su opasni stepenu integracije Web klijenta sa ostatkom okruženja. Internet Explorer, kao jedan od najpopularnijih Web klijenata danas, često je uzrok bezbednosnih problema na Windows operativnim sistemima. Na primer, u verziji 7 Internet Explorer-a, puštenoj u opticaj sredinom oktobra 2006. godine, ozbiljan sigurnosni propust je pronađen za manje od 24 časa nakon objavljivanja.

10.6.11.Razvoj HTTP protokola

HTTP protokol predstavlja komponentu Web-a koja je pretrpela najmanji broj izmena od svog pojavljivanja. HTTP protokol se razvijao u dva pravca - ka dodavanju novih funkcionalnosti i ka obezbeđivanju bezbednog transporta podataka.

Prva verzija HTTP protokola koja se našla u široj upotrebi bila je verzija 0.9 i datira iz 1991. godine. Ova verzija je podržavala samo metod GET (što znatno ograničava količinu informacija koju klijent može da dostavi serveru) i nije imala podršku za zaglavlja na nivou HTTP protokola tako da je već 1992. godine zamenjena novijom verzijom. Naredna verzija iz 1999. godine - HTTP/1.0 - donela je podršku za nove metode, zaglavlja i sl. Verzija 1.0 je još uvek u širokoj upotrebi iako je poslednja predložena verzija 1.1. Glavne novine HTTP/1.1 verzije su mogućnost stalnih konekcija i istovremeno slanje više zahteva. Danas, HTTP protokol podržava sledeće metode:

1. HEAD
2. GET
3. POST
4. PUT
5. DELETE
6. TRACE
7. OPTIONS
8. CONNECT

10.6.12.XHTML, CSS, XML, XSLT

Razvojem HTML-a, a pre svega tehnologija za kreiranje dinamičkih dokumenata, iskristalisala se potreba za razdvajanjem strukture i sadržaja od prezentacije (prikaza). Ova potreba se dodatno povećala uvođenjem tehnologija koje omogućavaju osobama sa oštećenim čulom vida da koriste računare preko audio interfejsa.

Glavno unapređenje se javilo u vidu CSS-a (Cascading Style Sheets), tehnologije koja omogućava nezavisno definisanje prikaza elemenata HTML-a.

```
p {
            margin: 10px;
            border-width: 3px;
            border-style: double;
            border-color: #FF0000;
            padding: 20px;
            background-color: #0000FF;
            text-align: justify;
            text-transform: uppercase;
            font-family: Times New Roman;
            font-size: 11pt;
            font-weight: bold;
}
```

Listing X - primer CSS definicije prikaza <p> elementa.

Uvođenje CSS tehnologije je omogućilo prečišćavanje HTML-a tj. izbacivanje oznaka (tagova) i atributa koji se odnose na definisanje prikaza a ne na strukturu i sadržaj. Rezultat ove izmene je XHTML (Extensible HyperText Markup Language) format čija je specifikacija znatno restriktivnija.

Pored XHTML-a, XML (Extensible Markup Language) predstavlja još jedan od Markup jezika koji se koriste u okviru Web servisa (s tim da primena XML-a nije ograničena samo na Web). XML je jezik orijentisan ka strukturi dokumenta i ne podrazumeva bilo kakvu definiciju prikaza. Ova osobina čini XML jezikom čiji su dokumenti pre ulaz računarskog programa nego dokumenti koji će interpretirati Web klijent (Web browser). XML dokumente je moguće prikazati direktno u Web klijentima preko dva tipa transformacija:

1. definisanja prikaza elemenata putem pomenutih CSS definicija
2. prevođenja dokumenata u (X)HTML putem XSLT transformacija

XSLT (Extensible Stylesheet Language Transformations) je jezik baziran na XML-u i koristi se za prevođenje XML podataka u neki drugi format. Uz korišćenje XSLT-a, XML dokumenti se mogu prevesti u HTML format na svakom Web klijentu koji ima XSLT procesor.

10.6.13.Nastanak i razvoj Web direktorijuma i pretraživača

Umnožavanje Web sajtova i dokumenata na Internetu dovelo je do potrebe za indeksiranjem resursa radi lakšeg pronalaženja željenog sadržaja. Prvi odgovor na ovaj problem se javio u vidu Web direktorijuma a kasnije, kada su se i Web direktorijumi pokazali nemoćnim pred količinom sadržaja, u vidu Web pretraživača.

Web direktorijumi (eng. Web directory) predstavljaju specijalne Web sajtove čiji sadržaj čine linkovi ka ostalim sajtovima organizovani po određenom kriterijumu. Web direktorijumi su najviše polu-automatizovani i zahtevaju dosta ljudskog rada za očuvanje ažurnosti baze. Danas, Web direktorijumi uglavnom postoje kao usko specijalizovani sajtovi za neku oblast. Neki od najpopularnijih opštih Web direktorijuma su Yahoo! Directory, Open Directory Project (ODP)...

Web pretraživači (eng. search engine) predstavljaju specijalne Web sajtove čija je uloga da korisnicima omoguće pretragu celokupnog Web-a na osnovu ključnih reči. Osnovne operacije koje Web pretraživači obavljaju su:

- krstaranje Web-om
- indeksiranje sadržaja
- pretraga indeksiranog sadržaja na zahtev korisnika

Krstarenje Web-om (eng. Web crawling) se obavlja preko namenskog Web klijenta (tzv. Web pauk, eng. Web spider) koji prati sve hiperveze u učitanom dokumentu. Sadržaj koji ovaj Web klijent učita se ne interpretira za pregled od strane korisnika već se indeksira (smešta u bazu Web pretraživača). Ovakve baze su posebno organizovane da bi se što brže pretraživale na zahtev korisnika.

Korišćenje Web pretraživača se najčešće vrši unosom kriterijuma u formulare na sajtu pretraživača nakon čega pretraživač prikazuje hiperveze ka sajtovima (dokumentima na sajtu) koji ispunjavaju zadate kriterijume. Današnji Web pretraživači imaju različite pristupne interfejse pa se mogu kao servis integrisati u ostale sajtove, desktop aplikacije i sl. Najpopularniji Web pretraživači danas su Google, Yahoo!, MSN Search...

10.6.14.Ostali izvedeni servisi

Ubrzan razvoj Web-a ne samo da ga čini najpopularnijim servisom Interneta već u njega unosi funkcionalnosti ostalih servisa. Trenutne mogućnosti tehnologija na kojima se Web zasniva daleko prevazilaze potrebe povezivanja dokumenata i omogućavaju integraciju sa ostalim servisima ili, čak, potpuno preuzimanje uloge nekog drugog servisa. Na primer, diskusione grupe, koje su nekad funkcionisale preko e-mail servisa, danas se češće dostupne putem Web-a u obliku Web foruma. Takođe, IRC (Internet Relay Servis) servis danas ima Web klijente ili čak kompletnu realizaciju putem Web tehnologija. E-mail servis, sledeći najpopularniji servis na Internetu, danas se često koristi putem Web interfejsa. Ovakav izveden Web servis se naziva WebMail.

Zahvaljujući razvoju tehnologija na kojima se zasniva Web danas su česti potpuno novi servisi na Web-u. Može se reći da većina postojećih servisa koji imaju mogućnost automatizacije bira Web kao noseći informacioni servis. Takođe, nije redak slučaj da se zbog pogodnosti u radu sa Web tehnologijama one biraju kao nosilac interfejsa ka ostalim informacionim servisima.

10.6.15.Web 2.0 (Web aplikacije)

Web 2.0 predstavlja sledeću generaciju usluga koje su dostupne na World Wide Web-u. Ove usluge omogućavaju korisnicima da sarađuju i razmenjuju informacije putem Web-a. U poređenju sa Web-om prve generacije, Web 2.0 korisnicima nudi interfejse koji više liče na desktop aplikacije nego na dokumente.

Osnovne tehnike na kojima se zasniva Web 2.0 su:

- web services - softverski sistemi koji omogućavaju međusobnu komunikaciju mašina putem mreže.
- Ajax (Asynchronous JavaScript And XML) - tehnika za kreiranje interaktivnih Web aplikacija. Cilj ove tehnike je podela stranice na dinamičke delove koji šalju odvojene zahteve i na taj način mogu komunicirati sa serverom (serverima) nezavisno.
- web syndication - forma udruživanja Web sajtova tako da je sadržaj na jednom sajtu dostupan za korišćenje i na ostalima.

10.7. Network Time Protocol (NTP)

U računarskim mrežama koje čine serveri različitog tipa (aplikativni, komunikacioni, baze podataka) ili klasteri servera, često je potrebno ostvariti preciznu vremensku sinhronizaciju između svih članova mreže. Na primer, ukoliko u serverskoj mreži jedne banke postoje dva servera za baze podataka od kojih je jedan zadužen za evidentiranje uplata na račune klijenata a drugi za evidentiranje isplata, vremenska nesinhronizovanost ova dva servera kasnije može usloviti netačne informacije vezane za redosled uplata i isplata. Iako na prvi pogled vremenska sinhronizacija ne predstavlja veliki problem za njeno ostvarivanje je potrebno:

1. inicijalno sinhronizovati vreme na časovnicima svih računara u mreži i
2. povremeno izvršavati sinhronizaciju da bi se neutralisale razlike nastale u međuvremenu

Zadatak Network Time Protocol-a jeste da omogući sinhronizaciju vremena na časovnicima računara u mreži.

```
bash-3.1# /usr/sbin/ntpdate ntp.nasa.gov
15 Mar 12:02:46 ntpdate[]: step time server 198.123.30.132 offset 1.914867 sec
bash-3.1# /sbin/hwclock --systohc
bash-3.1#
```

Listing X - Primer sinhronizacije sa NASA NTP serverom

Network Time Protocol je protokol aplikativnog nivoa koji za rad koristi usluge UDP protokola transportnog nivoa a podrazumevani port 123. Jedan od glavnih problema vezan za sinhronizaciju vremena putem računarskih mreža jeste varijabilnost vremena potrebnog da se podaci sa NTP servera prenesu do klijenta. Za rešavanje ovog problema u NTP protokolu se koristi algoritam koji je Kejt Marculo predstavio 1984. godine u okviru svoje doktorske disertacije. Više informacija o ovom algoritmu se može naći na Web sajtu autora (http://www.cse.ucsd.edu/users/marzullo/).

Za korišćenje NTP protokola je potrebno imati NTP server u lokalnoj mreži ili koristiti neki od javno dostupnih NTP servera na Internetu (npr. ntp.nasa.gov). Takođe, jedan od najboljih pristupa jeste podešavanje automatske periodične sinhronizacije na svim klijentima. S obzirom na to da proces sinhronizacije ne zahteva značajne mrežne, procesorske i memorijske resurse period između sinhronizacija se može postaviti i veoma kratkim, posebno u situacijama kod kojih interni časovnici računara pokazuju znatno odstupanje.

10.8. Simple Network Management Protocol (SNMP)

Kod jednostavnih računarskih mreža sa malim brojem članova uglavnom nije teško utvrditi da se javio problem i šta je uzrok problema. Međutim, kod kompleksnih računarskih mreža koje čini veliki broj članova često je neophodno a uz to i veoma komplikovano predvideti moguće probleme, utvrditi da je do problema na mreži došlo i utvrditi njegovu lokaciju i uzrok. Uloga SNMP protokola jeste da administratorima obezbedi informacije vezane za samu računarsku mrežu koje je moguće iskoristiti za sprečavanje i rešavanje problema u radu mreže.

Za korišćenje SNMP protokola u mreži potrebno je obezbediti odgovarajuće karakteristike mreže. Mreže sa omogućenim SNMP-om se čine tri tipa SNMP komponenti:

1. Mrežni uređaji sa podrđkom za SNMP upravljanje (eng. *managed device*).
2. SNMP agenti.
3. Sistemi za upravljanje mrežom (eng. *Network Management System*, NMS).

Mrežni uređaji sa podrškom za SNMP upravljanje su članovi mreže koji sadrže SNMP agente. Ovi uređaji kreiraju bazu podataka koja sadrži informacije o njihovom radu u proteklom periodu. Podaci iz ove baze su dostupni sistemu za upravljanje mrežom (NMS) putem SNMP protokola. Uloga SNMP agenata je da podatke iz baze podataka mrežnog uređaja prevede u oblik definisan SNMP protokolom kao i da kontrolne podatke dobijene od NMS sistema primeni na lokalnom uređaju. Zadatak NMS sistema jeste da informacije dobijene od SNMP agenata analiziraju kao i da kontrolišu mrežne uređaje. U jednoj SNMP mreži se može nalaziti i više NMS sistema. Takođe, s obzirom na hijerarhijsku strukturu SNMP mreža, jedan mrežni uređaj može istovremeno funkcionisati i kao SNMP agent i kao NMS.

Jedan od glavnih problema vezanih za SNMP protokol jeste nedostadak provere autentičnosti u oba smera. Iz tog razloga većina proizvođača mrežne opreme u uređaje ugrađuje samo mogućnost davanja SNMP informacija bez mogućnosti podešavanja rada uređaja putem SNMP-a.

10.9. Voice over IP (Internet telefonija)

Razvojem računarskih tehnologija i tehnologija na kojima počivaju računarske mreže skup usluga koje one nude došao je do nivoa na kome te usluge prestaju da budu korisničke a postaju infrastruktura za usluge višeg nivoa. Jedna od usluga namenjenih korisnicima jeste telefonija - mogućnost udaljene komunikacije kroz prenos glasovnih poruka putem javne telefonske mreže. Ova usluga se pojavila kao posledica otkrića telefona 1876. godine od strane Aleksandra Grahama Bela. Telefoni kod tradicionalne telefonije se povezuju putem javne telefonske mreže koja se u svojim ranim fazama sastojala od analognih linija za povezivanje dva aparata. 1960. godine su napravljena prva prevođenja na digitalni sistem prenosa koji je omogućio veću fleksibilnost kroz korišćenje efikasnijih centrala i komunikacionih kanala veće propusne moći.

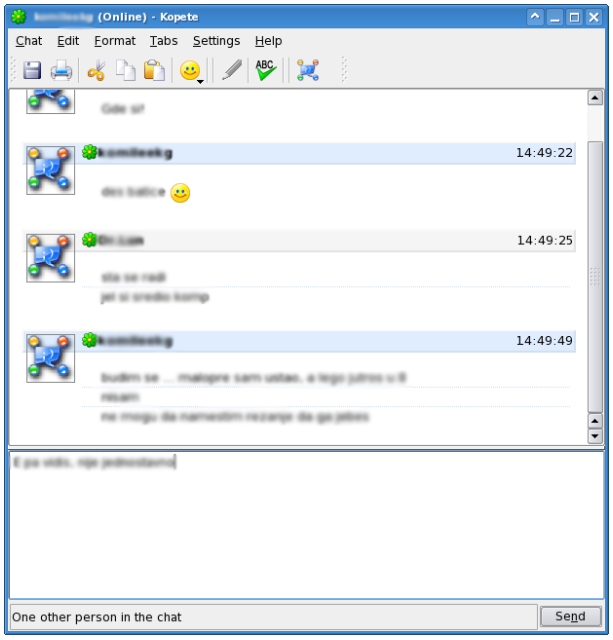
U ranim fazama razvoja Interneta kao najčešće korišćena fizička infrastruktura za povezivanje korisnika je korišćena javna telefonska mreža (PSTN, *Public Switched Telephone Network*) putem modemskih uređaja. Danas, potrebe korisnika Internet mreže daleko prevazilaze propusne moći koje omogućavaju modemski uređaji tako da se za pristup Internetu koriste druge infrastrukture (kanali kablovske televizije, satelitski linkovi, radio talasi itd.) i/ili komunikacioni uređaji (ISDT adapteri, ADSL modemi itd.). Ovaj podatak govori da infrastruktura na kojoj se zasniva Internet prevazilazi mogućnosti PSTN infrastrukture. Takođe, neuslovljenost komunikacije udaljenošću korisnika Interneta sa ekonomskog aspekta je dodatni parametar koji je uticao na prevođenje usluge telefonije na Internet infrastrukturu.

Internet telefonija (IP telefonija) je usluga bazirana na VoIP (*Voice over IP*) sistemu prenosa podataka koji primenjuje pravila IP protokola na glasovne poruke. Ovaj sistem omogućava prenos glasa računarskim mrežama koje se baziraju na IP protokolu. Prednosti ovakvog pristupa su značajne:

- Cena razgovora nije u direktnoj vezi sa fizičkom udaljenošću učesnika.
- Korišćenje VoIP telefona ne zavisi od fizičke lokacije korisnika što omogućava korišćenje istog odredišne identifikacije korisnika bez obzira na kojoj lokaciji je on priključen na Internet.
- ...

10.10.Instant Messaging

Instant Messaging (IM) ili servis za razmenu kratkih poruka je servis dostupan korišćenjem računarskih mreža a njegov razvoj se uglavnom podudara sa razvojem Internet mreže. Ovaj servis omogućava direktnu komunikaciju sa ostalim članovima mreže putem razmene kratkih pisanih poruka. Današnji IM servisi uglavnom nude i dodatne mogućnosti kao što su razmena fajlova ili čak neke oblike audio/video konferencija. IM servisi se uglavnom baziraju na nekoj vrsti Peer-to-Peer arhitekture. Klijenti IM servisa poruke najčešće razmenjuju direktno a za pronalaženje ostalih korisnika IM servisa u mreži koriste usluge centralnog IM servera.



Slika X - Primer IM klijenta Kopete

IM servis se može smatrati naslednikom nekada veoma popularnog IRC (Internet Relay Chat) servisa koji nudi sličnu uslugu ali sa tom razlikom što je realizovan na klijent/server arhitekturi te je za njegovo korišćenje potreban centralni server na koga su klijenti povezani putem komunikacionog kanala visoke propusne moći. Neki od najpopularnijim IM servisa jesu ICQ, AOL IM i MSN IM.

10.11. Video-konferencija

Servis video-konferencija omogućava prenos audio i video materijala u realnom vremenu sa ciljem omogućavanja održavanja sastanaka između osoba koje se nalaze na dve ili više udaljenih lokacija. Svi učesnici video-konferencija su opremljeni displejima sa zvučnicima za reprezentovanje materijala koji druga strana šalje kao i kamerama sa mikrofonima za slanje poruka drugoj strani. Učesnici video-konferencija mogu biti pojedinci sa ličnom opremom ali i grupe u specijalno opremljenim salama. Oprema i softver koji se koriste za video-konferencije se kreću u rasponu od ispod sto pa do nekoliko hiljada dolara u zavisnosti od kvaliteta i mogućnosti koje nude. Najveću korist od video-konferencija imaju poslovne organizacije koje na ovaj način mogu ostvariti značajnu uštedu štedeći novac i vreme potrebno za putovanje na lokaciju na kojoj bi se održala standardna konferencija.

Za korišćenje usluge video-konferencije je osim adekvatnog hadvera i softvera potrebno imati i vezu sa drugom stranom (ili drugim stranama) koja omogućava prenos audio i video poruka u realnom vremenu. Softver i uređaji koji se koriste kod video-konferencija uglavnom podržavaju kompresovanje/dekompresovanje audio i video materijala u cilju što efikasnijeg iskorišćenja komunikacionog kanala. Kod komunikacionih kanala male propusne moći uglavnom se pribegava kompromisu u pogledu kvaliteta audio/video poruka.

Većina proizvoda koji se koriste za održavanje video-konferencija se bazira na internim standardima proizvođača tako da kombinovanje rešenja različitih proizvođača najčešće nije moguće. Trenutno najčešće korišćeni javni standardi za kodiranje audio/video poruka su:

4. H.320
5. H.323
6. MPEG-2

Ovi standardi međusobno nisu kompatibilni ali postoje aplikacije koje omogućavaju korišćenje više od jednog standarda.

Poseban vid video-konferencija jeste *Webcasting*. On omogućava jednosmerni prenos audio/video materijala, od servera ka klijentima. Audio/video materijal se kreira i postavlja na server a klijenti zatim pristupaju materijalu. Za ovaj vid video-konferencija trenutno ne postoje formalni standardi ali na tržištu postoji veći broj rešenja baziranih na *de facto* standardima.

11. Bezbednost, dostupnost i performanse

U ranim fazama razvoja tehnologija na kojima se baziraju računarske mreže fokus je bio postavljen na omogućavanje što veće brzine prenosa podataka sa što manjom mogućnošću greške. Mala baza korisnika (koju su uglavnom činila tehnički visoko-obrazovana lica) i retke praktične primene omogućile su brz razvoj tehnologija i dovele računarske mreže do potencijala kojim prete da u potpunosti zamene ostale popularne sisteme komunikacije kao što su telefonija i televizija. Međutim, sa rastom popularnosti koja se bazira na povećanju baze korisnika računarske mreže su izašle iz čisto tehničko-tehnološkog domena i sve više na njihov razvoj i primenu imaju ekonomski i socijalni faktori.

Internet, kao najveća računarska mreža danas, se sastoji od miliona korisnika i stotina hiljada njima dostupnih servisa. Putem ove mreže se prenose lični podaci korisnika, obavljaju poverljive poslovne video-konferencije i razgovori, obavljaju finansijske transakcije, prenose poverljive vojne i državne informacije, obavljaju udaljeni hirurški zahvati i sl. Stoga, na primeru Internet-a možemo zaključiti da se putem računarskih mreža prenose vrednosti realnog sveta, daleko veće nego što je to slučaj kod telefonije i televizije. Međutim, svaka vrednost sa sobom nosi najčešće srazmeran rizik koga je, kako u realnom tako i u virtuelnom svetu računarskih mreža, cilj eliminisati ili u što većoj meri umanjiti. Postizanje ovog cilja pred inžinjere iterativno postavlja nove zadatke koji se rezultuju novim rešenjima. Ta rešenja mogu biti jednostavne tehničke izmene nosećih protokola ili kompleksni inteligenti softverski sistemi koji uče i svoje odluke donose putem heurističkih metoda.

Greške koje se javljaju na računarskim mrežama i kod resursa koji su putem njih dostupni možemo podeliti u četiri kategorije na osnovu uzroka njihovog pojavljivanja:

1. Greške koje se samoinicijativno pojavljuju usled propusta u definiciji hardverskih i softverskih komponenti računarskih mreža.
2. Greške koje se javljaju kao posledica neadekvatnog dizajniranja računarskih mreža i nenamenske upotrebe korišćenih komponenti.
3. Greške koje se javljaju usled neadekvatnog korišćenja računarskih mreža od strane korisnika nedovoljno obučenih za rad.
4. Greške koje se javljaju kao posledica iskorišćenja propusta u definiciji hardverskih/softverskih komponenti računarskih mreža, njihovom dizajnu i/ili (ne)pažnji korisnika a od strane zlonamernih korisnika i u cilju ostvarivanje određene koristi od napada na računarsku mrežu ili resurs.

Iako greške svih pomenutih kategorija mogu imati katastrofalne posledice, ovo poglavlje se bavi greškama četvrtog tipa jer se one mogu klasifikovati kao napadi

i sa sobom najčešće nose najveći negativan uticaj na poverljivost i dostupnost resursa i nesmetan rad mreže. Tema ovog poglavlja jeste bezbednost računarskih mreža ili tehnička rešenja za zaštitu računarskih mreža i putem njih dostupnih resursa od neregularnog korisničkog ponašanja.

11.1. Mogući napadi i zaštite računarskih mreža

Za određivanje efikasnih metoda za zaštitu računarskih mreža potrebno je prethodno izvršiti analizu čiji će rezultati sadržati dovoljan skup parametara koji karakterišu napade:

1. mogući izvori napada
2. mogući nosioci napada
3. mogući ciljevi napada
4. moguća ponašanja u okviru napada
5. mogući tragovi napada

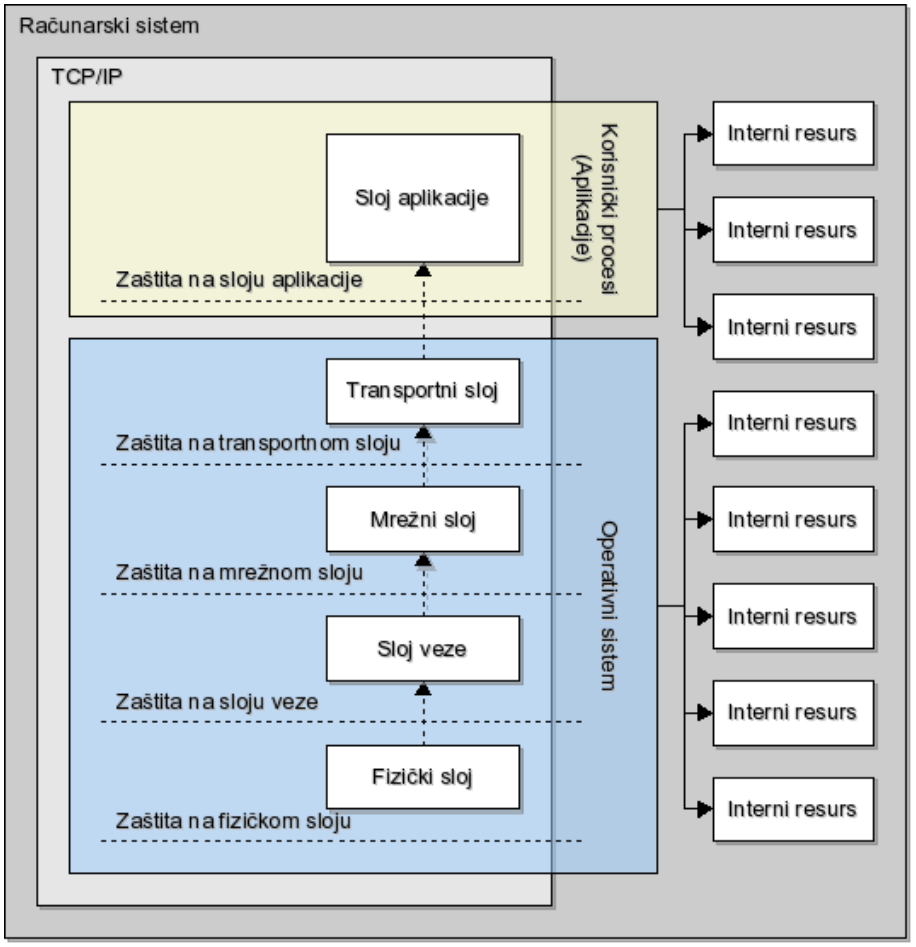
Podatak o mogućim izvorima predstavlja i socijalnu i tehničku karakteristiku napada što znači da se taj podatak može dobiti i na osnovu analize zaštićenih resursa sa socijalnog aspekta kao i na osnovu tehnički orijentisane analize već ostvarenog mrežnog saobraćaja. Podaci o izvorima napada se najčešće dobijaju iterativnim kombinovanjem podataka dobijenim analizama sa pomenutih aspekata.

Određivanje slojevima referentih modela na kojima je moguće realizovati napad predstavlja jednu od najznačajnijih informacija za zaštitu računarskih mreža. Na slici 1. je prikazan TCP/IP referentni model slojeva, područje na kome je realizovana podrška za određeni sloj modela (operativni sistem i aplikacije), kao i veza područja realizacije sa internim resursima računarskog sistema. Sa slike 1. se može primetiti da su svi slojevi TCP/IP modela podložni napadu (OSI model podleže istim zaključcima a TCP/IP model je uzet kao jednostavniji primer) što ukazuje i na to da je moguće/potrebno realizovati sistem zaštite na svim nivoima. Takođe, utvrđivanje i odbijanje napada na nižem nivou smanjuje stepen prodora napada i time dodatno smanjuje rizik i povećava performanse sistema jer se viši slojevi ne opterećuju obradom zahteva identifikovanim kao napad. Iz toga se može izvesti zaključak da se najpouzdaniji i najefikasniji sistemi zaštite nalaze na fizičkom sloju. Iako je ovaj zaključak tačan, u praksi najčešće zaštita fizičkog sloja nije moguća iz dva razloga:

1. Pri prenosu podataka se koriste javni/tuđi nezaštićeni komunikacioni kanali koje nije moguće menjati.
2. Filtriranje na osnovu parametara fizičkog sloja je uglavnom nedovoljno precizno da bi se odvojile regularne komunikacije od napada.

Najprecizniji sistemi za filtriranje i kontrolu pristupa podataka imaju mogućnost analize parametara svih slojeva (uključujući i aplikativni) i odluke o prihvatanju/odbijanju zahteva donose na osnovu sveobuhvatnih analiza.

Područje realizacije sloja modela takođe predstavlja bitan parametar iz razloga što propusti u realizaciji protokola na određenom sloju mogu prouzrokovati nestabilan rad sistema ili, u nekim slučajevima, pristup internim resursima korišćenjem pomenutih propusta. Na primer, greška vezana za softver zadužen za odgovaranje na HTTP zahteve u ranim verzijama serverske linije MS Windows operativhih sistema, omogućavala je pristup svim fajlovima na spoljnoj memoriji računara.



Slika X - Nivoi zaštite i pristup resursima

Još jedan bitan parametar napada je, svakako, i njegov cilj. Dve bitne karakteristike napada su njegova dubina i vremenska dimenzija. U skladu sa dubinom, napade možemo podeliti na:

- napade čiji je cilj komunikacioni kanal tj. dostupnost žrtve na mreži i
- napade čiji cilj predstavlja interni resurs žrtve

U skladu sa vremenskom dimenzijom, napade možemo podeliti na:

- konačne i
- dugotrajne napade

Kod podele u skladu sa dubinom i vremenskom dimenzijom treba imati u vidu da se u obzir uzima period nakon uspešnog obavljanja pre nego period potreban za ostvarivanje napada ukoliko je u pitanju napad čiji cilj predstavlja interni resurs žrtve. Kod napada kod kojih je cilj komunikacioni kanal, dugotrajnost napada se određuje u skladu sa vremenom trajanja napada. S obzirom na to da interni resurs žrtve može predstavljati resurs koji omogućava potpunu kontrolu nad njom, rezultat dugotrajnih napada može biti višegodišnje prisustvo napadača na kompromitovanom računaru a da zaduženi administrator toga nije ni svestan. Sa druge strane, DoS (Denial of Service) napadi su usmereni na komunikacione kanale koji napadnuti čvor povezuju sa ostatkom mreže. Na taj način ovi napadi onemogućavaju regularnu upotrebu računarskih mreža, smanjuju dostupnost napadnutih servisa i/ili povećavaju troškove korišćenja mreže. DoS napadi mogu imati u veću dubinu ukoliko je cilj obaranja operativnog sistema žrtve (ili softvera zaduženog za servis) velikom frekvencijom zahteva koje ona nije u stanju da obradi.

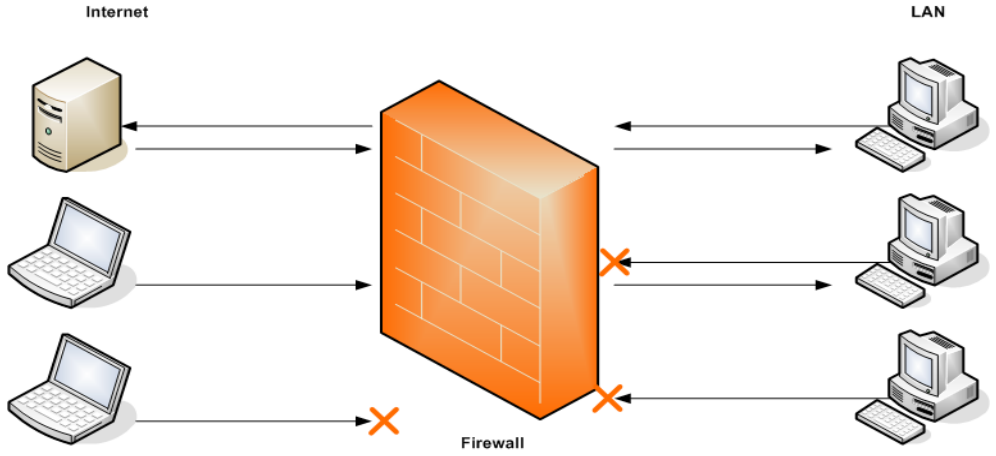
Za efikasnu odbranu od napada često nije dovoljno analizirati atomske jedinice protokola već je njih potrebno dovesti u vezu na osnovu koje će biti moguće kreiranje modela regularnog ponašanja korisnika. Na osnovu ovog modela se svako istupanje može pojačano pratiti ili onemogućiti. Softver koji omogućava ovakvu odbranu jesu napredniji firewall alati ili IDS sistemi.

Jedan od korisnih pristupa za podizanje bezbednosti jeste vođenje dnevnika o akciji korisnika tj. o ostvarenoj komunikaciji. Ovakvi dnevnici su poznati pod nazivom *log* fajlovi. Korišćenjem ovih dnevnika administrator može pregledati zahteve koji su se desili u nekom prošlom periodu i na taj način utvrditi da li je sistem normalno funkcionisao i da li je bilo nekih akcija koje su ugrozile bezbednost sistema. Najčešća greška kod korišćenja *log* fajlova jeste njihovo čuvanje na istom računaru na koji se oni odnose. U takvoj situaciji, napadač koji ostvari kontrolu nad računarom iz log fajlova može naknadno ukloniti zapise koji se odnose na njegove akcije i na taj način onemogućiti administratoru da utvrdi da se napad dogodio. Preporučeno korišćenje *log* fajlova jeste njihovo skladištenje na zasebnom serveru čija je to jedina uloga.

Ranije opisana mogućnost napadača da ukloni sve tragove napada može biti proširena zamenom regularnih alata za nadgledanje računara i mreže izmenjenim alatima koji namerno izostavljaju sve aktivnosti napadača. Na taj način napadač može godinama imatu potpunu kontrolu nad računarom a da administrator toga uopšte nije ni svestan.

11.2. Firewall

Jedan od najefikasnijih načina zaštita računarskih mreža i njenih članova jeste korišćenje *firewall* sistema za kontrolu pristupa. Ovi sistemi funkcionišu po principu prihvatanja ili odbijanja mrežnih komunikacija određenih polisama firewall sistema. Postoji više tipova firewall sistema u zavisnosti od toga u kom obliku su realizovani, kakve mogućnosti nude, na kom nivou se izvršavaju i koja je njihova uloga u mreži u kojoj se nalaze.



Slika X – Princip rada *firewall*-a

U zavisnosti od toga u kom obliku su realizovani firewall sisteme možemo podeliti na:

- namenske uređaje
- računarski softver

Namenski firewall uređaji su uglavnom namenjeni zaštiti računarskih mreža pre nego pojedinačnih računara. Realizovani su u obliku nezavisnih mrežnih uređaja sa najčešće dva mrežna interfejsa od koja sa jedan povezuje sa nepouzdanom mrežom (npr. Internet) a drugi sa mrežom koju treba zaštititi (npr. LAN). Uređaji u sebi sadrže firmware koji vrši analizu ulaznih i izlaznih podataka i na njih primenjuje postavljenja pravila (polise). Ova pravila se postavljaju najčešće putem računara koji se sa uređajem povezuje putem mrežnog ili serijskog kabla. Prednost namenskih firewall uređaja nad ostalim rešenjima jeste jednostavnost (nema dodatnog softvera) i namenski dizajn (hardver uređaja je prilagođen svrsi).

Računarski softver takođe može obavljati ulogu firewall-a. Ovakav softver se instalira na računare u vidu korisničkog softvera ili dela operativnog sistema što ujedno predstavlja i podelu po tome na kom nivou se softver izvršava. Prednost

integracije u kernel operativnog sistema jesu pre svega performanse a mana u određenim slučajevima (kada je napravljen propust u softveru) jeste mogućnost pristupa funkcijama operativnog sistema pri „pucanju“ softvera. Prednost realizacije firewall sistema u obliku dodatnog računarskog softvera jeste pre svega mogućnost instaliranja firewall sistema na obične računare i na svaki računar pojedinačno, jednostavno instaliranje novih verzija softvera kao i mogućnost izbora softverskog rešenja. Glavna mana realizacije firewall sistema u obliku dodatnog računarskog softvera naspram namenskih uređaja su, pre svega, performanse a zatim i potreba da se na računar instalira nenamenski operativni sistem tj. operativni sistem koji osim funkcionalnosti vezanih za firewall poseduje i dodatne funkcionalnosti koje mogu biti zloupotrebljene i izvor nestabilnosti/nesigurnosti sistema.

U zavisnosti od toga kakve mogućnosti nude firewall sisteme možemo pre svega podeliti na osnovu toga koje slojeve TCP/IP modela podržavaju i koje informacije o svakoj komunikaciji mogu izvući putem celokupne komunikacije a ne samo na osnovu trenutnog saobraćaja. U skladu sa takvim kriterijuma firewall sisteme možemo podeliti na:

- Sisteme prve generacije
  Ovi sistemi imaju mogućnost rada sa prva četiri sloja TCP/IP modela tako da je najviša jedinica iz koje mogu dobiti informacije port transportnog sloja. Dodatno, ovi sistemi nemaju mogućnost izvlačenja zaključaka na osnovu prethodno dostavljenih jedinica za prenos podataka već u analizu uključuju samo trenutno aktuelnu jedinicu.

- Sistemi druge generacije
  Firewall sistemi druge generacije se nazivaju i „statefull firewall“. Atribut statefull ukazuje na to da područje rada ovih sistema nije ograničeno samo na trenutno aktuelnu jedinicu za prenos podataka već jedinice analiziraju u kontekstu veze. Ovi sistemi najčešće mogu da utvrde da li je dostavljena jedinica inicijator nove veze (eng. new connection) ili je u pitanju jedinica već ostvarene veze (eng. established connection). Informacije ovog tipa predstavljaju dodatni kriterijum koji se može iskoristiti za kreiranje polisa statefull firewall sistema.

- Sistemi treće generacije
  Firewall sistemi treće generacije osim ranije opisanih funkcionalnosti imaju i mogućnost korišćenja parametara aplikativnog sloja. Iz tog razloga se ponekad nazivaju i proxy based firewall sistemima. Ovakvi sistemi najčešće dolaze sa modularnom podrškom za različite protokole aplikativnog sloja a skup modula je uglavnom moguće proširivati.

U zavisnosti od uloge koju imaju u mreži u kojoj se nalaze firewall sistemi se mogu podeliti na:

- mrežne firewall sisteme
- lične firewall sisteme

Mrežni firewall sistemi se najčešće nalaze na tačkama mreže koje je spajaju sa jednom ili više spoljnih mreža. Uloga ovih sistema jeste da zaštite sve članove lokalne mreže ili da im zabrane određene mrežne akcije usmerene ka spoljnim mrežama. Mrežni firewall sistemi se mogu štititi lokalnu mrežu od spoljnih mreža ali se takođe mogu naći i na više tačaka u lokalnoj mreži da bi štitili segmente lokalne mreže. Za razliku od mrežnih *firewall* sistema lični firewall sistemi imaju za zadatak da štite lokalni računar.

11.3. IDS i IPS sistemi

Za razliku od *firewall* sistema koji svoje odluke o dozvoli/zabrani određene mrežne komunikacije baziraju na statičnim polisama, IPS (Intrusion Prevention System) sistemi su sofisticiraniji i za izvršavanje svoga zadatka – sprečavanje upada na sistem(e) koji štiti – koriste detaljniju analizu (sličnu *firewall* sistemima treće generacije) a ponekad i „inteligentne" algoritme koji imaju mogućnost da razviju model „normalnog" ponašanja i da odbiju sve zahteve koji ne spadaju pod taj model. Kao i *firewall* sistemi, IPS sistemi mogu biti dizajnirani za zaštitu jednog računara (Host based IPS, HIPS) ili cele mreže (Network based IPS, NIPS).

Osim potrebe za odbranom od napada, u računarskim mrežama postoji i potreba za utvrđivanjem da li je do napada došlo i da li je napad uspešno obavljen. Iako na prvi pogled ove potrebe deluju manje važno, treba uzeti u obzir da cilj napada ne mora biti konačna akcija na napadnutom računaru već i kontinualna izmena podataka, sabotiranje obrade ili korišćenje resursa. Sa druge strane, uspešni napadi koji omogućavaju potpunu kontrolu napadnutog računara omogućavaju takvu izmenu log fajlova i alata za uvid u stanje sistema nakon koje više nije moguće utvrditi ne samo da je računar bio napadnut već i da je računar još uvek pod kontrolom napadača. Na Unix sistemima postoje tzv. *rootkit* alati koji iz log fajlova uklanjaju sve zapise o aktivnostima napadača a alate za uvid u stanje sistema (npr. uvid u liste procesa i fajlova na sistemu) zamenjuju izmenjenim alatima koji iz prikaza takođe izostavljaju procese i fajlove napadača. Računar na kojem je instaliran *rootkit* može godinama biti pod kontrolom napadača (što otvara mogućnosti stalnog preuzimanja/izmene/uklanjanja podataka i korišćenja resursa) a da nadležni administrator ne dobije ni najmanji nagoveštaj da je računar pod tuđom kontrolom. Uloga IDS (Intrusion Detection System) sistema je da prepozna uspešno obavljene napade, o tome obavesti administratora i evenutalno ukloni zaostale komponente napada. IDS sistemi se veoma razlikuju i najčešće su strogo vezani za određeni operativni sistem ili okruženje. Sistem rada ovih sistema se kreće od jednostavne provere adekvamih elemenata sistema putem alata koji se nalaze van dometa napadača do korišćenja „inteligentnih" algoritama sposobnih da razviju model normalnog ponašanja u sistemu i na osnovu njega prepoznaju sve akcije korisnika koje odstupaju od tog modela. Pitanje koje se postavlja kod IDS sistema jeste zašto se sistemi koji imaju mogućnost da utvrde da je napad ostvaren ne iskoriste preventivno. Odgovor na ovo pitanje leži u oblasti rada IDS sistema jer IDS sistemi najčešće ne analiziraju mrežni saobraćaj već interne aktivnosti sistema do kojih dolazi, osim kod regularnog korišćenja, tek kada je napad ostvaren. Takođe, IDS sistemi najčešće imaju mogućnost da obustave sve aktivnosti na sistemu i obaveste o tome administratora ukoliko utvrde da je napad ostvaren.

12. Operativni sistemi računara i mrežna podrška

Operativni sistem predstavlja sistemski softver, tj. softver koji je u direktnoj komunikaciji sa hardverom računarskog sistema. Osnovne funkcije operativnog sistema su:

1. upravljanje centralnim procesorom računara
2. upravljanje memorijom računara
3. upravljanje periferijskim uređajima

Pod operativnim sistemom u užem smislu se podrazumeva jezgro (eng. kernel) ali se operativni sistemi najčešće distribuiraju sa:

1. omotačem (eng. shell) koji može biti grafički (GUI - Graphical User Interface) ili vezan za komandnu liniju (CLI - Command Line Interface)
2. alatima za konfiguraciju jezgra
3. alatima za rukovanje (instalaciju, nadogradnju i uklanjanje) korisničkim softverom

tako da se u širem smislu i ove komponente najšeće podrazumavaju kao delovi operativnog sistema.

Operativni sistem takođe predstavlja podlogu na kojoj se mogu izvršavati korisnički programi. U zavisnosti od broja korisnika koji istovremeno mogu raditi na istom OS, oni se dele na:

1. jednokorisničke (eng. single-user)
2. višekorisničke (eng. multi-user)

U zavisnosti od broja korisničkih programa koji se mogu u istom trenutku izvršaviti na istom OS-u, oni se dele na:

1. operativne sisteme koji podržavaju *multitasking*
2. operativne sisteme koji ne podržavaju *multitasking*

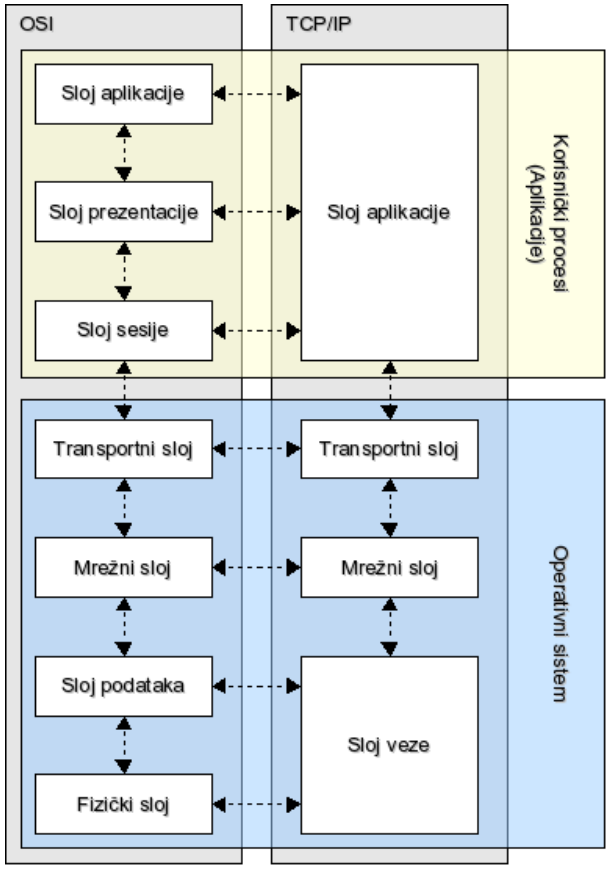
Multitasking je mogućnost operativnog sistema da na jednom procesoru izvršava više procesa (zadataka, eng. task) "istovremeno". Pošto se na jednom procesoru u jednom trenutku može izvršavati samo jedan proces, naizmeničnim dodeljivanjem procesora svakom od procesora, operativni sistem može simulirati korisniku da se procesi izvršavaju istovremeno. Ovakav način rada se naziva kvazi-paralelnim.

12.1. Realizacije mrežne podrške u operativnim sistemima

Iako se pod osnovne funkcije operativnog sistema ubrajaju upravljanje centralnim procesorom, memorijom i periferijskim uređajima, savremeni operativni sistemi poseduju i kompletan podsistem za rad u mrežnom okruženju. Mrežni podsistem (mrežna podrška) u operativnim sistemima se najčešće realizuje kroz:

- podršku za mrežni hardver (1. i 2. sloj OSI i TCP/IP modela)
- podršku za mrežne protokole (3. i 4. sloj OSI i TCP/IP modela)

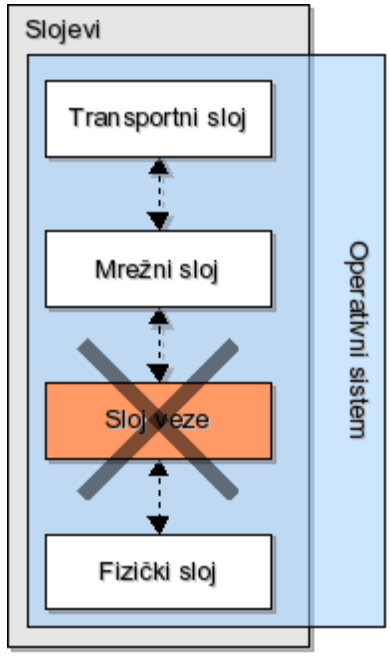
dok se podrška višim slojevima OSI modela uglavnom prepušta korisničkom softveru koji se izvršava na operativnom sistemu. Postoje i situacije u kojima se podrška za transportni pa čak i mrežni sloj prepušta korisničkom softveru kao i situacije u kojima operativni sistem ima ugrađenu podršku za protokole aplikativnog sloja.



Slika X - Slojevi referentnih model i oblast podrške

Osnovni nivo mrežne podrške jeste podrška za hardver koji služi za fizički pristup mreži (mrežna kartica, modem i sl.). Podrška za hardver računara se kod operativnih sistema realizuje u vidu modula jezgra operativnog sistema. Ovi moduli se nazivaju drajverima (eng. *driver*) i operativni sistemi se najčešće isporučuju sa već sadržanim drajverima za popularni mrežni hardver. U slučajevima kada podrška za hardver nije već uključena u operativni sistem od strane proizvođača operativnog sistema, drajveri se preuzimaju od proizvođača hardvera.

Osim podrške za mrežni hardver (fizički sloj) operativni sistem mora imati podršku za protokole sloja veze, mrežnog i transportnog sloja koji se koriste u mreži na koju je računar priključen.



Slika X - Operativni sistem bez adekvatne podrške na sloju veze

Ukoliko operativni sistem ne poseduje podršku za bilo koji od ovih slojeva, vertikalna komunikacija (komunikacija između slojeva unutar računara) će biti prekinuta i pristup mreži onemogućen. Na primer, ukoliko je računar priključen na Ethernet mrežu koja radi pod TCP i IP protokolima, poseduje odgovarajući mrežni hardver, podršku za IP protokol mrežnog sloja i podršku za TCP protokol transportnog sloja ali ne poseduje podršku za sam Ethernet protokol, pristup mreži će biti onemgućen usled prekida vertikalne komunikacije na sloju veze.

Primer realizacije mrežne podrške na različitim nivoima
Uključivanjem podrške u OS za određeni modem uređaj, kao i za *PPP (point-to-point*

protocol) (videti deo *"Unix operativni sistemi / Primer mrežne podrške u OS Linux 2.6.15"*), ostvarena je podrška za prva 2 sloja OSI modela. Uključivanjem podrške za *TCP/IP* protokole, ostvarena je podrška za 3. i 4. sloj OSI modela. Na ovaj način je moguće povezivanje računara koji radi pod tako konfigurisanim OS i poseduje pomenutim modem na mrežu (npr. Internet). Međutim, podrška za određeni servis koji radi na 5-7 sloju OSI modela, npr. HTTP, se realizuje, na serverskoj strani putem HTTP servera (Apache, IIS...), a na klijentskoj strani putem HTTP klijenta (Mozilla, Internet Explorer...).

12.2. Unix/Linux operativni sistemi

Unix operativni sistemi godinama dominiraju na serverskom tržištom usled svoje stabilnosti, sigurnosti i mrežnih mogućnosti. Kao primer Unix operativnog sistema biće uzet Linux OS (Slackware distribucija). Osnova mrežne podrške operativnih sistema danas se ogleda u:

1. podršci za hardver putem koga se računar povezuje na mrežu
2. podršci za mrežne protokole koji se koriste u mreži
3. podršci za servise na mreži ili podršci za aplikacije koje podržavaju pomenute servise

Podrška za mrežni hardver se pod Linux OS-om može smatrati veoma dobrom jer sve veći broj proizvođača mrežnog hardvera uviđa potencijal ovog operativnog sistema i svoju ekonomsku korist od podržavanja istog. Linux kernel u osnovnoj varijanti podržava većinu proizvoda popularnih proizvođača a podrška se može proširiti i pomoću drajvera iz drugih izvora. Ovi drajveri se nalaze u binarnom obliku i/ili sa dostupnum izvornim kodom. Podrška za popularne mrežne protokole u Linux OS-u postoji direktno u kernelu ili korisničkih programa, u zavisnosti na kom nivou OSI modela na kome protokol funkcioniše. Protokoli nižih nivoa (PPP, TCP, IP...) se mogu uključiti kao opcija pri konfigurisanju kernela. Protokoli viših nivoa (SMB, HTTP, FTP) se podržavaju putem korisničkih aplikacija (serverskog i klijentskog dela).

Jedna od glavnih odlika Linux operativnog sistema jeste dostupnost izvornog koda njegovog jezgra. Zahvaljujući tome, veliki broj programera širom sveta učestvuje u razvoju ovog operativnog sistema kroz programiranje novih modula i pronalaženjem eventualnih grešaka u modulima drugih autora. Danas se Linux najčešće sreće na računarima koji rade kao mrežni serveri. Nedostatak popularnih aplikacija za Linux radne stanice čini ovaj operativni sistem manje popularnim u toj oblasti od MS Windows operativnih sistema.

12.2.1.Konfiguracioni fajlovi

/etc/HOSTNAME

Fajl u kome se čuva mrežno ime lokalnog računara.

```
lokalniracunar.lokalnamreza
```

/etc/resolv.conf

Fajl u kome se čuvaju sledeći parametri:

- podrazumevani domen za imena računara kod kojih je domen izostavljen
- lista dostupnih DNS servera u redosledu po kom će im se pristupati

```
search singidunum.ac.yu singidunum.local
nameserver 212.62.48.42
nameserver 212.62.45.222
```

/etc/host.conf

Fajl koji određuje redosled po kome će se razrešavati imena.

```
order hosts, bind
multi on
nospoof on
```

/etc/hosts

Fajl u kome se nalazi lista (najčešće lokalnih) računara. Preteča DNS servisa.

```
127.0.0.1     localhost
192.168.1.1   lokalniracunar.lokalnamreza lokalniracunar
```

/etc/networks

Fajl u kome se nalazi lista mreža (imena i adresa). Retko se koristi i to najčešće pri podizanju sistema.

```
loopback      127.0.0.0
lokalnamreza  192.168.1.0
```

12.2.2. Alati za podešavanje mrežnih parametara

ifport
Alat koji se koristi kod mrežnih adaptera koji imaju više različitih tipova primopredajnika (interfejsa) za određivanje koji će biti aktivan.
ifconfig
Jedan od glavnih mrežnih konfiguracionih alata. Ovaj alat se koristi za podešavanje mrežnih adaptera i za prikaz njihovih konfiguracionih parametara. Pomoću ovog alata se može podesiti mrežna adresa adaptera, mrežna maska, broadcast, aktivnost i sl.
route
Alat kojim se podešava rutiranje izlaznih paketa. Ovim alatom se kreiraju tabele na osnovu kojih se za svaki paket određuje sledeća mrežna tačka kojoj će on biti prosleđen.
usernetctl
Alat kojim se omogućava korisnicima da bez administratorskih privilegija aktiviraju ili deaktiviraju određeni mrežni adapter.
arp
Alat za listanje i eventualnu izmenu ARP tabela mreže.

12.2.3.Alati za proveru rada mreže i rešavanje problema

ping
Jedan od tipova ICMP paketa je „echo request" koji od pimaoca zahteva odgovor u vidu paketa „echo reply". Alat ping služi za slanje „echo request" paketa i koristi se za određivanje: – da li je udaljeni računar uključen i na mreži – vremena potrebnog da se ostvari komunikacija u oba smera – procenata uspešno ostvarenih komunikacija u oba smera Ping alat je jedan od najčešće korišćenih alata za rešavanje problema na mreži.
traceroute
Dok se alat ping koristi za utvrđivanje performansi određene mrežne putanje, alat traceroute se koristi za prikaz putanje kojom se kreću paketi do udaljenog računara. Pomoću ovog alata je moguće otkriti tačnu lokaciju na putanju na kojoj se javlja veliko usporenje ili broj grešaka.
host, nslookup, dig
Ova tri alata služe za postavljanje DNS upita. Sva tri alata mogu da izvrše osnovne upite (ime računara i adresa u oba smera) i naprednije operacije (npr. listanje svih članova domena). Komanda dig se smatra najnaprednijom dok komanda host nudi samo najosnovnije informacije.
nstat
Ovaj alat prikazuje vrednosti nekoliko statistika vezaninh za mrežnu aktivnost koja se odvija unutar kernela. Ove statistike se najčešće dobijaju od SNMP daemon-a. Njima se takođe može pristupiti putem /proc/net/snmp fajla.
netstat
Ovaj alat prikazuje sadržaj fajlova u /proc/net a nudi šire informacije od nstat programa. Netstat ima mogućnost prikazivanja trenutno aktivnih mrežnih konekcija, prikazivanja statistike vezane za mrežne adaptere, čišćenja routing tabele i sl.
snmp
Grupa SNMP komandi (snmpget, snmpnext...) koja omogućava upite ka udaljenim uređajima koje imaju podršku za SNMP. Takođe, paket sadrži i snmp daemon koji obezbeđuje SNMP upite ka lokalnom računaru.
tcpdump

Ovaj program spada u grupu sniffer-a, programa koji snimaju komunikaciju koja se odvija preko nekog lokalnih mrežnih adaptera. tcpdump razume osnovne Internet protokole i ima mogućnost čuvanja rezultata zarad naknadne obrade.

12.2.4.Alati vezani za Dial-Up mreže

pppd
Ovaj daemon ima mogućnost slanja i primanja paketa kroz serijski link između dva računara. Najčešće se koristi kod računara koji se na Internet povezuju putem DialUp-a.
sliplogin
Ovaj program je sličan pppd alatu s tom razlikom što koristi stariji SLIP protokol za enkapsulaciju paketa umesto PPP protokola.
diald
Ovaj program analizira zahteve za mrežnim resursima i automatski pokreće Dial-Up konekciju ukoliko se pojavi zahtev za udaljenim resursima.

12.2.5.Mrežni klijenti i servisi

inetd i tcpd
inetd alat služi za nadgledanje određenih portova, definisanih u /etc/inetd.conf konfiguracionom fajlu i pokretanje pridruženih programa za obradu zahteva. Ukoliko se pojavi zahtev na naznačenom portu, inetd (podrazumevano) pokreće tcpd koji proverava fajlove /etc/hosts.allow i /etc/hosts.deny i na osnovu njih utvrđuje da li je izvorišna IP adresa zahteva ovlašćena za zahtev na pomenutom portu. Ukoliko se utvrdi da izvorišna adresa ima privilegiju rada na pomenutom portu, inetd pokreće program za obradu zahteva (ftpd, telnetd...). Program tcpd sve više izlazi iz upotrebe usled sve naprednijih firewall alata.
tcpdchk i tcpdmatch
Ovi mini alati omogućavaju proveru /etc/hosts.allow i /etc/hosts.deny fajlova. tcpdchk naredba proverava fajlove i prijavljuje eventualne greške. tcpdmatch naredba omogućava postavljanje hipotetičkih daemon/klijent parova i, u zavisnosti od konfiguracionih fajlova, utvrđuje da li će konekcija biti prihvaćena ili ne.
sendmail
Program sendmail je jedan od najpopularnijih MTA na Unix operativnim sistemima i Internetu uopšte. Najpopularnija alternativna rešenja su qmail i postfix.

ssh
Secure Shell (SSH) protokol omogućava rad na udaljenim Unix računarima. Ova usluga se realizuje putem ssh klijentskog alata i sshd serverskog dela servisa.
routed
Kod velikih mreža, glavni ruteri obično nisu podešeni pomoću statičkih tabela za rutiranje već svaki od njih koristi routing daemon koji razmenjuje informacije sa ostalim routing daemonima da bi ažurirao svoje tabele. routed daemon koristi Xerox-ovu varijantu RIT-a.

12.2.6.Podešavanje mrežnih interfejsa (ifconfig)

Većina savremenih Linux distribucija nudi sopstvene alate (konzolne i GUI) za jednostavnije podešavanje mrežnih adaptera (interfejsa). Međutim, većina ovih alate se oslanja na osnovni alat za podešavanje mrežnih adaptera, ifconfig. Za korišćenje ovog alata je su neophodne administratorske privilegije. Ukoliko želimo da prvi mrežni adapter računara podesimo za rad na mreži klase C koja ima sledeće parametre:

- Mreža: 192.168.1.0
- Mrežna maska: 255.255.255.0
- Gateway: 192.168.1.1
- Adresa računara: 192.168.1.10

korišćenjem ifconfig alata to možemo postići pomoću sledeće naredbe:

```
ifconfig eth0 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255
```

Ukoliko želimo samo da izvršimo pregled trenutnih podešavanja interfejsa pokrenućemo alat ifconfig bez parametara:

```
bash# ifconfig
eth0    Link encap:Ethernet  HWaddr 00:11:25:AA:0E:59
        inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:132492645 errors:0 dropped:0 overruns:0 frame:0
        TX packets:154256707 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:32797966 (31.2 Mb)  TX bytes:1679866715 (1602.0 Mb)
        Base address:0x2000 Memory:d0120000-d0140000
lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:3240825 errors:0 dropped:0 overruns:0 frame:0
        TX packets:3240825 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
```

```
        RX bytes:2704771622 (2579.4 Mb)  TX bytes:2704771622 (2579.4 Mb)
```

Pošto alat ifconfig nema mogućnost postavljanja gateway parametra, taj parametar možemo postaviti pomoću alata route:

```
/sbin/route add default gw 192.168.1.1 metric 1
```

U slučaju da želimo u toku rada da obustavimo rad određenog interfejsa na npr. 10 minuta iskoristićemo argumente up i down:

```
ifconfig eth0 down && sleep 600 && ifconfig eth0 up
```

Na ovaj način se mogu u toku rada menjati parametri jednog adaptera, može se podesiti veći broj mrežnih adaptera na jednom sistemu vodeći pri tome računa kako se postavljaju rute, u slučaju da postoji više gateway-a na mreži.

12.2.7.Primer mrežne podrške u OS Linux 2.6.15

```
Networking --->
   Networking options  --->
      < > Packet socket
      < > Unix domain sockets
      < > PF_KEY sockets
      [*] TCP/IP networking
      [ ]   IP: multicasting
      [ ]   IP: advanced router
      [ ]   IP: kernel level autoconfiguration
      < >   IP: tunneling
      < >   IP: GRE tunnels over IP
      [ ]   IP: multicast routing
      [ ]   IP: ARP daemon support (EXPERIMENTAL)
      [ ]   IP: TCP syncookie support (disabled per default)
      < >   IP: AH transformation
      < >   IP: ESP transformation
      < >   IP: IPComp transformation
      < >   IP: tunnel transformation (NEW)
      < >   INET: socket monitoring interface (NEW)
      [ ]   TCP: advanced congestion control (NEW)
      < >   The IPv6 protocol
      [ ] Network packet filtering (replaces ipchains) --->
      < > Asynchronous Transfer Mode (ATM) (EXPERIMENTAL)
      < > 802.1d Ethernet Bridging
      < > 802.1Q VLAN Support
      < > DECnet Support
      < > ANSI/IEEE 802.2 LLC type 2 Support
      < > The IPX protocol
      < > Appletalk protocol support
      < > CCITT X.25 Packet Layer (EXPERIMENTAL)
      < > LAPB Data Link Driver (EXPERIMENTAL)
      [ ] Frame Diverter (EXPERIMENTAL)
      < > WAN router
          QoS and/or fair queueing  --->
          Network testing  --->
   [ ]   Amateur Radio support  --->
   < >   IrDA (infrared) subsystem support  --->
   < >   Bluetooth subsystem support  --->
   < >   Generic IEEE 802.11 Networking Stack (NEW)
Device Drivers --->
   Network device support --->
      [*]  Network device support
      < >   Dummy net driver support
      < >   Bonding driver support
      < >   EQL (serial line load balancing) support
      < >   Universal TUN/TAP device driver support
      < >   General Instruments Surfboard 1000
        ARCnet devices  --->
        PHY device support  --->
        Ethernet (10 or 100Mbit)  --->
        Ethernet (1000 Mbit)  --->
        Ethernet (10000 Mbit)  --->
        Token Ring devices  --->
        Wireless LAN (non-hamradio)  --->
        Wan interfaces  --->
      [ ]   FDDI driver support
      [ ]   HIPPI driver support (EXPERIMENTAL)
      < >   PLIP (parallel port) support
      < >   PPP (point-to-point protocol) support
```

```
      < >   SLIP (serial line) support
      [ ]   Fibre Channel driver support
      < >   Traffic Shaper (EXPERIMENTAL)
      < >   Network console logging support (EXPERIMENTAL)
```

Literatura

[1] Andrews S. Tanenbaum, *Računarske mreže*, Mikro Knjiga, 2005, Beograd

[2] Davidson J., Peters J.: "Voice over IP Fundamentals", Cisco Press, 2000.

[3] Jerry Fitzgerald and Alan Dennis, *Business Data Communications and Networking* - 8th Edition, John Wiley & Sons, Inc, 2005., New York

[4] Leiner B., Cerf V., Clark D., Kahn R., Kleinrock L., Lynch D., Postel J., Roberts L., Wolff S.: "A Brief History of the Internet", Internet Society, 2002.

[5] Muller J. N., *Bluetooth Demystified*, McGraw-Hill, 2000, NY, USA.

[6] Stevens R.: "TCP/IP Illustrated, vol. 1", Addison-Wesley Longman, Inc., 1999.

[7] William Stallings, *Data and Computer Communication*, Pearson Prentice Hall, 2004, NJ, USA

[8] Robin Burk, David B Horvath, CCP i drugi, *Unix do kraja, izdanje za sistem administratora*, Kompjuter biblioteka, 1999.

[9] http://www.bluetooth.org

[10] www.wikipedia.org