5 UPRAVLJANJE I ODRŽAVANJE RAČUNALNIH MREŽA

5.1 UVOD

Upravljanje mrežom podrazumijeva pravilnu konfiguraciju, povezivanje i nadzor elemenata mreže: računala (osobnih i poslužitelja), komunikacijske opreme (zvjezdišta, pojačala, premosnika, prospojnika, poveznika). Uz sklopovsku osnovicu, upravljanje mrežom obuhvaća instalaciju, konfiguriranje i održavanje programske podrške (sistemske i aplikacijske), te brigu o korisnicima mreže i njihovim podacima. Cilj upravljanja i održavanja jest pouzdana, modularna i sigurna računalna mreža. Upravljanje i održavanje računalne mreže obavlja administrator mreže.

Mrežna komunikacijska oprema koja radi na nižim razinama komunikacijskog modela uglavnom ne zahtjeva konfiguriranje niti upravljanje, već funkcionalna postaje spajanjem u mrežu. Takva su zvjezdišta, pojačala (fizička razina) i premosnici (podatkovna). Prospojnici, također na podatkovnoj razini, zahtijevaju osnovno konfiguriranje pri spajanju na mrežu, odnosno dodatno konfirugiranje i administriranje u slučaju podrške virtualnim lokalnim mrežama. Uređaji koji rade na višim razinama kao što su usmjernici na mrežnoj, poveznici na prijenosnoj razini, te računala (poslužitelji i klijenti) koja obavljaju funkcije 5-7 razine, postavljaju znatno veće zahtjeve po pitanju konfiguriranja i administriranja jer su za njihov rad bitne informacije o drugim uređajima u mreži i drugim mrežama.

Uređaji na mreži međusobno se razlikuju po svojim jednoznačno definiranim adresama, bez obzira na veličinu i zemljopisnu rasprostranjenost mreže kojoj pripadaju. Kod TCP/IP skupa protokola na kojem je zasnovana danas jedina svjetska računalna mreža Internet, adresiranje uređaja povezanih na mrežu (računala, prospojnika, usmjernika i poveznika) realizira se primjenom brojčanih IP adresa i naziva, između kojih postoji jednoznačno preslikavanje.

Višekorisnički i višezadaćni operacijski sustavi na poslužiteljima i računalima klijenata ostvaruju funkcije sjedničke, predodžbene i korisničke razine. Upravljanje i održavanje na višim razinama komunikacijskog modela stoga se svodi na pravilnu konfiguraciju poslužničkih i korisničkih programa za odgovarajuće mrežne usluge, te njihov sukladan rad s instaliranim operacijskim sustavom.

Mrežne usluge na računalnim mrežama većinom su zasnovane na **modelu klijent - poslužitelj**. Poslužitelj je program i/ili računalo na kojem se nalaze podaci, te mora biti sposobno prepoznati zahtjev klijenta za tim podacima, donijeti odluku hoće li na zahtjev odgovoriti potvrdno ili ne i, u slučaju potvrdnog odgovora, poslati podatke natrag klijentu. Klijent je program i/ili računalo koje mora biti u stanju postaviti zahtjev za podacima poslužitelju koji ih posjeduje, prihvatiti odgovor poslužitelja i primljene podatke prikazati na zaslonu korisniku. Klijent i poslužitelj komuniciraju putem protokola odgovarajuće usluge.

Protokol je skup pravila koje moraju poštivati dvije strane kako bi komunikaciju uspostavile, održale određeno vrijeme potrebno za prijenos podataka i prekinule. Najpoznatije mrežne usluge na Internetu zasnovane na modelu klijent-posužitelj s odgovarajućim protokolima su: Telnet (za pristup udaljenom računalu), FTP (File Transfer Protocol) za prijenos datoteka između dva računala, POP3 i SMTP za razmjenu elektroničke pošte, HTTP (HyperText Tranfer Protocol) za prijenos WWW stranica itd.

Mrežni operacijski sustavi omogućavaju korisnicima lokalne mreže formiranje logičkih radnih grupa, koje za cilj imaju olakšani pristup zajedničkim resursima - datotekama, direktorijima ili mrežnim uređajima (npr. pisačima). Tako formirane radne grupe ne moraju nužno odgovarati radnim grupama formiranim prema pravilima strukturnog kabliranja, a uvjetovanim zasebnim domenama kolizije.

Održavanje računalnih mreža složen je i zahtjevan posao jer računalo povezano na računalnu mrežu nije više izolirani sustav, nego podložno interakciji drugih sustava - računala, korisnika i mreža. Posao kojeg mrežni administrator obavi na jednom računalu može utjecati na druge sustave u mreži.

5.2 MREŽNA ARHITEKTURA INTERNETA (TCP/IP)

Postoji više rješenja realizacije lokalnih mreža s ciljem međusobne komunikacije korisnika na lokalnim mrežama, prijenosom ili zajedničkim korištenjem podataka i mrežne opreme. To omogućavaju protokoli IPX Novell mreže, te Microsoftov NETBEUI, ali se sve više napuštaju zbog slabe kooperativnosti s operacijskim sustavima drugih proizvođača. Današnje se računalne mreže sve više temelje na TCP/IP skupu protokola, u prvom redu zbog jednostavnog definiranja adresa uređaja na mreži, te zbog mogućnosti povezivanja na Internet i korištenje njegovih mrežnih usluga, Stoga će model komunikacijskog sustava, koncept pojedinih

razina i odgovarajući osnovni protokoli biti objašnjeni na mrežnoj arhitekturi Interneta i pripadajućem TCP/IP skupu komunikacijskih protokola. Njegov naziv potječe od dva najčešće korištena protokola - TCP (Transmission Control Protocol) i IP (Internet Protocol).

5.2.1 Povijesni razvoj

Početak stvaranja Interneta vezuje se za 1969. godinu kad je Istraživački odjel ministarstva obrane SAD (DARPA - Defense Advanced Research Projects Agency) pokrenula projekt uspostave eksperimentalne mreže s prespajanjem paketa nazvane ARPANET, čija je namjena bila ispitati tehničke mogućnosti razmjene podataka putem računalne mreže. S obzirom na uspješan eksperimentalni rad ARPANET mreže, sve se više organizacija povezuje u tu mrežu koristeći je za svoje svakodnevne podatkovne komunikacije. Godine 1975. ARPANET je od eksperimentalne postala operativna mreža, a posao održavanja mreže dodijeljen je Odjelu komunikacija ministarstva obrane (DCA - Defense Communications Agency).

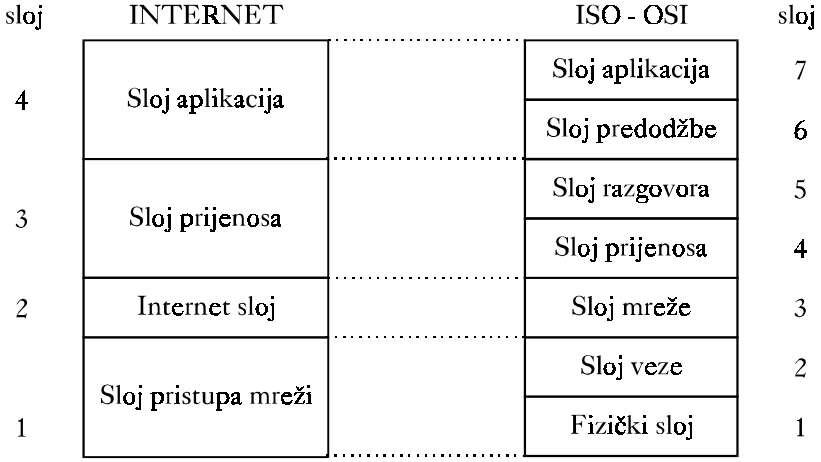
TCP/IP skup protokola usvojen je kao vojni standard (MIL STD - Military Standard) 1983. godine, a korištenje tog skupa protokola bilo je preduvjet za povezivanje na ARPANET. DARPA je potakla ugradnju TCP/IP skupa protokola u operacijski sustav UNIX i time je stvorena prva veza između operacijskog sustava UNIX (Sveučilišta Berkeley - BSD UNIX) i TCP/IP skupa protokola. U vrijeme kad je TCP/IP skup protokola postao standard, počeo se pojavljivati termin Internet, a mreža ARPANET podijeljena je u MILNET - dio podatkovne mreže ministarstva obrane SAD i manji ARPANET. S vremenom Internet postaje dominatna svjetska računalna mreža koja povezuje skoro sve ostale mreže u svijetu. Protokoli TCP/IP skupa definirani su kroz neku od tri izdanja Internet standarda: vojni standardi (MIL STD), tehničke bilješke Interneta (IEN - Internet Engineering Notes; uglavnom napušten), a danas uglavnom kroz sustav komunikacije među korisnicima "zahtjevi za komentarima" (RFC - Requests for Comments). Svi RFC dokumenti dostupni su na Internet adresi: http://www.rfc-editor.org/rfcsearch.html.

TCP/IP skup protokola prihvaćen je kao standard isključivo zbog određenih pogodnosti koje je jedini u datom trenutku nudio, a neke od njih su:

- neovisnost o tipu računalne opreme i operacijskih sustava, te neovisnost o pojedinom proizvođaču, što ga čini idealnim za povezivanje mreža različitih karakteristika.
- neovisnost o tipu mrežne opreme na fizičkoj razini i prijenosnog medija, što omogućava integraciju različitih tipova mreža (Ethernet, token ring, X.25, ATM).
- jedinstveni način adresiranja koji omogućava povezivanje i komunikaciju svih uređaja koji podržavaju TCP/IP skup protokola bez obzira na tip uređaja ili veličinu mreže
- standardizirani protokoli viših razina komunikacijskog modela, što omogućava široku primjenu mrežnih usluga.

5.2.2 Arhitektura TCP/IP skupa protokola

Za razliku od OSI modela koji ima sedam razina, TCP/IP model definira pojedine funkcije komunikacijskog modela kroz četiri razine.



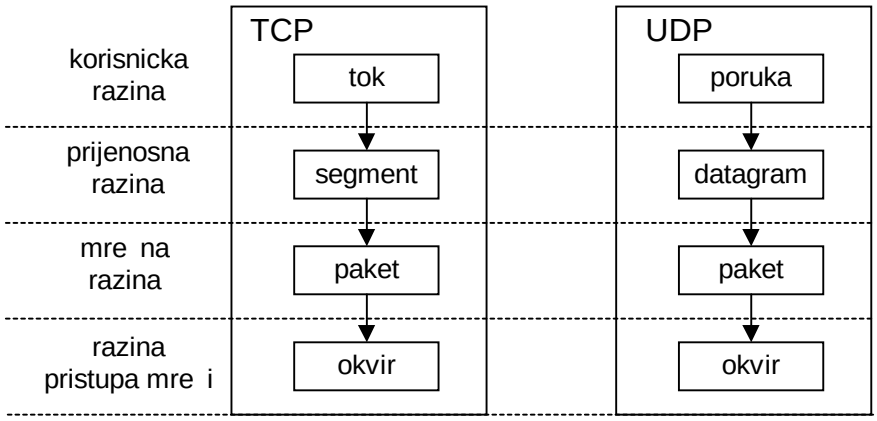
Slika 5.1. - Usporedba ISO OSI i TCP/IP modela

Svaka razina ne znači nužno jedan protokol, nego može biti predstavljena većim brojem protokola od kojih svaki definira i ostvaruje neku od funkcija:

1. razina pristupa mreži (Network Access Layer)
2. mrežna razina (Internet Layer)
3. prijenosna razina (Transport Layer)
4. korisnička razina (Application Layer)

Kao i kod OSI modela, podaci se prosljeđuju od viših razina prema nižim kad se šalju u mrežu, a od nižih prema višim kad se primaju iz mreže. Svaka razina dodaje svoje zaglavlje na podatke koje primi od prve više razine, a koji sadrže izvornu poruku i zaglavlja prethodnih razina. Pri prihvatu podataka s mreže, svaka razina odvaja njoj upućeno zaglavlje, obrađuje primljene informacije i sukladno njima podatke prosljeđuje sljedećoj višoj razini.

Pojedine razine koriste različite nazive za podatke koji se šalju ili primaju. Slika 2 daje pregled terminologije prema protokolima TCP i UDP, protokolima četvrte razine prema ISO OSI modelu, odnosno treće prema TCP/IP arhitekturi. Oba protokola koriste IP protokol na nižoj razini.



Slika 5.2. Struktura podataka

Razina pristupa mreži

Razina pristupa mreži, najniža razina TCP/IP arhitekture, obavlja funkcije prve dvije razine ISO OSI modela i odgovorna je za realizaciju komunikacije između dva uređaja u mreži. Podatke primljene od druge, mrežne razine prilagođava fizičkom mediju vodeći računa o svojstvima mrežnih uređaja. Na ovoj se razini IP paket s druge razine postavlja u okvire koji se šalju preko mreže, te se obavlja preslikavanje IP adrese uređaja na mreži u njegovu fizičku adresu. Protokoli prve razine TCP/IP modela su:

- Ethernet protokol kojim je definirano povezivanje lokalnih mreža zasnovanih na različitim tipovima fizičkog medija, pri različitim brzinama prijenosa, uz četiri formata Ethernet okvira trenutno u primjeni (Ethernet II, Ethernet 802.3, Ethernet 802.4 i SNAP Ethernet).
- SLIP (Serial Line Internet Protocol), RFC 1055 - de facto standard za prijenos IP paketa preko modemskih veza koje podržavaju TCP/IP protokol
- PPP (Point to Point Protocol), RFC 1548 - standard za prijenos podataka preko modemskih veza

Mrežna (Internet) razina

Mrežna razina TCP/IP modela Interneta omogućava uspostavu logičke veze između dva uređaja koja žele komunicirati. Osnovni protokol te razine je IP (Internet Protocol, RFC 791). Uređaji se prepoznaju preko 32-bitnih IP adresa koje imaju dva dijela: mrežni broj i broj računala. Mrežna razina prenosi podatke unutar TCP/IP modela, tj. prihvaća ih od razine pristupa mreži i predaje prijenosnoj razini, izdvajajući i analizirajući svoje zaglavlje. Osnovna jedinica podataka na ovoj razini jest paket. Osim IPa, među osnovne protokole mrežne razine ubrajaju se i:

- ICMP (Internet Control Message Protocol, RFC 792)
- ARP (Address Resolution Protocol), RFC 826 - protokol za određivanje adresa koji IP adresu zamijeni Ethernet adresom kartice, tj. fizičkom adresom
- RARP (Reverse Address Resolution Protocol), RFC 903 - Ethernet adresu zamijeni IP adresom; primjenjuju ga računala bez čvrstih diskova za doznavanje vlastite IP adrese prilikom inicijalizacije

- DHCP (Dynamic Host Configuration Protocol), RFC 1531 - omogućava dinamičku dodjelu raspoloživih IP adresa uređajima na mreži.

Prijenosna razina

Prijenosna razina osigurava vezu dva uređaja u bilo kojim dijelovima mreže i predstavlja sponu u komunikacijskom modelu između mrežne i korisničke razine. Mrežna razina iz svog zaglavlja saznaje kojem protokolu prijenosne razine treba predati podatke, a prijenosna razina na osnovu podataka u svom zaglavlju podatke prosljeđuje točno određenoj usluzi korisničke razine. Dva su osnovna načina prijenosa podataka te razine - s i bez uspostave logičkog kanala, a izbor ovisi o tipu i veličini poruke. Prijenos s uspostavom logičkog kanala (spojevni) osigurava pouzdanu isporuku podataka do odredišta uz što manje gubitaka i što manje pogrješaka i primjenjuje se kod prijenosa korisničkih podataka. Prijenos bez uspostave logičkog kanala (bespojni) primjenjuje se kod prijenosa upravljačkih poruka. Dva najznačajnija protokola te razine su:

- TCP (Transmission Control Protocol), RFC 793, spojevni, za vezu s detekcijom i korekcijom pogrješaka
- UDP (User Datagram Protocol), RFC 768 za bespojne komunikacije bez detekcije i korekcije pogrješaka.

Programeri mogu odabrati protokol koji najbolje odgovara njihovoj aplikaciji.

Korisnička razina

Korisničku razinu čine programi i procesi koji svoje zahtjeve ili podatke predaju izravno protokolima prijenosne razine. Dijelimo ih na dvije osnovne grupe ovisno o tome koji protokol koriste na prijenosnoj razini. TCP koriste protokoli:

- Telnet - protokol mrežnog terminala (Network Terminal Protocol) koji omogućava prijavljivanje za rad na udaljenom računalu u mreži
- FTP protokol za prijenos datoteka (File Transfer Protocol) za prijenos podataka između računala u mreži
- SMTP (Simple Mail Transfer Protocol), protokol za prijenos elektroničke pošte, definira slanje pošte lokalnog računala bilo kojem računalu u mreži, te prijem pošte upućene računalu u lokalnoj mreži i njeno prosljeđivanje lokalnim programima za obradu pristigle pošte.

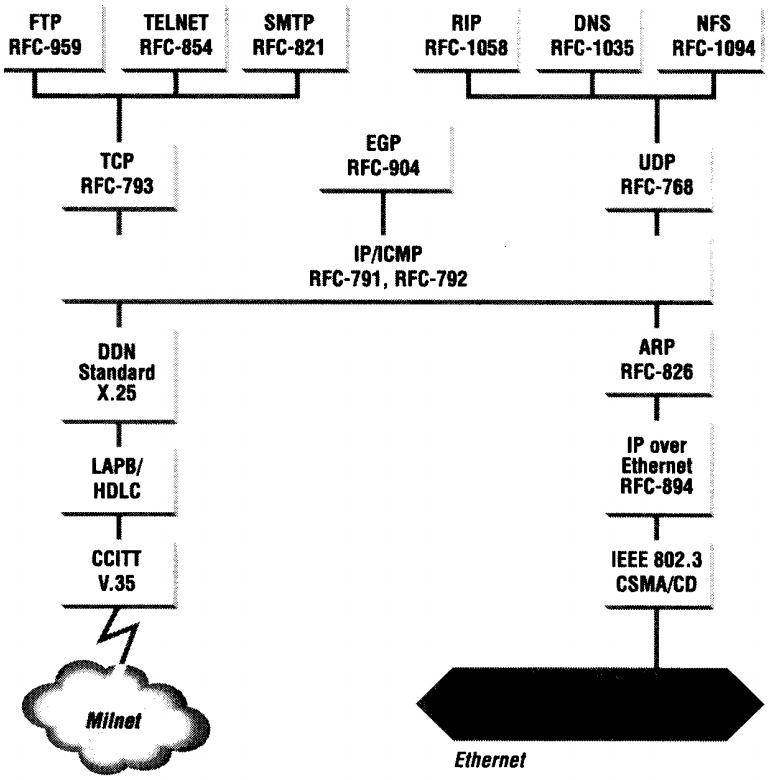
Protokoli druge skupine koriste UDP. Oni često obavljaju funkcije koje se izvršavaju neovisno o aplikacijama korisnika i za koje korisnik ne mora ni znati, a potrebne su za rad mreže. Takvi su protokoli:

- DNS (Domain Name Service, RFC 1035) - aplikacija koja preslikava IP adresu nekog uređaja na mreži u njemu dodijeljeno ime
- RIP (Routing Information Protocol, RFC 1058) - protokol za usmjeravanje informacija; koriste ga uređaji na mreži kada razmjenjuju informacij vezane za usmjeravanje paketa kroz mrežu
- NFS (Network File System, RFC 1094) - mrežni datotečni sustav; protokol omogućava dostupnost direktorija i datoteka različitim računalima na mreži.

Oba protokola prijenosne razine, a time i obje skupine aplikacija korisničke razine koriste IP i/ili ICMP protokole na mrežnoj razini.

Protokoli ne moraju nužno koristiti TCP ili UDP. Takav je EGP (Exterior Gateway Protocol, RFC 904) - protokol vanjskog poveznika koji definira povezivanje dva međusobno neovisna sustava s vlastitom upravom (autonomous systems).

Na Slici 4.3. prikazani su najčešće korišteni protokoli TCP/IP skupa po razinama Internet arhitekture od korisničke do razine pristupa mreži, pri čemu je napravljeno znatno pojednostavljenje funkcija protokola prikazujući ih kao blokove vezane isključivo uz jednu razinu. Međutim, neki protokoli (npr. ARP i RARP) obavljaju funkcije dviju razina koje povezuju. Uz naziv svakog protokola označen je i standard koji ga opisuje, kao smjernica u njihovom daljnjem proučavanju.



Slika 5.3. TCP/IP protokoli

5.2.3 Topološka struktura Interneta

Internet je svjetska računalna mreža organizirana kao skupina podmreža različitih karakteristika povezanih TCP/IP skupom protokola.

Računala jedne ustanove povezana su lokalnom mrežom koja se može prostirati na jednoj ili više lokacija, projektiranom da ispunjava funcionalne i druge zahtjeve ustanove. Takva lokalna mreža ima svoje područje mrežnih adresa i naziva, koje ju jednoznačno definira u svom gradu, zemlji i svijetu, neovisna je o drugim mrežama i čini neovisni ili autonomni sustav (AS - autonomous system). Više takvih neovisnih sustava u Internet povezuju pružatelji Internet usluga (ISP - Internet Service Providers). U jednoj državi obično ima nekoliko ISPova koji mogu udruženo ili posebno ostvariti međunarodnu vezu prema Internetu posredstvom neke od međunarodnih organizacija.

Osnovnu topološku strukturu Interneta čine podmreže formirane logički (zemljopisno i/ili prema ustroju), adresno (prema veličini mreža i mrežnim klasama), te infrastrukturno (kao jedna domena prostiranja okvira s univerzalnim adresama na podatkovnoj razini), što će detaljnije biti objašnjeno u narednim poglavljima.

Postoje mreže zasnovane na TCP/IP skupu protokola koje nisu povezane na Internet i koje ne žele biti dio Interneta, osim možda, koristiti neku od mrežnih usluga Interneta. Takve mreže mogu biti realizirane kao privatne, ili na principu intraneta. U drugom slučaju, cijela se mreža prema drugima predstavlja preko jedne IP adrese. Za takve mreže preporučljivo je koristiti neko od rezerviranih područja adresa.

5.3 PROTOKOLI TCP/IP SKUPA

Najvažniji protokoli TCP/IP skupa su: SLIP (Serial Line Internet Protocol), PPP (Point-to-Point Protocol), IP (Internet Protocol), ICMP (Internet Control Message Protocol), ARP (Address Resolution Protocol), UDP (User Datagram Protocol), te TCP (Transmission Control Protocol).

Na razini pristupa mrežama često se koriste protokoli koji nisu formalno dio TCP/IP skupa, kao npr. za Ethernet lokalne mreže, ISDN pretplatničke mreže i drugi.

5.3.1 SLIP - Protokol za modemske komunikacije (de facto standard)

SLIP definira mehanizam prijenosa IP paketa telefonskom linijom (serial line). IP paketu dodaje svega dva kontrolna znaka koji ga uokviruju. To je jedina funkcija koju obavlja, pa je jednostavan za primjenu. Omogućava povezivanje i međusobnu komunikaciju računala i usmjerivačkih uređaja.

SLIP protokol definira dva kontrolna znaka, END i ESC. END je C0 heksadecimalno (192 decimalno), a ESC DB heksadecimalno (219 decimalno) i ne treba ga miješati s ASCII ESCape znakom. Ako se prilikom slanja podataka naiđe na sam znak END, umjesto njega šalju se dva znaka ESC i heksadecimalno DC (220 decimalno). Ako se naiđe na sam znak ESC šalju se dva znaka ESC i heksadecimalno DD (221 decimalno). Na kraju posljednjeg okteta šalje se znak END. Naknadno je uvedeno da se prije slanja podataka pošalje znak END kako bi se odbacili okteti nastali šumom na liniji. Kako SLIP nije prihvaćen kao standard, ne postoji ni definirana maksimalna veličina SLIP paketa, a preporuča se maksimalna veličina od 1006 okteta kao kod Berkeley UNIX verzije SLIPa.

Nedostaci SLIP protokola su:

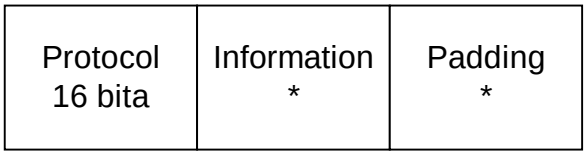
- nema mogućnost adresiranja niti razmjene informacija o adresi - računalo s jedne strane SLIP veze ne može doznati IP adresu uređaja s druge strane putem SLIP protokola.
- nema identifikaciju tipa paketa - jedna SLIP veza podržava samo jednu arhitekturu protokola (npr TCP/IP), koja mora biti ista za obje strane u komunikaciji.
- nema detekciju ni korekciju pogrješki, pa ni retransmisije paketa - podrazumijeva se da će to biti obavljeno protokolima više razine
- nema mehanizme sažimanja podataka.

Neki od nedostataka SLIP protokola razrješeni su naknadnim poboljšanjima, kao što je komprimiranje zaglavlja (CSLIP, RFC 1144). Razmjena informacije o adresi obavlja se tekstovnim načinom prije uključivanja SLIP protokola.

5.3.2 PPP - Point - to - Point Protocol

PPP je standardni Internet protokol koji omogućava prijenos paketa preko modemskih veza uz istovremenu podršku više protokola, te osigurava pouzdani prijenos preko bilo kojeg tipa serijske veze. Čine ga tri skupine pravila: za umetanje (enkapsulaciju) paketa više protokola mrežne razine u okvire PPP protokola, zatim protokol za nadzor veze (LCP - Link Control Protocol) za uspostavu, konfiguriranje i testiranje podatkovne veze, te protokol za "nadzor mreže" (NCP - Network Control Protocol) za dogovor o prijenosu različitih protokola mrežne razine.

Umetanje paketa omogućava multipleksiranje različitih protokola mreže razine preko iste veze, pa PPP omogućava povezivanje računala, premosnika i usmjernika koji rade na različitim protokolima. Dodaje zaglavlje od 8 okteta (kao dodatak HDLC okvirima), s mogućnošću skraćivanja na 2 ili 4 okteta.



Slika 5.4. Zaglavlje PPP protokola

Polje "protokol" definira kojem protokolu mrežne razine treba proslijediti paket. Polje "information" sadrži paket za protokol iz polja "protokol". Polja "information" i "padding" mogu biti promjenljive duljine, do popune okvira od 1500 okteta, što je ujedno najveći mogući okvir kojeg PPP može primiti (MRU - Maximum Receive Unit).

Protokol za nadzor veze (LCP) daje potrebne kontrolne informacije o stanju veze, uspostavlja vezu, dogovara konfiguracijske parametre, provjerava kvalitetu uspostavljene veze i raskida vezu. Tijekom dogovaranja parametara, LCP može dogovoriti prijenos uz sažimanje podataka, te iznos MRU. Ovim protokolom određene su procedure provjere identiteta korisnika i dodjele IP adrese.

Protokol za nadzor mreže (NCP) protokolima mrežne razine daje kontrolne informacije i informacije o konfiguraciji, odnosno, omogućava PPP protokolu ostvarivanje sigurnog prijenosa podataka različitih mrežnih protokola.

PPP protokol dopunjava sve nedostatke SLIP protokola (pouzdani prijenos, adresiranje, podrška za više protokola), što ga čini složenijim i zahtjevnijim. Trenutno se u praksi koriste oba protokola, iako ne komuniciraju međusobno. PPP se najčešće primjenjuje za vezu preko iznajmljene linije (leased line). Za privremene i povremene modemske veze (dial-up) primjenjuje se bilo koji od ta dva protokola, iako će PPP vjerojatno istisnuti SLIP.

5.3.3 IP - Internet protokol

Internet protokol (Internet Protocol - RFC 791) je osnovni protokol mrežne razine TCP/IP modela, a koriste ga protokoli svih razina - iznad mrežne razine. To je bespojni protokol, što znači da se dvije strane ne dogovaraju o početku ili završetku prijenosa podataka, nego predajno računalo uputi paket i dalje ne vodi računa o njemu. Protokoli više razine dužni su provjeriti konzistentnost korisnikovih podataka. Ti protokoli trebaju obaviti detekciju i korekciju pogreški. Zbog toga se IP protokol često naziva "nepouzdani protokol".

Osnovne funkcije IP protokola su:

- definiranje sheme Internet adresiranja
- definiranje paketa
- prosljeđivanje podataka između razine pristupa mreži i prijenosne razine
- podjela (fragmentacija) i sastavljanje paketa.

Funkcija mrežne razine je usmjeravanje paketa do udaljenog računala na osnovu IP adrese.

5.3.3.1 IP adrese (Internet Protocol Address)

IP shema adresiranja je jedna od prednosti TCP/IP skupa protokola jer omogućava jedinstveno, a ipak jednostavno adresiranje svih uređaja na svim mrežama Interneta. IP adresa je veličine 32 bita, četiri okteta , i sastoji se iz dva dijela:

- mrežnog broja (network number), identificira jednu Internet podmrežu
- broja računala (host number), identificira računalo unutar podmreže.

Zapisuje se kao četiri broja (polja) međusobno odvojena točkama:

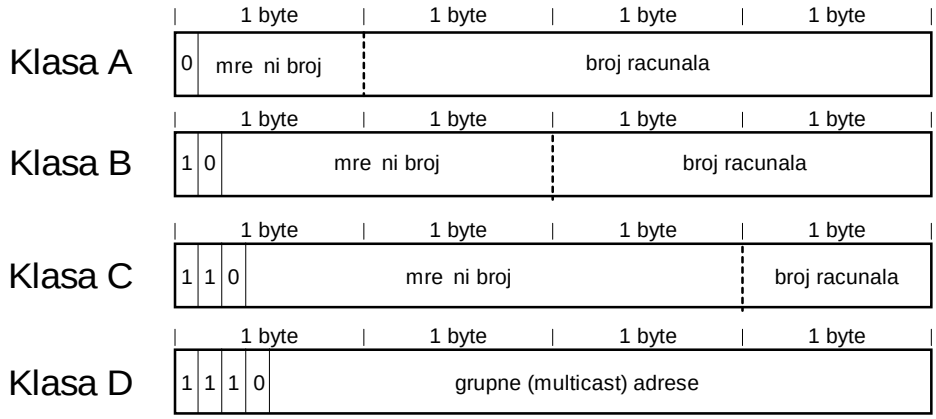
polje1.polje2.polje3.polje4

a svako je polje veličine jednog okteta i može imati decimalnu vrijednosti u granicama od 0 do 255. Značenje svakog polja i svakog bita unutar polja ovisi o klasi mreže. Polje1 uvijek pripada mrežnom broju. Prvi bitovi u polju1 određuju klasu mreže IP adrese, a time i koji dio cijele IP adrese čini mrežni, a koji broj računala.

Mrežni broj dodjeljuje centralna ustanova za administriranje Internet mreže NIC (Network Information Center for Internet), na osnovu informacija koje pruža podnositelj zahtjeva. Broj računala dodjeljuje se lokalno, a određuje ih i dodjeljuje administrator mreže.

Mrežne klase

IP adrese grupirane su u četiri osnovne mrežne klase: A, B, C i D.



Slika 5.5. Broj mreže i broj računala u mrežnim klasama

Mreže klase A imaju najznačajniji bit prvog okteta 0, čime je određeno da preostalih sedam bitova prvog okteta čine mrežni, a naredna tri okteta broj računala. Ukupno može biti 126 mreža klase A, a u jednoj mreži može biti 65.536 računala. Moguće IP adrese su 1.0.0.0 do 126.255.255.255. Klasa A predviđena je za mreže s velikim brojem računala, kakvih je u svijetu malo. Većina mreža pripada klasama B ili C.

Za IP adrese u **klasi B** najznačajniji oktet počinje bitovima 10, mrežni broj određuje narednih 14 bitova, a treći i četvrti oktet definiraju broj računala. Raspoložive IP adrese klase B su 128.0.0.0 do 191.255.255.255. Najviše može biti 16.384 (2^{14}) mreža klase B, a u jednoj mreži može biti od 256 do 65.536 računala.

Klasa C počinje bitovima 110 u najznačajnijem oktetu, mrežni broj proteže se zaključno s trećim oktetom, a može biti do 256 računala. Najviše je mreža klase C, a može ih biti 2.097.152, tj. 2^{21} mreža. Raspoložive IP adrese su 192.0.0.0 do 223.255.255.255.

Klasa D rezervirana je za grupne (multicast) adrese koje počinju bitovima 1110 prvog okteta. Ima ih ukupno 2^{28}. Grupne se adrese primjenjuju za aplikacije gdje jedan pošiljatelj šalje grupi primatelja, pri čemu se multiplikacija paketa obavlja u usmjerivačkim uređajima u točki razdvajanja prema pošiljateljima. U jednom trenutku na jednoj fizičkoj vezi postoji samo jedan paket grupne adrese odredišta.

IP adrese ovih klasa su globalno jedinstvene, što mreže i računala čini javnima.

U svakoj klasi postoje neke IP adrese posebne namjene, tzv. rezervirane adrese, koje se ne dodjeljuju računalu na mreži. IP adrese mreža s posebnim značenjem su:

- adresa 0 klase A (0.0.0.0) koja označava podrazumijevani put (default route). Toj adresi poslužitelj ili usmjernik prosljeđuje primljeni paket čije mu je odredište nepoznato.
- adresa 127.1.0.0 klase A, koja se uzima kao adresa povratne petlje (loopback address) i koristi za provjeru rada računala u mreži, jer se podaci poslani na tu adresu vraćaju natrag istom računalu. Naziv računala koji odgovara ovoj adresi je lokalno računalo (localhost).

Rezevirane adrese računala su:

- adrese svih mrežnih klasa sa svim bitovima broja računala u nuli - označava samu mrežu; npr. adresa 161.53.0.0 odnosi se na mrežu 161.53 klase B.
- adrese sa svim bitovima broja računala u jedinici je univerzalna adresa (broadcast) i paket upućen na tu adresu isporučuje se svim računalima na toj podmreži. Npr. poruka poslana na 161.53.255.255 bit će dostavljena svim računalima u mreži 161.53.0.0.

IP adresa označava mrežno sučelje i uređaji s više sučelja (prospojnici, usmjernici, poveznici) za svako od njih imaju različitu IP adresu.

IP protokol za usmjeravanje koristi mrežni dio IP adrese, a puna adresa gleda se tek kad paket stigle do odredišne mreže.

Problem IP načina adresiranja je u premalom broju raspoloživih blokova IP adresa, s obzirom na broj računala u Internetu i tendencije njegovog povećavanja. U početku je 32-bitna riječ izgledala dovoljno velika za sve buduće potrebe adresiranja. Podjela IP adrese na adresu mreže i adresu računala omogućila je vrlo efikasno administriranje adresa i usmjeravanje paketa. Međutim, u praksi je veliki broj adresa računala unutar dodijeljenog bloka adresa ostao neiskorišten, jer je svaki korisnik uzimanjem jedne mrežne klase rezervirao veliki broj pojedinačnih adresa za svoje buduće potrebe. Ovaj problem pokušava se riješiti na nekoliko načina:

- dijeljenjem adresnog prostora neke klase na manje blokova primjenom mrežnih adresnih maski,
- ujedinjavanjem susjednih blokova neke klase u jednu veću klasu (C u B)
- korištenjem skrivenih podmreža (intranet) s privatnim adresama i
- novom verzijom IP protokola, koja bi u zaglavlju paketa nosila adresu dovoljne duljine.

IPv6 uvodi novi sustav adresiranja od 128 bitova umjesto dosadašnjih 32 kod IPv4. Nastoji omogućiti prevođenje postojećih adresa u novi format kako bi se izbjegla ponovna dodjela adresa svim uređajima na mreži. Nedostatak adresiranja po IPv6 jest robustnos i potreba za složenijim obradama uređaja na krajevima mreže. Trenutno se na Internetu primjenjuje IPv4.

5.3.3.2 Mrežna maska i formiranje podmreža kao potklasa IP adresa

Svaka IP adresa pripada jednoj od mrežnih klasa. Međutim, primjenom mrežnih maski (netmask) omogućeno je formiranje potklasa i podmreža unutar jedne dodjeljene mrežne klase. Time se povećava broj mreža na račun broja računala u svakoj pojedinoj mreži.

Mrežna maska je 32-bitni broj koji kaže koje bitove originalne IP adrese treba promatrati kao bitove mrežnog broja. Ako je bit mrežne maske postavljen (vrijednost 1) smatra se da taj bit IP adrese pripada adresi mreže, svi ostali bitovi (vijednost 0) definiraju broj računala.

Sljedeća tablica daje primjer kako se jedna IP adresa može tumačiti na više načina ovisno o primjenjenoj mrežnoj maski. Adresa iz primjera 161.53.165.0 pripada, prema podjeli mrežnih klasa u klasu B, ali se primjenom mrežne maske 255.255.255.0 ponaša kao mreža klase C.

Mrežna maska	IP adresa **161.53.165.5**	
	4. oktet	**Interpretacija**
255.255.0.0	00000000	računalo 165.5 u mreži 161.53
255.255.255.0	00000000	računalo 5 u mreži 161.53.165; raspoloživa računala na mreži su 0-255 (rezervirani brojevi računala 0 i 255)
255.255.255.128	10000000	računalo 5 u prvoj od dvije podmreže; raspoložive adrese računala su: (1) 0-127 i (2) 128-255; granične su rezervirane
255.255.255.192	11000000	računalo 5 u prvoj od četiri podmreže; raspoložive adrese računala su: (1) 0-63; (2) 64-127 (3) 128-191 (4) 192-255; granične su rezervirane

Tablica 5.1 Interpretacija IP adresa, s obzirom na mrežnu masku

Formiranje podmreža primjenom mrežne maske omogućava decentralizirano administriranje i upravljanje dodijeljenom klasom adresa, sustavi su međusobno manje ovisni, a mogu se primjeniti dodatne sigurnosne mjere što doprinosi boljoj zaštiti sustava.

5.3.3.3 Identifikacija tokova podataka

IP adresa odredišta, kao ni par adresa odredište - izvorište, nisu dovoljni za identifikaciju toka podataka, jer svako računalo ili par računala može istovremeno prenositi više tokova podataka različitih korisnika i programa. Na prijenosnoj razini, korisnik komunikacije (toka) identificiran je brojem **priključne točke** (port). IP adresa i broj priključne točke se nazivaju **priključnica** (socket). Na strani poslužitelja koriste se unaprijed određeni brojevi priključne točke, tj. brojevi usluga. Na tom računalu moguća je pojava više tokova s istom priključnicom. Osim toga, različiti protokoli mogu istovremeno koristiti iste brojeve priključnih točaka. Stoga je za potpunu identifikaciju toka podataka, na Internetu potrebno koristiti izvorišnu i odredišnu priključnicu, dakle dvije IP adrese i dva broja priključne točke (usluge), te identifikaciju protokola prijenosne razine.

5.3.3.4 IP adrese za privatne mreže

Sustav adresiranja prema IP protokolu može se primjeniti na bilo kojoj mreži koja podržava TCP/IP skup protokola, bez obzira na namjeru njihovih povezivanja s drugim mrežama ili na Internet. Mreže za koje se smatra da se neće povezivati na Internet nazivaju se privatne mreže. No, dodjela IP adresa u takvim mrežama ne smije biti proizvoljna, jer u slučaju dupliciranih adresa pri povezivanju na Internet računala čije adrese već postoje ne bi ispravno funkcionirala. Upravni odjel za dodjelu mrežnih brojeva na Internetu (Internet Assigned Numbers Authority - IANA) rezervirao tri bloka IP adresa za privatne mreže:

10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

Računala unutar privatne mreže (privatna računala) kojima je dodijeljena IP adresa iz nekog od ovih blokova mogu komunicirati sa svim računalima, privatnim i javnim unutar organizacije, ali se ne mogu povezati IP vezom s vanjskim računalima. Takve mreže nazivaju se intranet mreže.

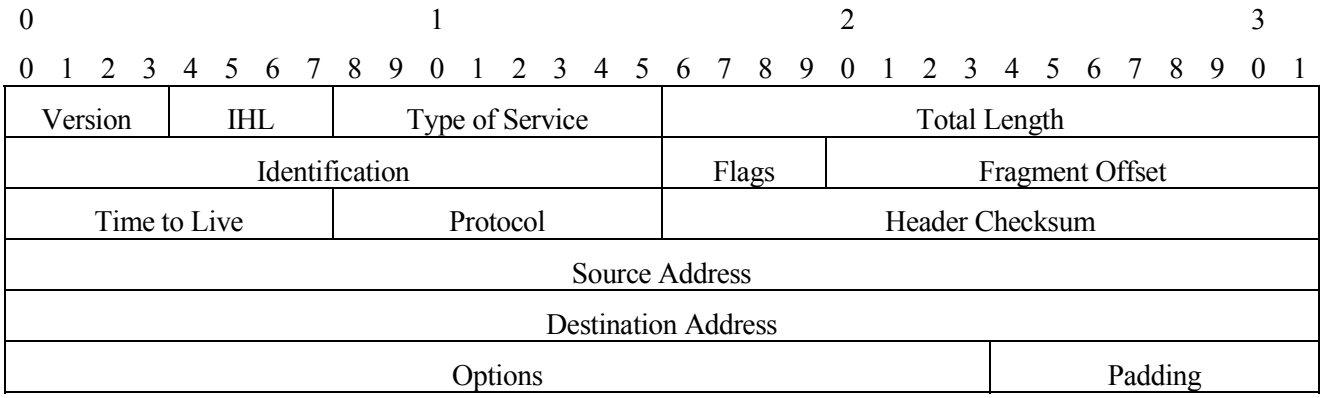
Mreže s privatnim IP adresama mogu se povezati na Internet na jedan od dva načina: maskiranjem (prevođenjem) IP adresa s privatne mreže na mrežnoj razini, ili primjenom proxy poslužitelja na prijenosnoj razini. U oba slučaja, cijela mreža je prema Internetu predstavljena jednim računalom koje ima javnu IP adresu.

Maskiranje privatnih IP adresa je postupak zamjene priključnice nekog računala s privatne mreže, priključnicom računala s javnom adresom. Maskaradu obavlja usmjernik, odnosno računalo koje je spojeno istovremeno na javnu i privatnu mrežu. Računalo s javnom IP adresom generira, za računalo s privatnom adresom, lokalni broj priključnice umjesto postojećeg broja. Na osnovu privatne IP adrese i broja priključne točke, računalo koje obavlja maskaradu zna kojem će računalu na lokalnoj mreži proslijediti primljene pakete.

Proxy poslužitelj ostvaruje dvije TCP veze, jednu prema računalu na Internetu i drugu prema računalu na lokalnoj mreži, te osigurava prosljeđivanje paketa s jedne veze na drugu. Primjenjuje se u realizaciji intranet mreža zaštićenih vatrenim zidom (firewall), odnosno za aplikacije kao što je WWW, gdje osim povećanih sigurnosnih mjera omogućava i smanjenje prometa u slučaju zahtjeva za nedavno dohvaćenim stranicama (caching). Kontrola pristupa obavlja se na početku uspostave TCP veze, a zatim se za odobrene komunikacije obavlja prijenos podataka između poslužitelja i klijenta.

5.3.3.5 IP zaglavlje

Prema IP protokolu, na podatke prijenosne razine (segment TCP, datagram UDP protokola) koji na mrežnoj razini čine jedinicu podataka ili SDU (Service Data Unit), dodaje se IP zaglavlje i tako formira PDU (Protocol Data Unit), odnosno IP paket. Zalgavlje sadrži kontrolne informacije i namjenjeno je mrežnoj razini prijemne strane. Prema potrebi, na mrežnoj razini se može obaviti fragmentacija IP paketa na manje IP pakete. Na osnovu podataka iz IP zaglavlja, na prijemnoj strani se obavlja sastavljanje svih fragmenata u originalni paket. IP zaglavlje ima oblik:



Slika 5.6. IP zaglavlje

Naziv	**bita**	**Opis**
Version	4	verzija IP protokola (trenutno u primjeni v4); određuje format zaglavlja
Internet Header Length (IHL)	4	duljina IP zaglavlja u 32-bitnim riječima, omogućava određivanje početka podataka; minimalna duljina ispravnog zaglavlja je 5
Type of Service (TOS)	8	tip usluge, omogućava usmjernicima različit tretman pojedinih paketa u cilju postizanja zadovoljavajuće kvalitete usluge (QoS), a s obzirom na dozvoljeno kašnjenje, veličinu prometa i zahtjevanu pouzdanost
Total Length	16	ukupna duljina IP paketa u oktetima, uključujući IP zaglavlje i podatke; najveća duljina paketa je 65,535 okteta (s obzirom na 16-bitno polje TL)
Identification	16	identifikator paketa, bitan pri povezivanju svih fragmenata u paket
Flags	3	kontrolne zastavice, definiraju je li fragmentacija dozvoljena i, ako jest, ima li još fragmenata istog paketa
Fragment Offset	13	definira mjesto fragmenta u originalnom paketu, mjereno u jedinicama od 8 okteta (64 bita); odstupanje prvog fragmenta je nula
Time to Live	8	maksimalno vrijeme života paketa u mreži, nakon čega se neisporučeni paket odbacuje; mjeri se u sekundama, čvorište koje obrađuje paket umanjuje vrijednost za najmanje 1, a ako je nula paket se odbacuje.
Protocol	8	označava protokol više razine kojem se podaci prosljeđuju
Header Checksum	16	kontrolni zbroj zaglavlja; ponovno se obračunava i provjerava pri svakoj promjeni podataka u zaglavlju (npr. pri umanjivanju TTL)
Source Address	32	adresa izvorišta paketa
Destination Address	32	adresa odredištapaketa
Options	*	varijabilne duljine, opcionalne; sadrže kontrolne informacije o usmjeravanju prijenosa, sigurnosne parametre itd.
Padding	*	varijabilne duljine, kako bi polje opcija dopunilo do 32 bita; popunjava se nulama

Tablica 5.2. Zaglavlje IP paketa

5.3.3.6 Fragmentacija paketa

Podaci putuju mrežama različitih fizičkih svojstava i zahtjeva na veličinu. Svaka mreža definira maksimalnu prijenosnu jedinicu (MTU - Maximum Transmission Unit) i taj podatak je dostupan svim usmjernicima koji povezuju Internet podmreže. Kad usmjernika primljeni paket treba poslijediti mreži s manjom MTU, na mrežnoj razini obavlja se fragmentacija, tj. podjela originalnog paketa u manje i svakom se dodaje IP zaglavlje. Podjela paketa može biti izričito zabranjena, na primjer u slučaju kad odredište nije sposobno sve primljene pakete spojiti u originalni. Nedjeljivost paketa označava se u polju zastavila. Isto polje definira ima li još fragmenata istog paketa (More Fragments bit), a udaljenost pojedinog fragmenta od početka definira polje Fragment Offset.

5.3.3.7 Usmjeravanje paketa

Cilj usmjeravanja je najkraćim putem u najkraćem roku dostaviti paket od izvorišta do odredišta. Konačni put kojim će paket proći kompromis je upravo ta dva uvjeta. U mrežama s komutacijom paketa koje svaki paket usmjeravaju zasebno, dva paketa koja pripadaju istoj poruci ne moraju proći istim putem. Usmjeravanje paketa od izvorišta do odredišta obavljaju usmjerivački uređaji na osnovu tablice usmjeravanja (routing table). Te se tablice u praksi formiraju na osnovu podataka o dostupnosti i udaljenosti podmreža. Podatke o dostupnosti usmjernici razmjenjuju nekim od usmjerivačkih protokola (RIP, EGP).

Na osnovu odredišne adrese u IP zaglavlju paketa obavlja se usmjeravanje paketa kroz mrežu. Pri tome se koristi samo mrežni dio adrese, sve dok paket ne stigne na odredišnu podmrežu. Ako je odredišna podmreža podjeljena primjenom mrežnih maski, paket se dalje usmjerava prema IP adresi i mrežnoj maski. Na krajnjoj podmreži, koja se obvezno proteže u granicama zone prostiranja lokalne mreže (broadcast domain), adresa krajnjeg uređaja saznaje se na osnovu broja računala u IP adresi paketa (ARP). Korištenjem dobivene adrese formira se okvir podatkovne razine u čijem se informacijskom polju nalazi IP paket (podatkovna razina dodaje zaglavlje IP paketu). Usmjernik šalje okvir s IP paketom krajnjem uređaju. Istom tehnikom razmjenjuju se paketi među računalima iste podmreže.

Kada IP primi paket upućen lokalnom računalu, on mora proslijediti podatke točnom protokolu prijenosne razine. Svaki protokol prijenosne razine ima jedinstveni broj preko kojeg ga IP prepoznaje, a u paketu se nalazi u trećoj riječi zaglavlja, u polju protokol (Protocol).

5.3.3.8 IP protokol i kvaliteta usluge

Internet je mreža s komutacijom paketa kod koje se prijenos podataka obavlja bez prethodne rezervacije kapaciteta. Usluge se pružaju po načelu najbolje što može u datom trenutku (best-effort). Mrežna razina ne jamči točnost isporuke podataka ni duljinu trajanja prijenosa - brzinu, dinamiku ni kašnjenje. Ovisno o raspoloživom kapacitetu i opterećenju varira i brzina prijenosa raspoloživa pojedinom korisniku.

Različite mrežne usluge na Internetu imaju različite zahtjeve s obzirom na kašnjenje, varijaciju kašnjenja (jitter), raspoloživu pojasnu širinu i brzinu prijenosa, u cilju postizanja zadovoljavajuće kvalitete usluge (Quality of Service - QoS). Na primjer, za uslugu prijenosa datoteka s jednog računala na drugo (FTP) bitno je da svi paketi stignu do odredišta, a dinamika prijenosa ne mora biti presudna. Usluge u realnom vremenu, te multimedijalni tokovi podataka zahtjevaju veću pojasnu širinu i osjetljiviji su na kašnjenje, ali ne toliko na gubitak paketa (zbog redundancije govora i video signala).

Radne skupine Interneta trenutno su usmjerene na pronalaženje rješenja koja će omogućiti prijenos usluga različitih zahtjeva prema parametrima kvalitete usluge preko IP mreže, uključujući tehnike rezervacije kapaciteta (RSVP - Resource Reservation Protocol), te definiranjem različitih tipova usluga (Diffserv).

IP protokol je bespojni protokol, što znači da ne omogućava kontrolu pogrješki, ne osigurava potvrdu prijema paketa u bilo kojem segmentu puta (od točke do točke, niti s kraja na kraj veze). Konzistenciju korisnikovih podataka mora osigurati protokol više razine, npr. TCP koji je spojevni. Kod IP protokola, detekcija pogrješke prepuštena je protokolima niže razine, osim kontrolnoh zbroja zaglavlja koji omogućava dodatnu kontrolu ispravnosti samoh zaglavlja. Paket s oštećenim zaglavljem se odbacuje, a obavijest o tome dojavljuje se izvorištu porukom ICMP protokola.

5.3.4 ICMP - Internet Control Message Protocol

ICMP (RFC 792) je protokol mrežne razine i sastavni dio IP protokola, iako se ponaša kao protokol više razine šaljući svoje poruke preko IP protokola. Osnovna namjena ICMP protokola jest osigurati nadzor i kontrolu

prijenosa podataka do odredišta, s obzirom da to IP protokol ne osigurava. ICMP šalje poruke koje osiguravaju kontrolu toka, prijavu pogreške, pojavu alternativnog puta do odredišta i druge informacije namijenjene samoj TCP/IP programskoj podršci. Time nije osiguran pouzdani prijenos podataka, već to treba osigurati protokol više razine. Poruke se šalju samo kao odgovor na poslane IP, ali ne i ICMP pakete. U slučaju gubitka ICMP poruke, ne generira se nova ICMP poruka o nastaloj pogrešci. ICMP poruke se šalju koristeći osnovno IP zaglavlje. Prvi oktet polja podataka IP paketa definira tip ICMP poruke, čime je određen format ostatka podataka. Vrijednost polja protokola za ICMP poruku je 1. Svaka ICMP poruka sadrži i IP zaglavlje poruke o čijem gubitku izvještava, te prvih 64 bita podataka originalnog paketa.

ICMP generira osam različitih poruka, od kojih tri zahtjevaju odgovor:

- **odredište nedostupno** (Destination Unreachable) - šalje se kad nije moguće uspostaviti vezu ili pronaći put do odredišnog računala, kao i u slučaju da odredišno računalo ne može prepoznati koja se usluga od njega traži (ne prepoznaje "port", odnosno uslugu protokola više razine); ako je nedostupna mreža ili računalo, poruku šalje usmjerivački uređaj, a ako nije prepoznata usluga - odredišno račnalo. Ista poruka šalje se i u slučaju kad paket, označen kao nedjeljiv, ne može proći nekim segmentom mreže.
- **istek vremena** (Time Exceeded) - šalje se kad je paket odbačen jer je polje "vrijeme života" postalo jednako nuli. Koristi se za određivanje puta kroz mrežu.
- **problem s parametrima** (Parametar Problem) - poruku generiraju usmjernik ili odredišno računalo kad paket treba odbaciti jer usljed problema s parametrima u zagljavlju ne mogu završiti obradu paketa.
- **blokiranje izvorišta** (Source Quench) - generira se kad paketi stižu brže nego što ih odredište može obraditi, pa usmjerivački uređaj ili odredišno računalo šalju pošiljatelju ICMP poruku za privremeni prekid slanja paketa. Ovaj mehanizam pokazao se štetnim, pa je isključen.
- **preusmjeravanje** (Redirection) je ICMP poruka koju šalje usmjerivač kad u svojoj tablici puteva nađe drugi put do odredišta kojim se postiže veća pouzdanost ili brži prijenos. Jedini uvjet koji mora biti zadovoljen jest da se i taj drugi usmjerivački uređaj nalazi na istoj mreži.
- **eho zahtjev i eho odgovor** (Echo Request/Echo Reply) je par poruka kojim se saznaje je li odredište aktivno. Adrese izvorišta i odredišta zahtjeva zamjene mjesta u odgovoru. Poruke koristi naredba *ping*.
- **vrijeme i odgovor vremena** (Timestamp/Timestamp Reply) šalju se kad je potrebno odrediti za koje vrijeme se poruka preko odredišta vrati do izvorišta (Round Trip Time).
- **zahtjev za informacijom i odgovor na informaciju** (Information Request/Information Reply) koriste se za doznavanje adrese vlastite mreže.

Minimalna duljina ICMP poruke je 56 okteta: 20 (IP zaglavlje) + 8 (ICMP zaglavlje) + 20 (IP zaglavlje originalne poruke) + 8 okteta (originalni paket).

5.3.5 ARP - Address Resolution Protocol

Internet standard koji omogućava određivanje adrese odredišta kao fizičkog uređaja na osnovu njegove IP adrese naziva se ARP i definiran je u RFC 826. Iako je predviđen za više tipova lokalnih mreža, trenutno se primjenjuje samo za Ethernet mreže i omogućava dinamičku distribuciju podataka potrebnih za izgradnju tablica za prevođenje odredišne IP adrese u 48-bitnu Ethernet adresu. Svaka stanica raspolaže ARP modulom za određivanje adrese, koji u memoriji održava tablicu parova adresa.

Razina pristupa mreži šalje zahtjev ARP modulu za određivanje fizičke adrese uređaja na osnovu IP adrese. Ako ARP modul pronađe traženi par u tablici, prosljeđuje Ethernet adresu razini pristupa i paket se šalje unutar standardnog Ethernet okvira. Ukoliko ne pronađe traženi par, ARP modul generira ARP upit, kojim proziva stanicu s traženom IP adresom. Kako je fizička adresa stanice nepoznata, razina pristupa mreži dodaje svoje zaglavlje s univerzalnom (broadcast) Ethernet adresom odredišta. Na taj način ARP paket primaju sve stanice na lokalnoj mreži. Stanica koja u ARP paketu prepozna svoju IP adresu odazove se ARP odgovorom, koji također primaju sve stanice i koji sadrži fizičku adresu stanice. Očito je da je za funkcioniranje ARP protokola prijeko potreban mehanizam univerzalne adrese (broadcasting), odakle veza između područja podmreže Interneta i domene prostiranja lokalne mreže.

Format ARP paketa prikazan je na slici 5.7., a duljina pojedinog polja izražena je u broju okteta.

2	2	1	1	2	n	m	n	m
ar$hrd	ar$pro	ar$hln	ar$pln	ar$op	ar$sha	ar$spa	ar$tha	ar$tpa

ar$hrd - fizička adresa
ar$pro- identifikacija protokola
ar$hln - duljina fizičke adrese u oktetima
ar$pln - duljina ident. protokola u oktetima
ar$op - kôd operacije (request/reply)
ar$sha - fizička adresa izvorišta
ar$spa - identifikacija protokola izvorišta
ar$tha - fizička adresa odredišta
ar$tpa - identifikacija protokola odredišta

Slika 5.7. ARP paket

U polju fizičke adrese je kôd mreže preko koje se obavlja prijenos:

Vrijednost	Tip mreže	Vrijednost	Tip mreže
1	Ethernet (10 Mb)	16	ATM
6	IEEE 802 Networks	17	HDLC
15	Frame Relay	20	Serial Line

Tablica 5.3. Kôdovi nekih mreža prema ARP protokolu

U polju identifikacije protokola je kôd protokola koji je zatražio određivanje adrese. Polja koja određuju duljinu fizičke adrese (u ovom slučaju Ethernet adrese, n=6) i duljinu adrese protokola (u ovom slučaju IP adrese, m=4) nepotrebna su, jer se duljina tih adresa može odrediti i iz kôdova mreže i identifikacije protokola navedenih u prva dva polja paketa. Kôd operacije određuje radi li se o zahtjevu (opcode=1) ili odgovoru na prethodni zahtjev (opcode=2). Duljine polja fizičke adrese i identifikacije protokola izvorišta i odredišta (n i m) određene su na osnovu polja ar$hln i ar$pln i izražene u oktetima.

Zapisi u ARP tablici povremeno se osvježavaju, pri čemu se brišu podaci o uređajima s kojima se duže vrijeme nije komuniciralo. Alternativa ARP protokolu u saznavanju fizičke adrese odredišta bila bi povremeno slanje paketa univerzalne adrese svim uređajima na mreži, što uzrokuje suvišan i nepotreban promet po mreži.

5.3.6 Broj protokola i broj usluge

Kad su podaci dostavljeni određenom računalu (na osnovu IP i fizičke adrese), treba ih dostaviti točnom protokolu na prijenosnoj razini, te točnom procesu ili aplikaciji na korisničkoj razini. IP protokol koristi brojeve protokola (protocol numbers) za prepoznavanje protokola na prijenosnoj razini, a ti protokoli koriste brojeve usluga (port numbers) preko kojih prepoznaju kojoj su aplikaciji upućeni podaci. Brojevi protokola i usluga nisu ništa drugo nego brojevi priključnih točaka na sučeljima između mrežne i prijenosne, te prijenosne i korisničke razine. Brojevi protokola i priključnih točaka poslužitelja (well-known ports) definirani su RFC dokumentima *Assigned Numbers*. Na UNIX računalu brojevi korištenih protokola i usluga nalaze se u datotekama */etc/protocols* i */etc/services*.

Broj protokola je veličine jednog okteta, a nalazi se u trećoj riječi IP zaglavlja paketa. Vrijednost tog polja identificira protokol prijenosne razine koji je generirao, odnosno kojem treba proslijediti podatke. Dovoljna je jedna identifikacija protokola prijenosne razine, jer se naravno radi o istom protokolu s obje strane veze. U datoteci */etc/protocols* na UNIX računalu nalaze se, u obliku tablice, imena i pridruženi brojevi protokola:

```
# Internet (IP) protocols
      ip    0     IP    # internet protocol
      icmp  1     ICMP  # internet control message protocol
      tcp   6     TCP   # transmission control protocol
      udp   17    UDP   # user datagram protocol
```

U datoteku se upisuju samo protokoli koji se koriste. Upis svih mogućih protokola je nepotreban.

IP proslijedi pristigle podatke protokolu prijenosne razine koji ih propušta točno određenom procesu korisničke razine. Aplikacijski procesi ili mrežne usluge, označeni su 16-bitnim brojem priključne točke (port), koja na poslužitelju ujedno označava uslugu. U prvoj riječi zaglavlja TCP segmenta i UDP datagrama nalaze se izvorišni broj priključne točke (source port number) koji upućuje na proces koji šalje podatke, te odredišni broj priključne točke (destination port number) procesa koji prima podatke.

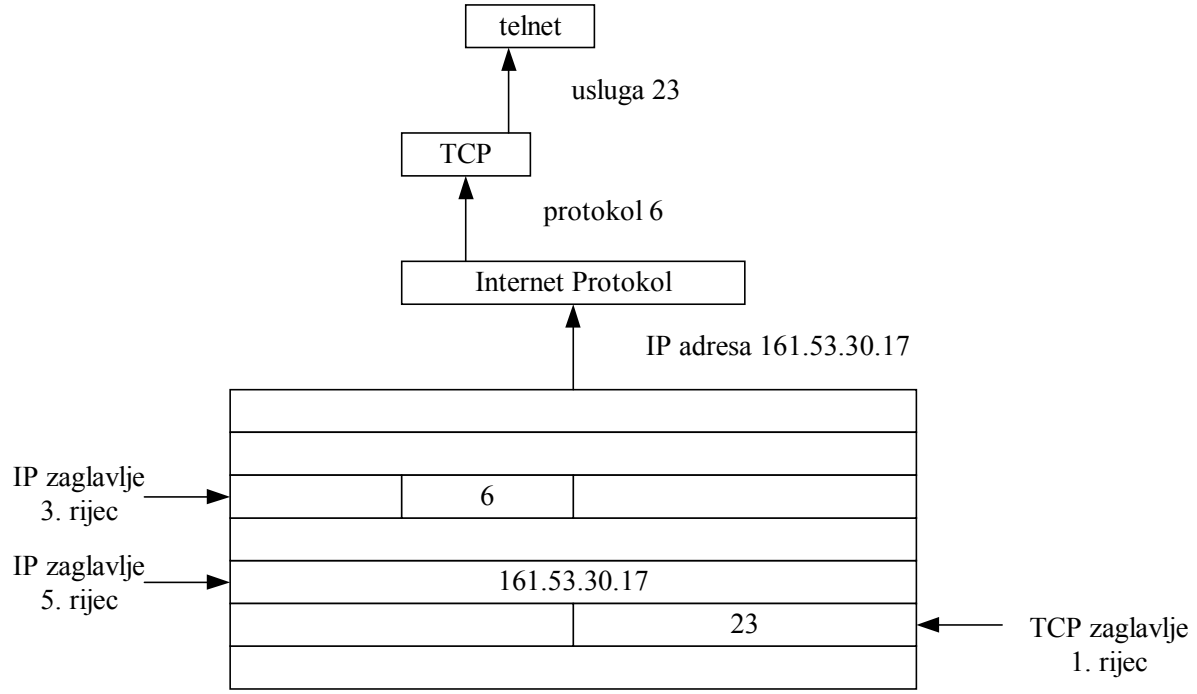
Brojevi priključnih točaka 0 - 1024 unaprijed su dodijeljeni uslugama. Na UNIX računalima, brojevi usluga nalaze se u datoteci */etc/services*. Brojevi usluga ispod 256 rezervirani su za najčešće korištene usluge kao što su FTP, TELNET, SMTP; brojevi 256 - 1024 koriste se za posebne UNIX usluge (npr. rlogin). Brojevi iznad

standardnih dodjeljuju se dinamički korisničkim procesima. Brojevi usluga su jedinstveni jedino unutar jednog protokola, dok više protokola prijenosne razine mogu dodjeljivati iste brojeve (npr. TCP i UDP koriste iste brojeve za svoje usluge).

Datoteka */etc/services* ima oblik tablice, a sadrži naziv usluge i zapis tipa broj_usluge/protokol, koji kaže koji protokola prijenosne razine koristi koji priključni broj za naznačenu uslugu:

```
# Network services #
ftp             21/tcp
telnet          23/tcp
smtp            25/tcp      mail
time            37/tcp      timeserver
time            37/udp      timeserver
# UNIX specific services #
login           513/tcp
who             513/udp     whod
talk            517/udp
```

Na slici 5.8. prikazan je proces dostave podataka do aplikacije u odredišnom računalu čija je IP adresa u petoj riječi IP zaglavlja. Na osnovu broja protokola u trećoj riječi IP zaglavlja (6), IP protokol određuje kojem se protokolu prijenosne razine prosljeđuju podaci (TCP). Prva riječ TCP zaglavlja sadrži odredišni broj usluge (23) čime je određeno kojoj se aplikaciji predaju podaci (telnet).



Slika 5.8. Broj protokola i broj usluge na odredištu

Odredišni broj usluge uvijek je standardni i unaprijed poznati broj definiran na sustavu kroz */etc/services* ili drugom odgovarajućom datotekom. Izvorišni broj usluge dodjeljuje se dinamički i nije unaprijed poznat. Takva dodjela brojeva usluge omogućava većem broju korisnika istovremeno korištenje iste usluge, a par izvorišni-odredišni broj usluge ostaje jedinstven.

IP adresa i broj usluge često se nazivaju **priključnica** (socket). Priključnica se zapisuje u obliku IP_adresa:broj_usluge, npr. 161.53.30.3:23. - 161.53.30.3 je adresa računala, a 23 je broj usluge telnet. Postoje priključnica izvorišnog računala (IP adresa izvorišnog računala i slučajno dodjeljen izvorišni broj usluge) i priključnica odredišnog računala (uz IP adresu se nalazi standardni broj usluge); računala razmjenjuju priključnice tijekom uspostave TCP veze (TCP rukovanja). Priključnica jedinstveno određuje mrežni proces unutar Interneta, a par priključnica - izvorišnog i odredišnog računala jedinstveno definira vezu sa spajanjem.

5.3.7 UDP - User Datagram Protocol

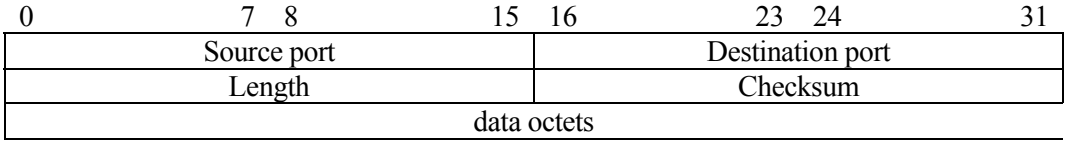
User Datagram Protocol, RFC 768 je protokol prijenosne razine koji koristi IP protokol, a omogućava protokolima više razine slanje poruka drugim programima uz minimalno korištenje mehanizama protokola. Temeljen je na bespojnom prijenosu, ne garantira sigurnu isporuku podataka i ne preporuča se za primjenu aplikacijama kojima je bitna sigurna i pouzdana isporuka. UDP osigurava točan prijenos unutar računala, tj. podaci dođu do viših slojeva onakvi kakvi su primljeni s mreže.

Postoji nekoliko slučajeva kada se za prijenos poruka koristi UDP, a ne TCP protokol

- potrebno poslati manji blok podataka, veličine jednog paketa, pa je jednostavnije i brže prenositi samo podatke (uz UDP zaglavlje), bez dodatnih kontrola, a u slučaju pogrešnog prijema poslati ponovno;
- slanje upita jednog računala drugom uz ponavljanje upita ako odgovor ne stigne nakon isteka određenog vremenskog intervala; na upit se također može odgovoriti primjenom UDP protokola;
- prijenos podataka aplikacija koje imaju vlastite tehnike osiguravanja pouzdanog prijenosa, ili su manji gubici dozvoljeni.

UDP dodaje znatno manje zaglavlje, što cijeli datagram koji predaje mrežnoj razini čini manjim.

U zaglavlju UDP datagrama nalaze se 16-bitne adrese izvorišnog i odredišnog broja usluge, informacija o duljini cijele poruke, te zbroj na osnovu kojeg se obavlja provjera je li poruka ispravno primljena. Minimalna duljina UDP zaglavlja je 8 okteta. Format zaglavlja UDP datagrama prikazan je na slici 5.9.:

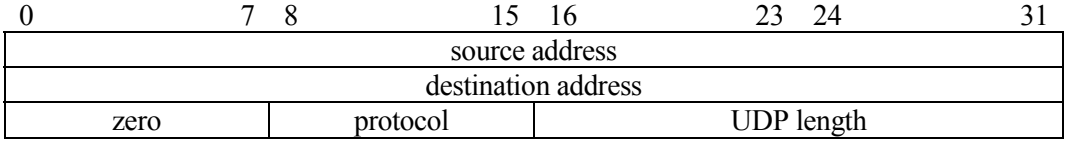


Slika 5.9. UDP zaglavlje

Naziv	bita	Opis
Source port	16	Izvorišni broj usluge je opcionalno polje. Kad se koristi, označava priključni točku procesa koji šalje podatke i na koju stiže odgovor u slučaju da ne postoji druga informacija. Ako se polje ne koristi popuni se nulama.
Destination port	16	Odredišni broj usluge, značenje na odredišnoj IP adresi
Length	16	Duljina UDP datagrama u oktetima uključujući zaglavlje i podatke. Minimalna duljina UDP datagrama je 8 okteta.
Checksum	16	Kontrolni zbroj zaglavlja, računa se na osnovu pseudo zaglavlja iz IP i UDP zaglavlja i podataka. Ako je polje ispunjeno nulama znači da pošiljatelj nije računao zbroj; ako je zbroj jedna nuli, prenosi se kao niz jedinica.
data octets		Podaci

Tablica 5.3. UDP zaglavlje

Pseudo zaglavlje prethodi UDP zaglavlju, sadrži adrese izvorišta i odredišta, protokol i duljinu UDP datagrama, a osigurava protiv pogrešno usmjeravanih datagrama. Kontrolni zbroj računa se na isti način kao i za TCP zaglavlje:



Slika 5.10. Pseudo UDP zaglavlje

UDP protokol koriste protokoli NFS (Network File System, RFC 1094), SNMP (Simple Network Management Protocol, RFC 1157).

5.3.8 TCP - Transmission Control Protocol

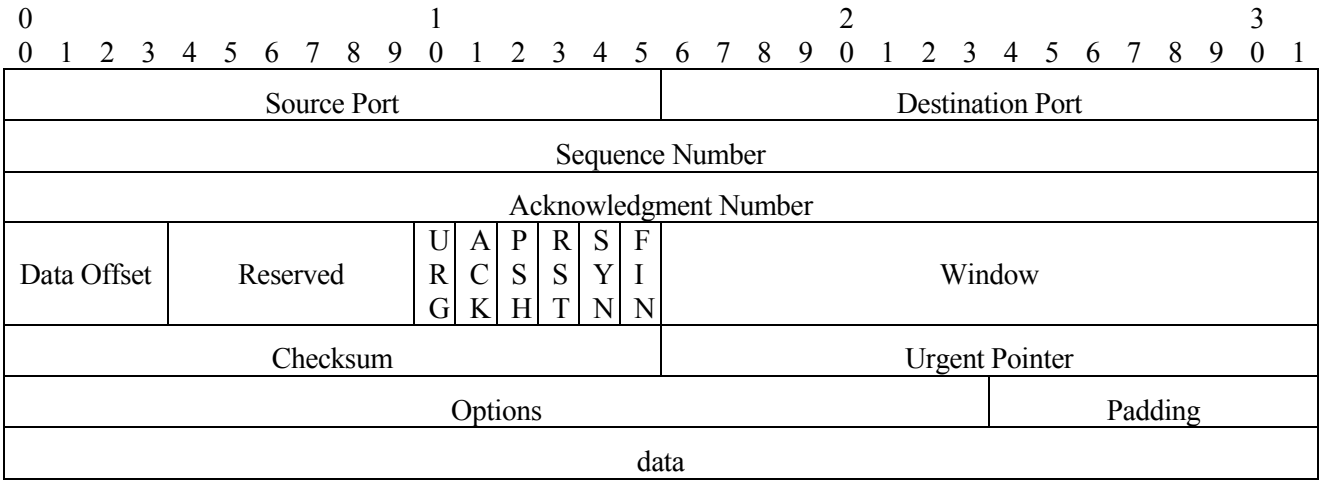
TCP je protokol prijenosne razine TCP/IP komunikacijskog modela i opisan je u dokumentu RFC 793. To je pouzdan, spojevni protokol, koji podatke promatra kao kontinuirani slijed, a ne skup međusobno neovisnih poruka. Osnovna jedinica podataka TCP protokola koja se izmjenjuje između dva krajnja uređaja, naziva se segment.

TCP je **pouzdan** protokol jer za svaki poslani segment očekuje potvrdu prijema (ACK - Acknowledgment). Ako nakon isteka određenog vremenskog intervala pozitivna potvrda ne stigne, ili stigne informacija o netočno primljenim podacima, prijenos se ponavlja sve dok ne stigne pozitivna potvrda prijema.

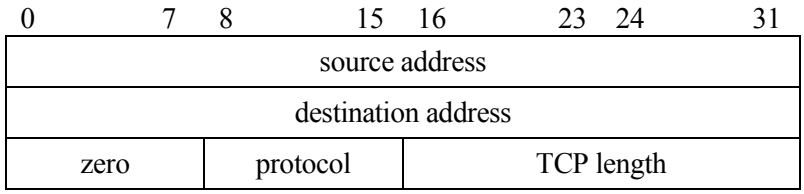
TCP je **spojevni** protokol (connection-oriented), osigurava vezu sa spajanjem, uspostavlja logičku vezu ili virtualni kanal između dva krajnja uređaja. Uspostavi veze prethodi razmjena tri segmenta s upravljačkim informacijama u procesu koji se označava kao trostruko rukovanje (three-way handshake). Pozivajuće računalo prvo šalje sinkronizirajuću poruku *SYN* kojom obavijesti drugo računalo da želi s njim komunicirati i pošalje svoj redni broj (Sequence Number), a to je broj od kojeg predajna strana počinje označavati segmente koje šalje. Redni brojevi se koriste kako bi se sačuvao pravilan slijed podataka. Pozvano računalo odgovara šaljući segment koji sadrži potvrdu prijema *ACK* (Acknowledgment) i SYN. Tim segmentom pozvano računalo potvrđuje prijem poziva i pošalje pozivajućem računalu svoj redni broj. Na kraju, pozivajuće računalo pošalje segment kojim potvrđuje prijem segmenta pozvanog računala i šalje svoje prve podatke. Nakon te razmjene, TCP pozivajućeg računala zna da je udaljeno računalo aktivno i da je spremno primiti podatke. Čim se veza uspostavi, podaci se mogu prenositi. Kad se prenesu svi podaci, dva uređaja trostrukim rukovanjem razmjenjuju segmente s kontrolnim informacijama, koji sadrže *FIN* (Final) bit i kojim se veza prekida (zatvara), jer pošiljatelj nema više podataka za odredišno računalo.

TCP osigurava pravilan **tok podataka**, označavajući redni broj segmenta u poruci. Broj prvog segmenta može biti bilo koji, iako je najčešće nula. Stizanje segmenata poruke na odredište potvrđuje poruka ACK, na osnovu koje izvorište prima informaciju koliko je ispravnih segmenata do tada primljeno, te koliko ih se još može primiti. Na potvrdama prijema temelji se kontrola toka i određuje dinamika daljnjeg slanja podataka odredištu. Potvrđeni broj, kojeg nosi ACK, je redni broj posljednjeg okteta kojeg je udaljeno računalo ispravno primilo. Udaljeno računalo ne mora slati potvrdu prijema za svaki primljeni paket. Prema standardu, pošiljatelj može smatrati da su ispravno primljeni svi okteti zaključno s onim na kojeg ukazuje potvrđeni broj. Polje prozor (Window) u zaglavlju segmenta sadrži broj okteta koje udaljeno računalo još može primiti, pa predajno računalo može slati segmente sve dok ukupni broj okteta ne bude veći od broja okteta upisanih u polju prozor. Prijemno računalo mijenja veličinu prozora nakoln svakog okteta koji primi i tako nadzire tok podataka. Kad je veličina prozora jednaka nuli, predajno računalo treba prekinuti slanje paketa dok ne dobije segent u kojem je veličina prozora veća od nule.

TCP zaglavlje i pseudo zaglavlje (koje konceptualno prethodi TCP zaglavlju) dani su na slikama 5.11. i 5.12.:



Slika 5.11. TCP zaglavlje



Slika 5.12. Pseudo TCP zaglavlje

Pojedina polja TCP zaglavlja objašnjena su u sljedećoj tablici:

Naziv	**bita**	**Opis**
Source Port	16	izvorišni broj priključne točke (usluge)
Destination Port	16	odredišni broj priključne točke (usluge)
Sequence Number	32	redni broj prvog okteta podataka u tom segmentu; ako je postavljena zastavica SYN, onda je to početni redni broj (ISN - initial sequence number), a prvi oktet podataka ima broj ISN+1
Acknowledgment Number	32	potvrdni broj; ako je postavljen ACK bit, polje sadrži redni broj sljedećeg okteta kojeg primatelj očekuje
Data Offset	4	pomak podataka - pokazuje na početak podataka u TCP segmentu, izraženo u 32-bitnim riječima (TCP zaglavlje je uvijek višekratnih 32-bitne riječi).
Reserved	6	rezervirano za buduće potrebe; popunjeno nulama
Control bits	6	kontrolni bitovi: URG - indikator hitnih podataka ACK - indikator paketa koji nosi potvrdu PSH - inicira prosljeđivanje korisniku svih do tad neprosljeđenih podataka RST - ponovna inicijalizacija veze SYN - sinkronizacija rednih brojeva FIN - predajnik više nema podataka za slanje
Window	16	prozor označava koliko je okteta prijemnik spreman primiti
Checksum	16	kontrolni zbroj; računa se kao 16-bitni komplement jedinice komplementa zbroja svih 16-bitnih riječi u zaglavlju i podacima; pokriva i 96 bitova pseudo zaglavlja koje sadrži izvorišnu i odredišnu adresu, protokol i duljinu TCP zaglavlja i podataka (Slika 5.12.)
Urgent Pointer	16	pokazivač na redni broj okteta gdje se nalaze hitni podaci; polje se gleda jedino ako je postavljena zastavica URG
Options		mogu, a ne moraju biti uključene; ako postoje, veličine su x*8 bita
Padding		dopuna nulama do 32 bita
data		podaci korisničke razine

Tablica 5.4. Polja TCP zaglavlja

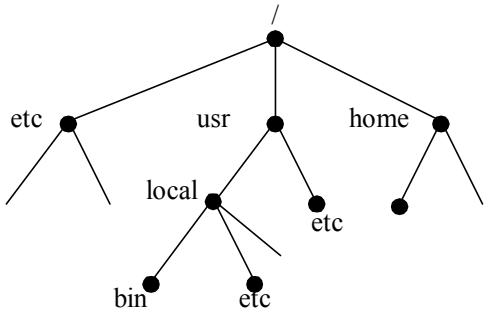
TCP osigurava dopremu podataka od mrežne razine (IP protokola) do željenog aplikacijskog procesa ili usluge, definiranih 16-bitnim brojem usluge. Izvorišni i odredišni broj usluge nalaze se u prvoj riječi TCP zaglavlja.

5.3.9 NFS - Network File System Protocol

NFS protokol (RFC 1094) razvila je tvrtka Sun Microsystems, a pruža transparentni pristup datotekama na udaljenim računalima koje istodobno može koristiti više korisnika. Protokol se lako prenosi na različita računala, operacijske sustave, te različite mrežne arhitekture. Na prijenosnoj razini koristi UDP protokol. NFS znatno povećava opterećenje mreže i nepraktičan je na sporim linijama, ali pruža znatne prednosti. NFS klijent ugrađen je u jezgru operacijskog sustava i omogućava aplikacijama i naredbama korištenje priključenog čvrstog diska kao da je lokalan.

NFS pretpostavlja hijerarhijski datotečni sustav - sustav direktorija i datoteka organiziran počevši od korijena stabla (root, korijenski direktorij) koji sadrži više poddirektorija, od kojih svaki može sadržavati daljnje poddirektorije i datoteke. Svaki element direktorija (datoteka, poddirektorij, uređaj, veza, itd.) ima naziv u obliku niza znakova, a njegovo je mjesto jednoznačno definirano stazom ili putem (path). Različiti operacijski sustavi imaju različita pravila o dozvoljenim nazivima, odnosno postavljaju ograničenja na broj znakova u imenu,

definiraju mogućnosti i pravila korištenja specijalnih znakova i znakova interpunkcije, a može se razlikovati i način označavanja puta do datoteke.



Slika 5.13. Hijerarhijski organiziran datotečni sustav

Mjesto datoteke ili direktorija u hijerarhijskoj strukturi može biti zadano apsolutno (od korijena stabla) ili relativno (gledano od mjesta gdje se trenutno nalazi u datotečnom sustavu). NFS analizira jedan po jedan segment puta do datoteke počevši od korijena stabla, a prednost takvog pristupa jest u činjenici da različiti operacijski sustavi koriste različite znakove kao separatore u apsolutnom putu do datoteke. Pri dodavanju datotečnih sustava drugih računala vlastitom (mounting), sustavi direktorija se, na UNIX sustavu, prikazuju kao dodatna datoteka postojećem korijenskom (root) direktoriju.

Neki operacijski sustavi (MS Windows) koriste druge protokole za pristup datotečnom sustavu drugih računala. Povezane diskove prikazuju kao dodatne uređaje, koji se pojavljuju na popisu uređaja ravnopravno s disketnom jedinicom, cd rom-om, te jednim ili više diskova samog računala.

Povezivanje udaljenog datotečnog sustava kontrolira se provjerom prava korisnika. Na udaljenom računalu, datotečni sustav mora biti označen za daljinski pristup, te moraju biti definirani korisnici koji na pristup imaju pravo. Takav korisnik sa svog računala mora inicirati pristup udaljenom sustavu, te mu po potrebi dokazati svoj identitet (imenom računala, ili korisničkim imenom i lozinkom). Povezivanje udaljenog datotečnog sustava najčešće se obavlja automatski kod uključenja računala.

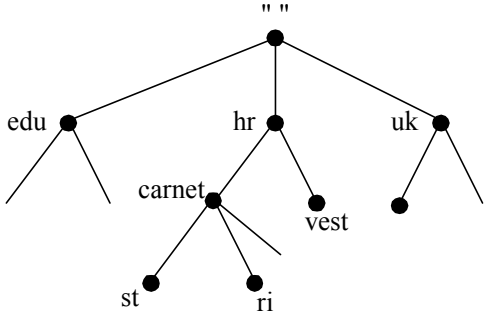
Slično daljinskom korištenju datotečnog sustava, mogu se koristiti i ostali resursi udaljenih računala (pisač, cd rom, disketna jedinica, uređaj magnetske trake).

5.3.10 DNS - Domain Name System

Svakom adresabilnom uređaju na mreži može se pristupiti na dva načina - preko IP adrese ili preko Internet naziva računala. Uređaji međusobno komuniciraju na osnovu binarnih adresa, dok je ljudima puno jednostavnije pamtiti i raditi s logički dodjeljenim imenima. Ime računala označava se kao FQDN (Fully Qualified Domain Name), tj. potpuno definirani područni naziv. Sustav koji omogućava jednoznačnu vezu između numeričkih IP adresa i naziva računala, naziva se sustav područnih naziva ili DNS (Domain Name System). Alternativa DNS sustavu su tablice računala (host table), ali je takav pristup uglavnom napušten. DNS je definiran u RFC dokumentima 1034 i 1035.

Organizacija domena

Sustav područnih naziva predstavlja se, slično datotečnom sustavu, u obliku okrenutog stabla s korijenom na vrhu:



Slika 5.14. Hijerarhijski organiziran sustav područnih naziva

Domene prve razine ispod korijena stabla nazivaju se vršne ili primarne domene (Top-Level Domain). Vršna domena je za većinu zemalja u svijetu oznaka države kojoj mreža pripada (npr. *ca* - Kanada, *de* - Njemačka, *hr* - Hrvatska, *uk* - Velika Britanija, i sl.). Izuzetak su Sjedinjene Američke Države, gdje vršne domene predstavljaju vrstu organizacije (npr. *com* - poduzeća i komercijalne ustanove, *edu* - obrazovne, *gov* - vladine, *mil* - vojne ustanove, *org* - privatne organizacije, društva i udruge).

Vršna domena može imati jednu ili više poddomena (sekundarnih domena). Sekundarna domena je najčešće oznaka organizacije (tvrtke, fakulteta, instituta) unutar vršne domene kojoj računalo pripada. Sekundarna domena također može imati više poddomena, itd. Sve grane koje izlaze iz jednog čvora, nose naziv tog čvora kao naziv poddomene.

Administracija jedne domene povjerava se jednoj organizaciji, koja tu domenu može dijeliti u više poddomena i za njihovo održavanje odrediti druge organizacije.

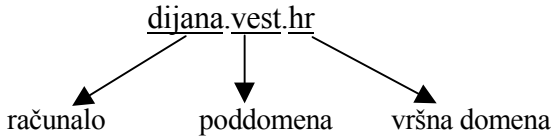
Dodjelu IP adresnog prostora i povjeravanje administriranja domenskih poslužitelja za cijelu Internet zajednicu koordinira organizacija ICANN (The Internet Corporation for Assigned Names and Numbers), nasljednik organizacije IANA (Internet Assigned Number Authority).

Vršna domena Republike Hrvatske je **.hr**, a administrator domene je ustanova CARNet - Hrvatska akademska i istraživačka mreža. Pravila registracije sekundarnih domena unutar vršne domene .hr, dostupna su na adresi http://www.CARNet.hr/DNS/.

Formiranje naziva uređaja (FQDN)

Kao što se IP adresa sastoji iz dva dijela - mrežnog broja i broja računala, tako se i u nazivu računala jedan dio odnosi na mrežu kojoj računalo pripada - domenu, a drugi na samo računalo. Domena predstavlja područje definiranosti i organiziranosti mreže i obično se sastoji od vršne domene i jedne ili više poddomena. Naziv vršne domene obično ima 2 ili 3 znaka, dok je naziv poddomene ograničen na najviše 63 znaka.

Naziv računala jedinstveno definira sam uređaj na mreži. Puni naziv uređaja piše se od čvorova prema korijenu stabla, a pojedini djelovi naziva međusobno se odvajaju točkama, npr:



Jedan uređaj može imati više simboličkih naziva. Npr, glavni poslužitelj koji je ujedno i WWW i proxy poslužitelj može uz vlastiti naziv imati imati simboličke nazive - www i proxy. Jedna od prednosti simboličkih naziva jest što promjena naziva uređaja ne implicira promjenu konfiguracijskih parametara i ne remeti dostupnost usluge. Na primjer, zamjenom proxy poslužitelja nije potrebno mijenjati konfiguraciju Web preglednika svih računala korisnika; adresa www.poddomena.domena može ostati ista bez obzira na kojem se računalu nalaze WWW stranice.

Rad DNSa

DNS (Domain Name Server) je distribuirani sustav baza podataka. Zapisi u bazi odnose se na uređaje na mreži i sadrže naziv domene kojoj uređaj pripada, IP adresu, te jedan ili više naziva kojim se uređaj definira. Zapisi su indeksirani prema nazivima domena.

Sustav područnih naziva organiziran je na principu klijent-poslužitelj, a distribuiranost omogućava lokalni nadzor i održavanje pojedinog segmenta baza podataka. Lokalna administracija se najčešće povjerava čvorovima poddomene. Podaci svakog lokalno administriranog segmenta dostupni su putem mreže postavljanjem upita klijenata domenskom poslužitelju.

Domenski poslužitelj (name server) je program koji sadrži potpune informacije o svim uređajima dijela neke domene. Područje koje pokriva naziva se **zona**. Jedan poslužitelj može pokrivati više zona. U cilju olakšavanja administriranja, DNS definira dva tipa domenskih poslužitelja - primarni i sekundarni. Primarni sadrži podatke o određenoj zoni, a sekundarni preuzima te podatke u fazi inicijalizacije i osvježava ih tijekom rada povremenim upitima primarnom domenskom poslužitelju. Podaci o uređajima nalaze se bazi podataka koja je u obliku tekstualne datoteke i njezin se sadržaj može mijenjati ručno, običnim uređivačem teksta. Jedan domenski poslužitelj može biti primarni za jednu ili više zona, a isto tako može biti sekundarni za jednu ili više zona. Također, jedan poslužitelj može biti primarni za jednu, a sekundarni za drugu zonu. Domenski poslužitelj odgovara na upite klijenta.

Klijent (resolver) je obično ugrađen u programe mrežnih usluga, npr. telneta i ftpa. On postavlja upite domenskom poslužitelju, interpretira primljene odgovore i rezultat (točan odgovor ili obavijest o pogrešci) vraća procesu koji ih je tražio.

Upiti se mogu postaviti rekurzivno ili iterativno. Kod rekurzivnih upita, domenski poslužitelj koji je primio upit, a nije nadležan za traženu zonu, postavlja upit nadređenom domenskom poslužitelju koji dalje, rekurzivno prosljeđuje upit dok ne dobije odgovor, kojeg vraća natrag poslužitelju koji mu je postavio upit. Kod iterativnih upita, svaki domenski poslužitelj odgovori informacijom koju trenutno posjeduje (u svojoj bazi ili privremenoj memoriji) i, ako nema traženu informaciju, odgovori kojeg se drugog domenskog poslužitelja može pitati, ali ispitivanja prepušta onom koji je postavio upit.

Domenski poslužitelj daje odgovor na upite o podacima koje posjeduje. Ako je upit izvan zone za koju je odgovoran, odgovor se saznaje pretraživanjem ostalog domenskog prostora. Taj proces naziva se **određivanje imena** (name resolution) ili samo određivanje (resolution). S obzirom da je domenski prostor organiziran kao obratno stablo, domenski poslužitelj može postaviti upit izravno korijenu stabla. Glavni domenski poslužitelj vrati odgovor o domenskom poslužitelju vršne domene, koji vrati odgovor o domenskom poslužitelju sekundarne poddomene, i tako sve do poslužitelja poddomene koji vrati odgovor o samom računalu.

Kako bi svi upiti korijenu stabla znatno opteretili glavni domenski poslužitelj svih vršnih domena, primjenjuju se tehnike njegovog rasterećenja. Postoji više od jednog korijenskog domenskog poslužitelja i raspoređeni su po različitim djelovima Internet mreže. Tu su još i pohrana u privremenu memoriju (caching), te kopiranje (mirroring) informacija domenskih poslužitelja.

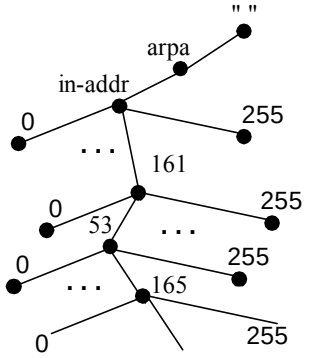
Privremeno pamćenje informacija drugih domenskih poslužitelja olakšava pronalaženje odgovora na upit klijenata. Domenski poslužitelji koji rade na principu rekurzivnih upita, u pronalaženju odgovora, informacije spremaju u svoju privremenu memoriju (cache). Na primjer, informaciju o tome koji je domenski poslužitelj odgovoran za koju zonu, te koje su njihove adrese. Također sprema i odgovor koji je pronašao. Time se ubrzava proces pri narednim upitima. Pri sljedećem upitu, domenski poslužitelj provjerava ima li odgovor u vlastitoj bazi podataka, ako ne, ima li u privremenoj memoriji, a tek onda pita druge domenske poslužitelje, s tim da možda točno zna koji je domenski poslužitelj odgovoran za traženu zonu.

Privremeno pohranjene informacije imaju određeno vrijeme života (TTL - time to live) nakon kojeg se podatak izbacuje iz privremene memorije i ponovno traži odgovor nadležnog domenskog poslužitelja. Na koliku će vrijednost to vrijeme biti postavljeno, ovisi o kompromisu zahtjeva za većom performancom sustava (dulji TTL), odnosno konzistentnošću podataka (kraći TTL).

Određivanje naziva uređaja na osnovu njegove IP adrese

Povezivanje IP adresa i naziva koristi se kako bi dobijeni odgovor bilo ljudima jednostavnije protumačiti (npr. u log datotekama, ili pri autorizaciji). U tablicama računala (host table), ispituju se reci tablice u potrazi za odgovarajućim zapisom, a u DNS-u bi to bio presložen i nepraktičan pristup. Puno je jednostavnije naći IP adresu uređaja na osnovu njegovog naziva, nego obratno.

U cilju pojednostavljenja potrage naziva uređaja na osnovu njegove IP adrese, napravljen je domenski adresni prostor **in-addr.arpa**, koji koristi adrese kao imena. Čvorovi u domeni in-addr.arpa nazvani su prema brojevima IP adresa, zapisanih kao četiri okteta međusobno odvojena točkama. Ta domena može imati do 256 vršnih domena, svaka nazvana po jednoj vrijednosti koju prvi oktet IP adrese može poprimiti. Svaka od domena može imati do 256 poddomena (sekundarnih domena) i tako sve do četvrte razine.



Slika 5.15. Struktura in-addr.arpa domene

Zapisana prema domeni, IP adresa se piše od najmanje značajnog okteta do najznačajnijeg, tj. prvo se piše broj računala, zatim poddomene, vršne domene i obvezni dio in-addr.arpa. Na primjer, IP adresa 161.53.165.145, u in-addr.arpa domeni je 145.165.53.161.in-addr.arpa.

5.3.11 SNMP - Simple Network Management Protocol

SNMP je protokol za izmjenu informacija o nadzoru i upravljanju mreže između nadzornih stanica i mrežnih elemenata. Temelji se na TCP/IP skupu protokola i opisan je u RFC 1157. Informacije o uređajima na mreži prikupljaju agenti - programi koji se izvršavaju na pojedinim uređajima, a pohranjuju se u bazu upravljačkih informacija (MIB - Management Information Base). Na osnovu tih podataka, mrežni nadzorni programi mogu uočiti i dijagnosticirati probleme na mreži. SNMP na prijenosnoj razini koristi UDP protokol.

5.3.12 Korisnički račun

Korisnički račun podrazumijeva korisničko ime, lozinku, te resurse sustava koji se korisniku daju na raspolaganje za rad na tom računalu. **Korisničko ime** je ime korisnika na sustavu. Jedinstveno je za svakog korisnika, a definira ga administrator sustava, najčešće na osnovu imena i prezimena korisnika ili nekih njegovih podataka. **Lozinka** je niz znakova koji svaki korisnik zasebno tajno definira i kojom sustavu potvrđuje svoj identitet. S ciljem zaštite tajnosti, lozinka se prilikom upisa ne vidi na ekranu.

Lozinka je prva razina zaštite korisnika i njegovih podataka na sustavu. Uz poznavanje tuđeg korisničkog imena i lozinke, korisnik se sustavu može lažno predstaviti, a za sve izvršene akcije odgovara korisnik čiji su identifikacijski podaci korišteni. Stoga se svim korisnicima preporuča podatke o svom korisničkom računu ne davati drugim korisnicima i posebno pažljivo odabrati lozinku. Pri izboru lozinke, ne treba koristiti podatke kao što su ime, prezime korisnika, njegove podatke koji postoje na samom sustavu, te opće poznate riječi ili pojmove iz govornog jezika. Preporuča se lozinka koje je kombinacija velikih i malih slova (za sustave kao što je UNIX koji ih razlikuju), brojeva i specijalnih znakova, takva da je korisnik može lako zapamtiti, a da drugima nije lako prepoznatljiva. Također, moguće je koristiti i jednokratne lozinke, koje vrijede samo za jedno prijavljivanje na sustav. Dobro odabrana lozinka sastavni je dio dobre zaštite vlastitog korisničkog računa, a time i vlastitih podataka na sustavu. Lozinku treba mijenjati, sukladno učestanosti korištenja korisničkog računa, te ovisno o zaštićenosti računala s kojih mu se pristupa.

5.3.13 Telnet

Telnet je protokol korisničke razine koji omogućava prijavu za rad na udaljeno računalo. Definira pravila za povezivanje korisnikove tipkovnice i ekrana na klijent sustavu s komandnim interpreterom na udaljenom poslužitelju. Osnovna svrha telnet protokola jest osigurati da poslužitelji i klijenti ne moraju čuvati informacije o terminalskim karakteristikama onog na drugom kraju veze.

Sastoji se iz tri cjeline - protokola za uspostavu veze (ICP - Initial Connection Protocol), definicije mrežnog virtualnog terminala (NVT - Network Virtual Terminal) i definicije kontrolnih signala koji se prenose skupa s podacima. Podaci se prenose 7-bitnim ASCII kodom, preko uspostavljene TCP veze. Telnet protokol koristi priključni broj usluge 23.

Opći oblik naredbe telnet je:

telnet [IP_address | host_name] [port]

IP adresa, ili naziv računala napisan iza naziva naredbe telnet označava udaljeno računalo kojem se želi pristupiti. Navođenjem priključnog broja usluge nakon naziva ili adrese računala, moguće je pristupiti određenoj usluzi, pri čemu se terminal koristi kao klijent za datu uslugu. To može biti praktično u slučaju kad korisnik nema odgovarajući klijent program, ili kad je to jedini način za pristup određenoj usluzi. Odjava s udaljenog računala obavlja se upisom naredbe logout ili exit, a korisnik može nastaviti rad na lokalnom sustavu.

Najčešće je pristup udaljenom računalu omogućen samo potvrđenim korisnicima, onima koji imaju otvoren korisnički račun na tom računalu. Međutim, postoje računala koja na određenom priključnom broju usluge pružaju neku javnu mrežnu uslugu za pristup kojoj od korisnika ne traže autorizaciju, ali su prava korisnika ograničena samo na pregled publiciranog sadržaja. Napuštanjem usluge, prekida se i rad korisnika na tom sustavu.

5.3.14 Adrese na Internetu

Adrese na Internetu imaju uređaji, korisnici i dokumenti, kako bi se bilo kome od njih moglo na jednoznačan način pristupiti. Uređajima se pristupa preko numeričkih IP adresa, ili FQDN naziva. Korisnicima se dodjeljuje elektronička adresa u prvom redu zbog jedne od najviše korištenih mrežnih usluga - elektroničke pošte. Dokumentima se pristupa preko njihove URL adrese koja je taj naziv dobila i od posebnog značaja postala tek s pojavom još jedne, možda najčešće korištene usluge - World Wide Weba.

Elektroničke adrese korisnika, tzv e-mail adrese, sastoje se iz dva dijela, oznake korisnika, te oznake računala na kojem taj korisnik ima svoj korisnički račun. Ta dva dijela odvajaju se znakom @ (Alt+64, ludo A, monkey, i sl):

username@host-name.subdomain.domain

Primjer jedne e-mail adrese je:

asd285@nippur.nets.net

korisničko ime u ovom primjeru je asd285, a naziv računala je nippur.nets.net.

Osim tako formiranih, osnovnih e-mail adresa, na svakom sustavu se vrlo često definiraju **simboličke adrese** (alias). Više je mogućih primjena simboličkih adresa:

- umjesto korisničkog imena uvesti oblik ime.prezime, jer je to jednostavnije za pamćenje
- umjesto naziva računala ostaviti samo oznaku mreže; kod promjene poslužitelja za elektroničku poštu, ne mijenja se e-mail adresa korisnika
- uvođenje simboličke adrese zajedničke za skupinu korisnika (npr. adresa studIIg za studente druge godine, a poruku poslanu na tu adresu dobili bi svi upisani studenti druge godine).

URL (Uniform Resource Locator) je adresa dokumenta na Internetu koja ima oblik:

protokol://poslužitelj/put-do-datoteke/datoteka.nastavak

Počinje oznakom protokola korisničke razine, a najčešće je to http (za prijenos WWW stranica), ftp (prijenos datoteka), news (mrežne novine). Obvezni dio "://" odvaja oznaku protokola od mjesta datoteke, koje počinje nazivom poslužitelja, slijedi (neobvezni) dio poddirektorija "put-do-datoteke" i dolazi se do samog naziva datoteke. Ako u adresi nema naziva datoteke, nego završava znakom /, učitava se podrazumijevana početna datoteka, koja je na većini sustava index.html ili index.htm. Nastavak u imenu datoteke definira tip same datoteke, odnosno koji program treba koristiti za ispravan prikaz datoteke. Iako se pojam URL adrese vezuje za World Wide Web, a Web preglednik može prikazati samo nekoliko tipova datoteka (slika .gif i .jpg formata, te dokumente pisane u HTML jeziku nastavaka .html ili .htm), sama primjena takvog adresiranja dokumenata nadilazi okvire WWW-a i koristi se i za bilo koje druge datoteke. Za pregled datoteka koje nisu namijenjene Web pregledniku koriste se dodatni programi koji moraju biti instalirani na računalu klijenta.

5.3.15 FTP - File Transport Protocol

FTP je protokol za prijenos datoteka, definiran u RFC 959. FTP protokol koristi dvije odvojene istovremene TCP veze, jednu za upravljanje (priključni broj usluge 21), a drugu za prijenos podataka (20). Za upravljačku vezu, FTP radi po specifikaciji telnet protokola. Upravljačka veza se koristi za prijenos naredbi i odgovora na naredbe. Podaci se prenose samo preko podatkovne veze. Pri prijenosu podataka mora se voditi računa o formatu podataka. Za prijenos tekstualnih podataka definira se ascii način prijenosa (podrazumijevan pri uspostavi veze), odnosno binarni - za prijenos binarnih podataka.

FTP omogućava prijenos podataka između dva računala, od kojih jedno može biti lokalna radna stanica na kojoj korisnik radi, a druga udaljeno računalo, ili se može raditi o dva udaljena računala. Također, prijenos datoteka korisnik može obavljati između dva računala na kojima ima svoj korisnički račun, na primjer u slučaju kad želi svoje datoteke prebaciti s jednog udaljenog računala na drugo.

Drugi način primjene FTP protokola je prijenos podataka s **javnih** (anonymous) **FTP poslužitelja**. Osnovna namjena javnih FTP poslužitelja jest datoteke koje posjeduje staviti na raspolaganje svim korisnicima koji mu žele pristupiti. Pri tome oni na javnom poslužitelju ne moraju imati otvoren korisnički račun, tj. svoje korisničko ime i lozinku. Kao korisničko ime koristi se "ftp" ili "anonymous", a kao lozinku korisnik upisuje svoju e-mail adresu. Prijavljen pod javnim korisničkim imenom, korisnik može pristupiti i preuzeti datoteke koje se nalaze u (hijerarhijski organiziranom) direktoriju pub, koji je uvijek poddirektorij osnovnog

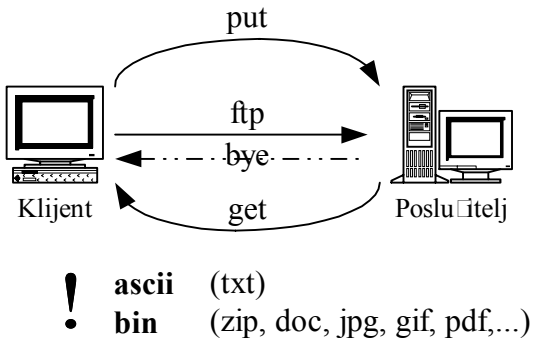
direktorija (root). Neki FTP poslužitelji dozvoljavaju korisniku ostavljanje svojih datoteka u direktoriju inbox (ili incoming, ili nekog sličnog naziva), ali to ne mora biti pravilo. Korisniku se ne dozvoljava pristup bilo kojem direktoriju osim dva navedena (pub i inbox/incoming).

Opći oblik naredbe za uspostavu FTP veze s udaljenim računalom je:

ftp [IP_address | host_name]

Korisnik će biti upitan za korisničku oznaku i lozinku (lozinka se neće vidjeti na ekranu prilikom upisa), a korisnik upisuje podatke o vlastitom ili o javnom korisničkom računu.

Ako se uz ftp ne navede ime računala ulazi se samo u program FTP, a veza s udaljenim računalom uspostavlja se naredbom "open host_name" ili "open IP_address", nakon čega slijedi proces autorizacije.



Slika 5.16. FTP

Prijenos jedne datoteke s lokalnog (s kojeg je pokrenuta naredba "ftp") na udaljeno računalo, obavlja se naredbom:

put local_file_name remote_file_name

pri čemu je potrebno odabrati određeni način prijenosa datoteke (ascii ili bin) ovisno o tipu. Prijenos više datoteka obavlja naredba mput, koja dozvoljava uporabu zamjenskih znakova (* i ?) za oznaku više od jedne datoteke i ne zahtjeva definiranje odredišne datoteke.

Prijenos datoteke s udaljenog računala na lokalno obavlja, uz isti zahtjev za definiranjem načina prijenosa, naredba:

get remote_file_name local_file_name

Analogno naredbi mput, postoji i naredba mget. Naredba "bye" ili "quit" prekida uspostavljenu FTP vezu.

Pasivni mod rada FTP poslužitelja

Prema FTP protokolu, kada klijent zatraži podatke od poslužitelja, poslužitelj otvara posebnu TCP vezu prema klijentu kojom se ti podaci prenose, dozvoljavajući samo jednu uspostavljenu podatkovnu vezu. Pri tome FTP klijent program javlja poslužitelju, naredbom PORT, priključni broj otvorene podatkovne veze. Takav način nije prikladan kad je neka mreža zaštićena vatrenim zidom temeljenim na filtriranju paketa, jer on načelno zabranjuje dolazne pozive na dinamički dodijeljene priključne brojeve.

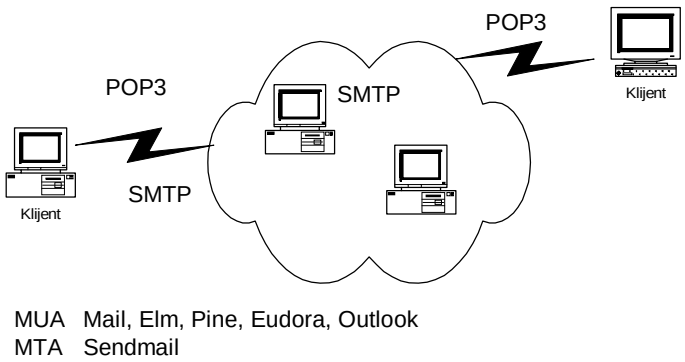
No, ako klijent koristi naredbu za uspostavu veze u pasivnom načinu rada (PASV), podatkovna veza koja se uspostavlja zapravo je odlazni poziv kroz vatreni zid i moguće ga je ostvariti. U tom slučaju, FTP klijent pošalje poziv poslužitelju koji otvara pasivnu TCP vezu na nekom dinamički dodijeljenom priključnom broju i taj priključni broj javi klijentu. Klijent tada otvara aktivnu vezu prema poslužitelju. Ako poslužitelj ne podržava naredbu PASV i pasivni način rada, klijent će dobiti poruku da poslužitelj ne razumije poslanu naredbu, što će mu biti indikacija da vezu treba zatražiti na standardni način. Pri tome se možda veza neće moći uspostaviti ako postoji vatreni zid.

5.3.16 Protokoli za razmjenu elektroničke pošte

Elektronička pošta jedna je od najčešće korištenih usluga na Internetu. Svaka strana u komunikaciji mora imati svoju elektroničku (e-mail) adresu. Suvremeni programi za razmjenu elektroničke pošte omogućavaju prijenos tekstualne poruke, kao i priključivanje datoteka osnovnoj poruci, bez obzira na njihov format ili program kojim su generirane. Na taj način, elektronička pošta kao mrežna usluga donekle integrira uslugu prijenosa datoteka - ftp.

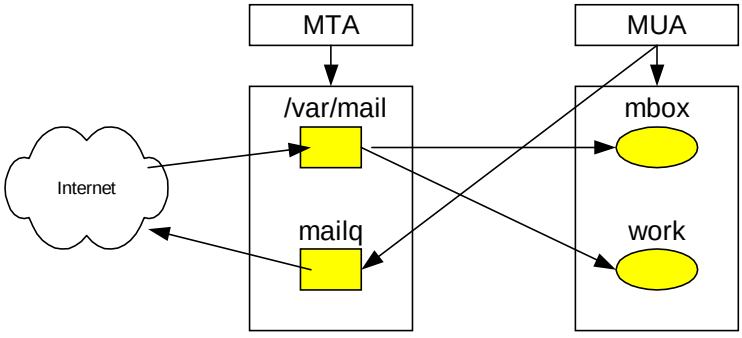
I usluga elektroničke pošte temeljena je na modelu klijent - poslužitelj. Poslužitelj elektroničke pošte zadužen je za prijem i prihvat pošte upućene nekom korisniku i za svakog svog korisnika formira poštanski pretinac gdje sprema njegovu dolaznu poštu. Osim toga, uloga poslužitelja je otpremiti poštu koju šalju korisnici na njegovom sustavu. Programi odgovorni za rad sustava elektroničke pošte nazivaju se MTA (Message Transfer Agents).

Uloga klijent programa instaliranih na računalima korisnika jest s poslužitelja dohvatiti poštu (ako je ima), sadržaj poruka prezentirati na ekranu korisnika, te omogućiti korisniku slanje poruka. Programi za sastavljanje, slanje i prijem elektroničke pošte označavaju se kao MUA (Message User Agents).



Slika 5.17. Model sustava elektroničke pošte

U razmjeni elektroničke pošte, ključnu ulogu igraju poštanski pretinci. Postoje pretinci koje koristi poslužitelj i oni koje koristi klijent. Slika 5.18. ilustrira pretince na UNIX sustavu: dolazni pretinac poslužitelja je /var/mail gdje za svakog korisnika postoji zasebna datoteka - koja predstavlja korisnikov dolazni pretinac, a odlazni pretinac je mailq (red čekanja). Pročitanu poštu korisnik premješta iz dolaznog pretinca na sustavu u pretinac svom direktoriju, označen na slici kao work.



Slika 5.18. Poštanski pretinac

Za razmjenu elektroničke pošte trenutno se koriste protokoli: POP3 (Post-Office Protocol, version3), SMTP (Simple Mail Transfer Protocol), te IMAP (Internet Message Access Protocol). Standardni priključni broj usluge elektroničke pošte je 25.

POP3 - Post-Office Protocol

POP3 protokol, opisan u dokumentu RFC 1939, omogućava klijentovom računalu pristup poslužitelju elektroničke pošte i preuzimanje pošte iz dolaznog pretinca korisnika. Ovisno o konfiguraciji klijent programa, sadržaj dolaznog pretinca korisnika se kopira (ostavljajući sadržaj i na poslužitelju) ili se, nakon

preuzimanja, briše. POP3 ne omogućava nikakve intervencije na poslužitelju, nego jedino dohvat pošte. Podatkovna veza ostvaruje se preko TCP protokola na prijenosnoj razini. Prilikom pristupa poslužitelju, korisnik svojim korisničkim imenom i lozinkom potvrđuje svoj identitet.

SMTP - Simple Mail Transfer Protocol

SMTP protokol osigurava pouzdan i efikasan prijenos elektroničke pošte između pošiljatelja i primatelja. Pošiljatelj i primatelj su krajnji korisnici - klijenti, a stvarno slanje pošte umjesto pošiljatelja obavlja poslužitelj (SMTP pošiljatelj), preko prijenosnih sustava na putu do odredišnog poslužitelja (SMTP primatelja) koji poštu prosljeđuje primatelju. Pojam "prijenosni sustav" može obuhvaćati dio jedne mreže, cijelu mrežu ili više mreža, pa pojam prijenosnog sustava i mreže ne treba poistovjećivati ni izjednačavati. Kao posebnu prednost, SMTP protokol ističe mogućnost prijenosa elektroničke pošte neovisno o prijenosnim sustavima na putu do odredišta. Zahtjeva jedino pouzdanu vezu za prijenos podataka.

Kao rezultat zahtjeva korisnika, SMTP pošiljatelj uspostavlja dvosmjerni prijenosni kanal do SMTP prijemnika. koji može biti posrednik ili krajnje odredište. SMTP pošiljatelj šalje naredbe primatelju, a on na njih odgovara.

Kad je jednom uspostavljen prijenosni kanal, SMTP pošiljatelj šalje naredbu MAIL, kojom definira pošiljatelja poruke. Ako SMTP prijemnik može primiti poruku, odgovara porukom OK. SMTP pošiljatelj zatim šalje RCPT naredbu kojom definira primatelja poruke. Ako SMTP primatelj može primiti poruku za tog korisnika odgovara s OK, a ako ne može javi da odbija prijem poruke za tog primatelja, ali ne i cijelu mail transakciju. Ista poruka može biti poslana za više primatelja. Kad su definirani primatelji poruka, SMTP pošiljatelj šalje podatke koji završavaju posebnom sekvencom. Ako SMTP primatelj uspješno obradi sve podatke odgovara s OK.

SMTP uspješno šalje poštu od pošiljatelja do primatelja, bez obzira jesu li njihova računala provezana na isti prijenosni sustav, ili je podatke potrebno prosljeđivati preko jednog ili više SMTP poslužitelja, jer izvorišni i odredišni poslužitelj nisu spojeni na isti prijenosni sustav. SMTP poslužitelj koji obavlja prosljeđivanje mora znati nazive odredišnog računala i odredišnog poštanskog pretinca.

Kad se ista poruka šalje većem broju primatelja, prema SMTP protokolu, prenosi se samo jedna kopija podataka za sve primatelje na istom odredišnom računalu.

IMAP - Internet Message Access Protocol

IMAPv4 je protokol za pristup porukama elektroničke pošte na poslužitelju. Korisniku omogućava uvid u poštanski pretinac na udaljenom računalu kao da je lokalni i pri tom mu omogućava brisanje poruka i pretinaca, kreiranje novih ili preimenovanje pretinaca, pretraživanje poruka, te provjerava novopristiglu poštu. Porukama pristupa preko brojeva, dodijeljenih slijedno od prve poruke u pretincu ili kao jedinstveni identifikatori poruka. Ne omogućava slanje pošte, već tu funkciju za njega obavlja neki drugi protokol za prijenos elektroničke pošte, na primjer SMTP. Podrazumijeva pouzdani prijenos podataka, pa na prijenosnoj razini koristi TCP protokol, s priključnim brojem usluge 143.

IMAP podržava samo jedan poslužitelj, ali se ispituju mogućnosti podrške za više poslužitelja.

Temelji se na modelu klijent-poslužitelj i na njihovoj međusobnoj interakciji. Klijent i poslužitelj razmjenjuju naredbe u tekstualnom obliku, poslužitelj šalje podatke klijentu i obavijest o završetku prijenosa. Poslužitelj promptno izvještava klijenta čim se dogodi neka promjena s dolaznim poštanskim pretincem. Na poslužitelju može biti postavljeno vrijeme neaktivnosti nakon koje on prekida vezu s klijentom. Prema protokolu, to vrijeme mora biti najmanje 30 minuta, a bilo koja naredba od klijenta prema poslužitelju u tom intervalu inicira ponovni početak odbrojavanja.

Korisnik se treba predstaviti poslužitelju upisom svog korisničkog imena i lozinke. IMAP dozvoljava konfiguraciju na poslužitelju po kojoj za pristup nekim pretincima korisnik ne bi morao imati vlastito korisničko ime nego bi mogao koristiti javno - "anonymous", uz određenu lozinku. Ograničenja pristupa i izbor lozinke se mogu posebno definirati.

Usporedba protokola za razmjenu elektroničke pošte

SMTP je jedini od tri navedena protokola koji omogućava prijenos poruka elektroničke pošte od pošiljatelja do primatelja i tu njegovu sposobnost koriste IMAP i POP3 protokoli. Međutim, SMTP protokol je nesiguran na lokalnoj razini zbog mogućnosti slanja poruka pod tuđim imenom. Stoga se na lokalnoj razini najčešće koriste IMAP i POP3, a SMTP samo posredno.

5.3.17 HTTP - HyperText Transfer Protocol

HTTP je protokol korisničke razine koji omogućava prijenos datoteka koje u sebi sadrže veze na druge dokumente. Takvi dokumenti označavaju se kao hipertekst, a za veze koje sadrže kaže se da su hipertekstualne veze. Primjenjuje se od 1990. godine s pojavom mrežne usluge WWW - World Wide Web. HTTP 1.0 verzija protokola opisana je u dokumentu RFC 1945, a HTTP 1.1 u RFC 2068.

Temelji se na modelu klijent - poslužitelj, a za prijenos podataka zahtijeva pouzdanu vezu na prijenosnoj razini, s tim što se ne vezuje uz određeni protokol, već dozvoljava u budućim primjenama i neki drugi protokol osim TCP-a. Izvorno je definirano da je priključni broj 80, ali nije strogo vezan za taj broj.

HTTP 1.0 protokol definira otvaranje odvojenih TCP veza za prijenos svakog dokumenta. Na primjer, HTML dokument koji poziva dvije slike unutar stranice izazvat će otvaranje dvije nove TCP veze od klijenta prema poslužitelju. Prema HTTP 1.1. između klijenta i poslužitelja otvara se stalna HTTP veza, koja se koristi za razmjenu podataka više zahtjeva između klijenta i poslužitelja preko jedne uspostavljene veze. Na taj način, štedi se procesorsko vrijeme, smanjuje dodatni promet i umanjuje mogućnost pojave zagušenja.

HTTP protokolom definira se, između ostalog, i:

1. forma komunikacije između klijenta i poslužitelja, tj. format (način) postavljanja upita i odgovora
2. način prijenosa raznih tipova znakova karakterističnih za brojne jezike u svijetu (character set)
3. označavanje sadržaja (content coding)
4. pristup dokumentima za različite tipove protokola
5. pristup dokumentima uz provjeru identiteta (autorizacija i autentifikacija)
6. pohrana dokumenata u privremenu memoriju (caching)
7. sigurnosne aspekte - osjetljive točke u komunikaciji između klijenta i poslužitelja, odnosno, u procesu dostave podataka do korisnika:

5.3.17.1 Klijent-poslužitelj model HTTP protokola

HTTP poslužitelj prima zahtjeve klijenata za dokumentima koje posjeduje. Svaki dokument kojim poslužitelj raspolaže opisan je s nekoliko parametara - identifikator (URI - Uniform Resource Identifier), adresa (URL - Uniform Resource Locator) i naziv (URN - Uniform Resource Name). Na osnovu njih poslužitelj odlučuje na koji će način odgovoriti na postavljeni zahtjev.

Zahtjev klijenta sadrži naredbu koja definira željenu akciju klijenta (GET, POST, DELETE,...), adresu dokumenta, verziju HTTP protokola, te odgovarajuća zaglavlja kroz kojih su definirani parametri klijenta. Odgovor poslužitelja na zahtjev sastoji se najprije u odluci hoće li prihvatiti komunikaciju s klijentom i uspostaviti vezu ili ne. U slučaju pozitivne odluke na zahtjev za podacima (GET), poslužitelj šalje odgovor klijentu koji se sastoji od zaglavlja i podataka. Zaglavlje prethodi informaciji namjenjenoj korisniku, a sadrži parametre o samom poslužitelju, o podacima i klijentu. Primljene podatke klijent prihvaća, izdvaja informaciju namijenjene korisniku i prezentira mu ih.

Umjesto podataka, klijent može dobiti obavijest o pogrešci, kojoj uzrok može biti na strani klijenta ili poslužitelja. Najčešće poruke o pogrešci su "Datoteka nije pronađena" (File not found -404) ili "Pristup dokumentu nije dozvoljen" (Forbidden - 403).

5.3.17.2 Kodiranje znakova (Character Set)

HTTP koristi MIME definiciju skupa znakova i omogućava, definiranjem skupa znakova primjenjenog u dokumentu, razmjenu dokumenata znakovlja različitih svjetskih jezika. Kodiranje znakova se primjenjuje kako bi se slijed okteta mogao ispravno protumačiti kao slijed znakova. Oznake skupova znakova definira IANA. Ako nije navedena oznaka za tip znakova, podrazumijeva se ISO-8859-1. Znakovlje hrvatskog jezika definirano je kao ISO-8859-2.

5.3.17.3 Označavanje sadržaja (Content Codings)

Označavanjem sadržaja, HTTP protokol omogućava ukazivanje na transformaciju primjenjenu nad podacima, kao što je komprimiranje (compress, zip), ili kriptiranje. Time se postiže opis sadržaja koji nije čisti ascii tekst, na primjer datoteka generiranih nekim od programa za osobna računala (doc, ppt, xls, vsd...).

5.3.17.4 Prijenos podataka različitih protokola

HTTP protokol omogućava komunikaciju između drugih protokola, kao što su SMTP (razmjena elektroničke pošte), NNTP (mrežne novine), FTP (prijenos datoteka) i drugi. Na taj način je omogućen dostup najčešće korištenim mrežnim uslugama uporabom samo jednog korisničkog programa - Web preglednika. U slučaju kad se HTTP protokolom prenose informacije drugih protokola, primjenjuje se ili postupak tuneliranja (gdje se informacije prosljeđuju, bez analize o kojem se protokolu radi), ili postupak prevođenja kojeg obavljaju poveznici (gateway). U takvim slučajevima, veza između klijenta i poslužitelja odvija se preko posrednika.

Posrednik može biti i proxy poslužitelj, čija je uloga u rasterećenju prometa od poslužitelja na lokalnom sustavu prema ostatku Interneta. Klijent postavlja zahtjev proxy poslužitelju koji provjerava sadrži li traženu informaciju u svojoj privremenoj memoriji (cache) i, ako je pronađe vraća je vraća natrag klijentu. Ako nema traženu informaciju, postavlja upit poslužitelju, umjesto samog klijenta. Odgovor poslužitelja prosljeđuje korisniku koji je postavio zahtjev, ali ga i pohranjuje u svoju privremenu memoriju, kako bi pri sljedećem upitu postigao brži odziv.

Protokol za pristup do dokumenta, poslužitelj, kao i mjesto dokumenta na poslužitelju definira jedinstvena adresa dokumenta - URL.

5.3.17.5 Autorizirani pristup

HTTP protokol omogućava postavljanje dozvola pristupa dokumentima isključivo skupini autoriziranih korisnika, kojima je definirano korisničko ime (user-ID) i lozinka (password). Pri tome je moguće pristup ograničiti samo na određena računala. Prilikom postavljanja zahtjeva putem HTTP klijenta, korisnik će biti upitan za korisničko ime i lozinku, nakon čega slijedi provjera unijetih podataka. U slučaju ispravno unijetih podataka korisnik dobija tražene informacije, a u slučaju netočnih podataka obavijest o pogrešci. Kako se korisničko ime i lozinka definiraju na Web poslužitelju, ne treba ih miješati s korisničkim oznakama na računalima s višekorisničkim operacijskim sustavima, kakvi se primjenjuju za protokole telnet i ftp.

Kako na putu između poslužitelja i klijenta informacije prolaze kroz proxy poslužitelje, proxy poslužitelji moraju biti tako konfigurirani da ne pohranjuju informacije koje se razmjenjuju u procesu provjere identiteta korisnika, nego da te podatke prosljeđuju nepromjenjene.

5.3.17.6 Pohrana u privremenu memoriju

HTTP protokol koristi se za dohvat informacija s distribuiranih mrežnih informacijskih sustava, pa je moguće povećati učinkovitost i ubrzati sveukupni rad pohranom već dohvaćenih podataka u privremenu memoriju koja je na raspolaganju HTTP poslužitelju. Privremena memorija organizira se lokalno i na razini podmreže (proxy). Pretraživanje privremene memorije i dohvat informacija obavlja se prvo na lokalnom računalu, a zatim na proxy poslužitelju.

Kada klijent postavi zahtjev za nekim dokumentom, provjerava se postoji li već ta datoteka u privremenoj memoriji. Ako postoji dostavlja se klijentu, a kako je pretraživan lokalni ili mrežni diskovni prostor, odziv bi trebao biti brz. Pri tome se nije opterećivala veza prema udaljenom poslužitelju. Ako podatak ne postoji, zahtjev se upućuje poslužitelju naznačenom u URL adresi, a pristigli odgovor pohrani se u privremenu memoriju i dostavi klijentu.

Vrijeme zadržavanja informacije u privremenoj memoriji može ovisiti o veličini privremene memorije, jer se, u slučaju kad je potrebno spremiti neki dokument u popunjenu privremenu memoriju, dokument zapisuje preko postojećeg sadržaja. Uz to, u zaglavlju svakog dokumenta može se postaviti vrijeme nakon kojeg podatak više ne bi trebalo čuvati u privremenoj memoriji (polje "Expire"). Na taj način se, implicitno, definira ažurnost informacije. To je od posebnog značaja za stranice dinamički generiranog sadržaja, na primjer nastale kao rezultat pretrage baze podataka, ili rezultat neke obrade na poslužitelju.

5.3.17.7 Sigurnosni aspekti HTTP protokola

Razmjena informacija između poslužitelja i klijenta obavlja se uz moguće posredovanje drugih poslužitelja, što samu komunikaciju čini nesigurnom. Uloga administratora sustava jest zaštiti podatke koje posjeduje ili koje šalje korisnik sustava kojeg štiti. Jedna od osnovnih zaštita vlastitih podataka jest postavljanjem prava pristupa - dozvolom pristupa raspoloživim podacima, a zabrana pristupa svim ostalim. Drugi oblik zaštite jest pristup uz autorizaciju, pri čemu osnovni oblik razmjene korisnikovih identifikacijskih podataka ne

pruža dovoljnu zaštitu jer se prenosi kao čisti tekst, ali sam HTTP protokol ostavlja mogućnost uvođenja drugih tehnika autorizacije. Također, korisnicima se preporuča oprez pri definiranju vlastitih podataka kroz zaglavlja HTTP protokola, kao i pri prijenosu osjetljivih podataka. Dodatne sigurnosne mjere definira Secure HyperText Transfer Protocol - SHTTP, opisan u RFC 2660.

5.3.18 HTTP, WWW i HTML

HTTP je osnovni protokol za prijenos WWW stranica pisanih u HTML jeziku. WWW je oznaka za World Wide Web, a kao distribuirani, multimedijalni, mrežni, informacijski servis, temeljen na načelu hiperteksta, trenutno predstavlja najviše korištenu uslugu Interneta. Distribuiranost Web poslužitelja po svijetu omogućava raspodjelu zahtjeva klijenata, čime se postiže znatno rasterećenje i brži odziv nego da se radi o samo jednom poslužitelju. Naziv "multimedijalni" potječe od činjenice da se putem HTTP protokola mogu prenositi svi tipovi i formati podataka, a upravo mogućnost prijenosa slika, zvučnih, audio i video zapisa učinila je ovu uslugu dominantnom u razmjeni informacija svijetom danas.

WWW stranice pisane su HTML jezikom, što je kratica od HyperText Markup Language. HTML jezik primjenom kontrolnih oznaka (tag) oblikuje tekst koji će se pojaviti na ekranu korisnika, definirajući tip, veličinu i boju slova, mjesto teksta na stranici, te omogućavajući osnovno oblikovanje dokumenta. HTML dokumenti zapravo su čisti tekst, pa se za generiranje i pregled izvornog HTML dokumenta (HTML Source) može koristiti bilo koji uređivač teksta. Polja zaglavlja HTTP protokola definiraju se u okviru zaglavlja HTML dokumenta, unutar META kontrolne oznake (tag). Nastavak HTML datoteka je .html ili .htm. Slike se, unutar HTML stranica, uključuju postavljanjem kontrolne oznake IMG kojoj se kao argument navodi relativna ili apsolutna (URL) adresa slike koja mora biti u .jpg ili .gif formatu. Za sve ostale formate (koji nisu .html, .jpg ili .gif), Web preglednici omogućavaju aktiviranje korisničkog programa. Danas s instalacijom Web preglednika korisnik može dobiti najčešće korištene aplikacije za pregled multimedijalnog sadržaja, pod uvjetom da su besplatne.

Svojstvo WWW-a je interaktivnost korisnika-klijenta i poslužitelja, što je omogućeno dodatnim svojstvima i obradama na strani poslužitelja ili na strani klijenta. Dodatne mogućnosti u prikazu HTML dokumenata obradama klijentovog Web preglednika omogućavaju: Dinamički HTML, ActiveX kontrole, Java i JavaScript. S druge strane, uz ASP (Active Server Pages), CGI (Common Gateway Interface) i SSI (Server Side Includes), pri svakom postavljenom zahtjevu na strani Web poslužitelja dinamički se generira Web stranica.

Dinamički HTML je kombinacija HTML jezika, stilskih predložaka (CSS - Cascading Style Sheets) i komandnih datoteka koje omogućavaju uvođenje animacije u dokument.

Java applet je kôd pisan u Java jeziku, koji putuje mrežom skupa sa stranicom, a izvršava ga preglednik, ako je u HTML stranicu ugrađena odgovarajuća kontrolna oznaka.

JavaScript su programi ugrađeni unutar HTML stranice koje izvršava preglednik dok se stranica prikazuje.

Active Server Pages (ASP) je tehnologija koja se koristi za izradu dinamičkih Web stranica, a zahtjeva dodatnu aktivnost Web poslužitelja. Razvio ju je Microsoft.

Common Gateway Interface (CGI) je standardni način za pristup dokumentima koje dinamički generira Web poslužitelj, primjenom procedura definiranih cgi komandnim datotekama nad postojećim dokumentima.

Kolačići (Cookies) su male količine podataka koje generira poslužitelj, a pohranjuje Web preglednik, koje sadrže informacije o Web poslužitelju kojem je korisnik pristupio. Kad korisnik postavi zahtjev, Web preglednik provjerava ma li sačuvan kolačić tog Web poslužitelja i, ako ima, šalje ga skupa sa zahtjevom.

Server Side Includes (SSI) omogućava dinamičko uključivanje sadržaja u Web stranicu. Uključeni sadržaj mogu biti datoteke (npr. na vrhu ili na dnu stranice), informacije koje poslužitelj generira automatski (npr. današnji datum, datum posljednje promjene, datum kad se radi na dokumentu) ili izlazne podatke za CGI program (npr. broj pogodaka).

Većina ovih tehnika koje omogućuju interaktivnost korisnika s poslužiteljem putem svog klijent programa, primjenjuju se za pristup bazama podataka, postavljajući upite na osnovu kojih se obavlja pretraživanje, generiranje podataka kao rezultat obrada na poslužitelju i prezentacija podataka korisniku. Uz odgovarajuće dozvole, korisniku je omogućen pristup bazi, mijenjanje ili brisanje (DELETE naredba HTTP protokola) postojećih zapisa, te dodavanje novih (PUT, POST).

6 UPRAVLJANJE RAČUNALNIM MREŽAMA

6.1 UVOD

Pretpostavlja se da je izvedeno ožičenje (kabliranje) lokalne mreže zgrade (ustanove, tvrtke,...) prema potrebama naručitelja, što je napravljeno s obzirom na broj potrebnih/raspoloživih radnih mjesta, ili sukladno raspoloživoj radnoj površini. Podrazumijeva se da će lokalna mreža biti temeljena na TCP/IP skupu protokola, i vjerojatno spojena na Internet.

Prije povezivanja uređaja, potrebno je, na osnovu projekta, napraviti plan povezivanja i definirati razdiobu raspoloživih IP adresa dodijeljene skupine adresa (mrežne klase ili dijela mrežne klase). Dio adresa treba odvojiti za spajanje glavnih poslužitelja i opreme za komunikaciju. Preostale adrese treba organizirati ovisno o ustroju ustanove čija je mreža. Preporuča se podjela adresa na blokove koji se, u slučaju potrebe, mogu objediniti nekom mrežnom maskom. Kolika će biti veličina bloka ovisi o broju i veličini ustanovljenih (radnih) grupa. Pri podjeli na grupe, uvijek treba predvidjeti širenje radnih grupa povećanjem broja uređaja.

Sljedeći zadatak je spojiti u lokalnu mrežu računala i drugu mrežnu opremu tako da zadovoljava funkcionalne i praktične zahtjeve korisnika, s posebnim naglaskom na formiranje radnih grupa, ovisno o unutarnjoj organizaciji i potrebama za suradnjom. Pri tome se moraju poštivati pravila i zahtjevi strukturnog kabliranja i funkcionalnog rada mreže sukladno primjenjenom protokolu (skupu protokola).

Konfiguracijom poslužitelja, te otvaranjem korisničkih računa, lokalna mreža postaje funkcionalna, a mrežne usluge postaju dostupne korisnicima u njihovom svakodnevnom radu.

6.2 ORGANIZACIJA LOKALNE MREŽE

Ako se nakon isprojektirane mreže pojavi potreba za većim brojem računala od planiranog, više računala može se povezati zvjezdištem (hub). Broj računala ovisi o broju ulaza (port), a obično je to 4, 8, 12, 16,...

Jednostavna zvjezdišta najčešće ne zahtijevaju nikakvu konfiguraciju. Postaju funkcionalni samim spajanjem u mrežnu utičnicu i napajanje. Zvjezdišta i pojačala, za koja također nije potrebno konfiguriranje, čine mrežnu opremu na fizičkoj razini i povezuju djelove mreže jedne zone kolizije.

6.2.1 Spajanje računala u mrežu

Uključivanje računala u mrežu zahtjeva dodatni vezni sklop, te promjenu konfiguracije programske podrške. Računalo može biti priključeno na mrežu, jedino ako posjeduje mrežnu karticu (NIC - network interface card). Mrežna kartica se ugrađuje u računalo, a ima svoju jedinstvenu MAC adresu. Može imati priključak za UTP konektor mrežnog kabela i/ili za BNC konektor. Ako ima oba konektora, označava se kao COMBO. S obzirom da se današnje mreže uglavnom grade prema kategoriji 5 strukturnog kabliranja koje zahtjeva UTP konektore, najčešće nije potrebno imati oba priključka na mrežnoj kartici, no to ne mora biti pravilo. Na odabir mrežne kartice može, ali ne mora, utjecati postojanje i način izrade lokalne mreže.

NICu treba podesiti:

- prekidni broj (interrupt number)
- memorijsku adresu (I/O address)

Najčešće se to podesi automatski (pogotovo kod novih operacijskih sustava), a tamo gdje to nije tako, parametre treba odabrati na osnovu slobodnih vrijednosti. U tome mogu pomoći odgovarajući dijagnostički programi za mrežne kartice koji se isporučuju s driverima.

Operacijski sustav mora imati podršku za protokol ili skup protokola na kojem se temelji mreža. Za mreže tipa Interneta, mora postojati podrška za TCP/IP skup protokola. Tim skupom protokola danas raspolaže većina operacijskih sustava. Za one koji ne raspolažu mrežnom programskom podrškom, postoje dodatni programi čijom se instalacijom omogućava povezivanje na mrežu. Način definiranja potrebnih parametara, preko grafičkog sučelja ili upisom u tekstualne datoteke, ovisi isključivo o tipu operacijskog sustava.

Parametri koji se upisuju kod konfiguracije računala na mrežu tipa Interneta su:

- IP adresa
- mrežna maska
- adresa uređaja koji obavlja prosljeđivanje (default gateway)
- DNS - FQDN, te primarni DNS poslužitelj (ili više njih)

Pod Windows operacijskim sustavom sve to postavlja se na jednom mjestu (Control Panel - Networks, ili nešto slično), a na UNIX sustavima je to nekoliko datoteka koje treba editirati i upisati odgovarajuće vrijednosti čiji naziv i mjesto u datotečnom sustavu ovise o tipu i verziji operacijskog sustava.

Spajanje računala na mrežu obavljeno je kad je računalu konfigurirana mrežna kartica i upisani odgovarajući parametri - adresa i naziv koji moraju biti jedinstveni za svako računalo, zatim spojen kabel između mrežne kartice računala i utičnice na zidu ili priključka na zvjezdištu, te kad je odgovarajući kabelski završetak na prespojnom panelu povezan s priključkom aktivne mrežne opreme.

Dodavanje bilo kojeg uređaja u lokalnu mrežu mora se dokumentirati, kako bi u svakom postojao uvid u trenutno stanje mreže, raspoložive resurse, moguće nedostatke, dakle bitno je kako za održavanje postojeće mreže tako i za planiranje i nadogradnju mreže. Također, od ogromnog je značaja u slučaju promjena u administriranju mreže, bez obzira radi li se o promjeni opreme, radnih grupa ili angažiranog osoblja.

Dokumentacija o uređaju dodanom na mrežu treba sadržavati podatke kao što su: fizička lokacija utičnice gdje je uređaj spojen (oznaka prostorije), oznaka utičnice koja mora biti u paru s oznakom na prespojnom panelu, broj priključnice na mrežnoj opremi (zvjezdištu, prospojniku), dodijeljena IP adresa, te dodijeljeni FQDN naziv. Poželjno je dokumentaciju uređaja voditi prema obrascu u Dodatku A.

6.2.2 Premosnici i prospojnici

Premosnici (bridge) i prospojnici (switch) rade na podatkovnoj razini, a primjenjuju se kad je potrebno povezati dva ili više segmenata mreže različitih zona kolizije. Prospojnici omogućavaju i formiranje virtualnih lokalnih mreža koje posebnu ulogu imaju u formiranju i povezivanju radnih grupa.

Premosnici povezuju dva segmenta mreže izravno uporabom jednog premosnika, ili preko nekog kanala primjenom dva premosnika i pri tom nema ograničenja kašnjenja, a povezani segmenti čine dvije različite zone kolizije. Premosnici mogu prosljeđivati datagrame namjenjene samo jednom odredištu (unicast), ili namjenjene većem broju računala (broadcast, multicast). Kad se spoji na mrežu, premosnik provjerava MAC adresu okvira koji kroz njega prolaze kako bi definirao tablicu poznatih odredišta. Ako premosnik zna da je odredište okvira na drugom segmentu mreže, premosnik prosljeđuje okvir samo tom segmentu. Ako premosnik ne zna odredišni segment, ili se radi o okviru univerzalne adrese odredišta (broadcast), okvir se prosljeđuje svim segmentima osim izvorišnog. Ovakva tehnika prosljeđivanja okvira naziva se metoda poplave (flooding).

Učinkovitije rješenje za prosljeđivanje okvira s univerzalnom adresom odredišta od metode poplave jest tehnika razapinjućeg stabla (spanning tree) koju koriste IEEE-802 MAC premosnici. U cilju izbjegavanja petlji, od postojećih se čvorova označava stablo u kojem se za neke grane označi da pripadaju stablu, a za druge ne. Skup odabranih grana čini graf bez petlje ili stablo; prostire se na sve čvorove u mreži i odatle potječe naziv "razapinjuće stablo". Kad je razapinjuće stablo jednom formirano, okviri se jednostavno prosljeđuju na način da čvor koji primi okvir prosljeđuje isti odlaznim granama koje su dio stabla, s iznimkom dolazne grane. Kako stablo nema petlje, okviri se sigurno neće ponovno pojaviti u istom čvoru, a stići će na sva odredišta. Razapinjuće stablo uspostavlja se pri inicijalizaciji mreže označavajući jedan čvor kao glavni i on postaje privremeno centar mreže, te označavajući zatim sve grane koje su na najkraćem putu do nekog drugog premosnika i tog centralnog čvora. Osnovna korist primjene premosnika jest ograničavanje prometa na pojedine segmente mreže. Ne zahtjevaju konfiguraciju ni upravljanje, već rade automatski.

Prospojnici povezuju više segmenata lokalne mreže od kojih je svaki posebna zona kolizije. Pri određivanju kojem segmentu treba proslijediti okvire koriste tablicu MAC adresa - Source Address Table (SAT). Prospojnici imaju i dodatne mogućnosti kao što je formiranje virtualnih LANova od segmenata mreže. Na drugoj razini, protokoli premošćavanja su IEEE 802.10 i ISL (Inter Switch Link) i definiraju postojanje virtualnih lokalnih mreža ili VLANova različite mrežne opreme uključujući i LAN prospojnike.

Modificirana verzija postojećeg IEEE 802.10 protokola (802.10 Security Protocol) definira prospajanje kroz FDDI (Fiber Distributed Data Interface) okosnicu. Svakoj virtualnoj lokalnoj mreži dodijeli se jedinstveni broj (identifikacijski broj, VLAN ID) veličine 32 bita (4 okteta). Prema 802.10 protokolu, svakom se okviru dodaje zaglavlje koje u sebi sadrži VLAN ID, a prosljeđuje se samo onom mrežnom uređaju (prospojniku ili usmjerniku) koji povezuje segment istog identifikacijskog broja VLANa.

ISL protokol svakom okviru dodaje svoje zaglavlje veličine 30 okteta u kojem je sadržan identifikacijski broj VLANa (VLAN ID) veličine 10 bita. Okvir se prosljeđuje jedino onom VLANu čiji je broj odgovara broju u zaglavlju. ISL protokol primjenjuje se na Fast Ethernet okosnicama.

6.2.3 Korisnici i korisnički računi

Za mrežni sustav korisnik može biti fizička osoba, grupa osoba, računarski sustav, ili to može biti oznaka za neku funkciju sustava koja koristi neke, ili sve mogućnosti koje sustav pruža (posjedovanje ili razmjenu datoteka, korištenje mrežnih resursa, servisa i usluga, te izvršavanje programa). Korisnikom se tako može smatrati neka druga mreža računala koja sa promatranim sustavom jedino razmjenjuje datoteke (poruke, podatke, programe), zatim, grupa osoba koja koristi iste podatke ili iste izvore podataka (npr. istraživačka ili radna grupa), ili to može biti oznaka za posebnu skupinu sistemskih ili izvršnih datoteka koje postoje jedino kao vlasnici tih datoteka (npr. korisnik sys je vlasnik datoteka kojima se definiraju parametri sustava, a korisnik adm datoteka vezanih uz korisničke račune) i ne koriste druge mogućnosti mreže. Međutim, korisnik je najčešće stvarna osoba koja koristi mrežu na više načina: može se prijaviti za rad na sustavu, raspolagati svojim i dostupnim tuđim datotekama i direktorijima, te koristiti brojne mrežne usluge lokalne ili neke druge mreže.

Korisnik je na sustavu prikazan preko korisničkog računa koji sadrži osnovne podatke o korisniku i prati njegove aktivnosti. Osnovni podaci koji korisnika čine prepoznatljivim sustavu i ostalim korisnicima su: korisničko ime, identifikacijski broj korisnika UID, identifikacijski broj grupe GID i lozinka. Korisničko ime definira administrator sustava (preporuča se logična i dosljedna dodjela korisničkih imena), lozinku definira sam korisnik (osim početke koju definira administrator), a UID se dodjeljuje kao prvi sljedeći slobodni UID broj na sustavu.

Korisnik se može nalaziti u jednoj ili u više grupa. Grupu čine korisnici koji imaju slične potrebe, prava i mogućnosti. Svaka grupa ima svoj identifikacijski broj GID (group identification number) i, analogno korisničkom UID broju, preko tog broja sustav prepoznaje grupu. Identifikacijski brojevi UID i GID, odnosno korisničko ime i grupa kojoj korisnik pripada, zajedno definiraju prava pristupa datotekama i dijelovima sustava.

Identifikacija i potvrda autentičnosti korisnika prilikom prijave za rad na sustavu obavlja se provjerom korisničkog imena i lozinke.

Korisnički računi na UNIX računalima

Na UNIX sustavu, postupak dodavanja novog korisnika, odnosno otvaranje korisničkog računa obuhvaća:

- dodjelu korisničkog imena, jedinstvenog identifikacijskog broja korisnika UID, grupe i lozinke
- upis podataka u datoteke /etc/passwd i /etc/group te definiranje parametara korisničkog računa, npr. maksimalno i minimalno vrijeme trajanja lozinke
- kreiranje kućnog direktorija korisnika i kopiranje inicijalnih datoteka kako bi se korisnik mogao prijaviti i raditi na sustavu, te definiranje vlasništva i prava korisnika nad direktorijem
- kreiranje dolaznog pretinca za elektroničku poštu
- testiranje novog računa.

Podaci o korisničkom računu nalaze se u datoteci /etc/passwd. To je tekstovna datoteka u kojoj svaka linija sadrži podatke o jednom korisniku. Podaci su organizirani po poljima međusobno odvojenih dvotočkom. Jedna linija ima oblik:

name:coded-passwd:UID:GID:user information:home-directory:shell

a sadrži redom:

- korisničko ime (name) kojim se korisnik predstavlja sustavu i postaje prepoznatljiv ostalim korisnicima
- šifriranu lozinku (coded-passwd), ili se tu nalazi znak *, a lozinka se sprema u drugu datoteku
- jedinstveni korisnički identifikacijski broj (UID)
- identifikacijski broj osnovne grupe korisnika (GID); korisnik može biti član više grupa, ali se prilikom prijave na sustav uvijek postavlja prvo u grupu definiranu brojem GID u datoteci /etc/passwd, a tijekom rada može prijeći u drugu grupu kojoj pripada te koristiti njihove datoteke na propisani, dozvoljeni način
- podatke o korisniku (user information), najčešće su to ime i prezime, te radno mjesto korisnika odvojeno razmaknicama; informacije iz ovog polja koriste neke naredbe sustava, npr. naredba finger koja ispisuje trenutno prijavljene korisnike na sustavu
- kućni direktorij korisnika (home-directory) u koji se pri prijavi za rad na sustavu automatski postavlja
- ljuska (shell) - definira program koji će UNIX sustav koristiti kao naredbeni interpreter.

Veličina prostora koja se stavlja na raspolaganje korisniku u njegovom kućnom direktoriju, uglavnom je ograničena resursima sustava.

Popis svih grupa nalazi se u datoteci /etc/group. Svaka linija ove datoteke sadrži podatke o jednoj grupi, a oni su zapisani u obliku:

group-name:*:GID:additional-users

Odgovarajuće oznake su:

- naziv grupe (group-name), jedinstveno na sustavu
- identifikacijski broj grupe (GID)
- korisnička imena članova grupe (additional-users) definirana u /etc/passwd, odvojena zarezima

Datoteke /etc/passwd i /etc/group može čitati bilo koji korisnik, a njihov sadržaj može mijenjati samo administrator sustava (root), koji je vlasnik ovih datoteka.

Na kraju treba provjeriti ispravnost i mogućnost rada na novom korisničkom računu. To se može jednostavno napraviti prijavom za rad na sustav pod imenom novog korisnika i ako sustav prepozna njegovo korisničko ime i lozinku, treba provjeriti mogućnost pristupa njegovom direktoriju i pripadnim datotekama. Dodatna provjera sastojala bi se u tome da se ispita je li korisnik vidljiv za druge osobe i funkcije na sustavu, te ima li dostup osnovnim mrežnim uslugama na sustavu.

Zatvaranje korisničkog računa i onemogućavanje pristupa sustavu može se zahtjevati ako korisnik više ne zadovoljava uvjete na osnovu kojih je dobio pravo pristupa sustavu ili ako nije poštivao definirana pravila. Uklanjanje korisničkog računa obuhvaća:

- brisanje odgovarajuće linije u datoteci /etc/passwd;
- brisanje korisnikovog direktorija sa svim pripadnim poddirektorijima i datotekama;
- brisanje njegovog pretinca za dolaznu elektroničku poštu
- brisanje korisnikovog imena iz naziva grupa u /etc/group, ako je korisnik pripadao još nekoj grupi osim osnovne
- zaustavljanje možebitnih pokrenutih procesa korisnika

Na većini sustava, otvaranje i uklanjanje korisničkih računa obavlja se putem komandnih datoteka ili programa.

Korisnički računi na operacijskom sustavu MS Windows

Operacijski sustav MS Windows primarno je bio namjenjen osobnim računalima pojedinaca, ali se posljednjih godina pojavljuju verzije koje dozvoljavaju kreiranje i administriranje više korisnika na jednom osobnom računalu. MS Windows NT WS 4.0 je primjer takovog operacijskog sustava za više korisnika. To nije pravi višekorisnički sustav, jer u jednom trenutku može biti prijavljen i računalo koristiti samo jedan korisnik, ali ipak omogućava fizičko odvajanje i izoliranost direktorija korisnika. Kroz izbornik "Administrative Tools - User Manager", korisnik koji ima administratorska prava može otvarati nove korisničke račune, te mijenjati njihove parametre ili ih brisati. Prilikom otvaranja svakog korisničkog računa, kreira se direktorij korisnika, kopiraju odgovarajuće datoteke (tzv. Profile) koje se tiču izgleda ekrana i rasporeda ikonica, te datoteka i direktorija. Korisnik ima ograničena prava na instaliranje programa, dostupnost drugim datotekama na sustavu, a administrator može definirati duljinu trajanja lozinke korisnika.

Mrežni operacijski sustavi mogu pratiti aktivnosti korisnika jer se u njegovom korisničkom računu nalaze informacije o korištenim datotekama, prostoru na disku (zauzetom i raspoloživom), pokrenutim aplikacijama, radu na sustavu (datum i vrijeme prijave i odjave); registrira se pristup perifernim uređajima, poslane poruke, prijenos podataka na zahtjev korisnika i slično. Na taj način se može pratiti korištenje mrežnih resursa.

Administrator sustava uglavnom postavlja neka ograničenja na račune korisnika. Na primjer, ograničava se duljina trajanja korisničkog računa (ovisno o statusu korisnika, razlogu otvaranja korisničkog računa i sl.), količina prostora na disku dostupna jednom korisniku, broj neuspjelih pokušaja pristupa sustavu (npr. ako korisnik nakon pet pokušaja ne upiše točno lozinku račun se može privremeno ili trajno blokirati), može se definirati da korisnik može pristupiti sustavu samo s točno određenog računala i slično. Od korisnika se obično zahtjeva da nakon nekog vremena promijeni svoju lozinku. Može se definirati maksimalno vrijeme trajanja lozinke (ako korisnik nakon isteka tog vremenskog perioda nije promijenio lozinku njegov korisnički račun se blokira), ali i minimalno vrijeme trajanja lozinke (korisnik mora zadržati lozinku bar neko vrijeme, tj. mora proći bar nekoliko sati, dana ili tjedana, prije nego se korisniku dozvoli ponovna promjena lozinke). Ograničenja se definiraju ovisno o potrebama i mogućnostima sustava te zahtjevanom stupnju sigurnosti.

Otvaranje korisničkih računa znači omogućavanje pristupa sustavu, što uz uporabu resursa kao osnovni cilj otvaranja korisničkih računa, omogućava i zlouporabu. Stoga je sigurnost bitan element o kojem treba voditi brigu pri otvaranju korisničkih računa. Bitno je da sva korisnička imena označavaju fizičke osobe (osim onih potrebnih za rad samog sustava) koje su svojim osobnim podacima - imenom i prezimenom prijavljeni na sustavu, te da svaki administrator vodi urednu evidenciju o svakom otvorenom korisničkom računu i da ga, u slučaju potrebe, može opravdati odgovarajućom potvrdom ustanove za koju radi.

6.3 ORGANIZACIJA MREŽE PREMA RADNIM GRUPAMA

U fazi kad je u zgradi izvedeno ožičenje za lokalnu mrežu, korisnici raspoređeni po prostorijama, te uređaji povezani na mrežu, segmentiranje lokalne mreže provodi se iz jednog od dva razloga - prema potrebama korisnika, ili s ciljem rasterećenja mreže.

Korisnikovi zahtjevi mogu biti opravdani ako se radi o skupini korisnika koji uglavnom komuniciraju međusobno, pa se većina prometa odvija upravo unutar njihove radne grupe (pravilo 80/20), kad zbog zajedničkog ili srodnog posla imaju potrebe za dodatnom sigurnosnom zaštitom, ili kad na taj način učinkovitije mogu koristiti resurse mreže.

S druge strane, kad je ukupni promet po mreži mali, mrežu nije potrebno segmentirati. S porastom opterećenja i prometa po mreži, raste i potreba za odvajanjem segmenata mreže u cilju sprječavanja zagušenja i rasterećenja mreže.

Formiranje radnih grupa povezano je s podjelom klase adresa na blokove. Jednoj radnoj grupi može se dodijeliti jedan ili više blokova adresa, ovisno o potrebama. Takav se pristup preporuča jer, primjenom mrežnih maski, omogućava postavljanje dodatnih mogućnosti ili zabrana određenoj skupini korisnika i njihovih uređaja, čime se postiže funkcionalnija i sigurnija mreža. Također, ovisno o načinu formiranja radnih grupa, dodijeljenu domenu moguće je podijeliti u poddomene. Međutim, to zahtjeva dodatno administriranje, a jedina prednost takvog načina definiranja imena uređaja na mreži jest formalno označavanje pripadnosti određenoj ustrojbenoj jedinici ustanove.

Organizacija u radne grupe može se obaviti na nekoliko načina:

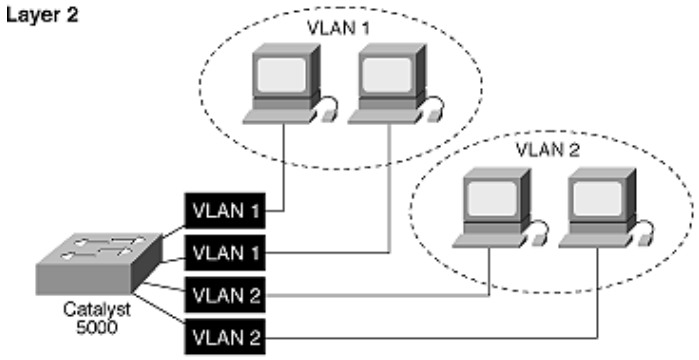
- na fizičkoj razini, formiranjem grupa iste zone kolizije prema fizičkom rasporedu prostorija, pri čemu se ne radi o logičkim radnim grupama korisnika, već je to isključivo posljedica izvedenog ožičenja
- primjenom VLANova na podatkovnoj razini
- primjenom VLANova na mrežnoj razini
- na aplikacijskoj razini kroz operacijski sustav, dozvoljavajući korisnicima iste radne grupe zajedničko korištenje datoteka, direktorija i resursa

U prva tri slučaja radi se o svrstavanju uređaja u radne grupe (sukladno potrebama korisnika, ili potrebama upravljanja mrežom), a u četvrtoj o organizaciji korisnika u radne grupe, najčešće prema potrebama posla kojeg obavljaju.

Kad je odluka o podjeli mreže donijeta, radne grupe je potrebno dobro osmisliti i isprojektirati. Treba predvidjeti moguća širenja radnih grupa, mogućnost pripadnosti korisnika većem broju radnih grupa, te premještanje korisnika iz jedne radne grupe u drugu.

6.3.1 Virtualne lokalne mreže na podatkovnoj razini

Virtualne lokalne mreže primjenjuju se kad je potrebno međusobno povezati korisnike iste interesne grupe, koji ne moraju nužno biti na istoj fizičkoj mreži (mogu biti u različitim dijelovima zgrade, ili čak na potpuno odvojenim lokacijama), a za koje se pretpostavlja da će većina prometa ići upravo unutar tog VLANa.



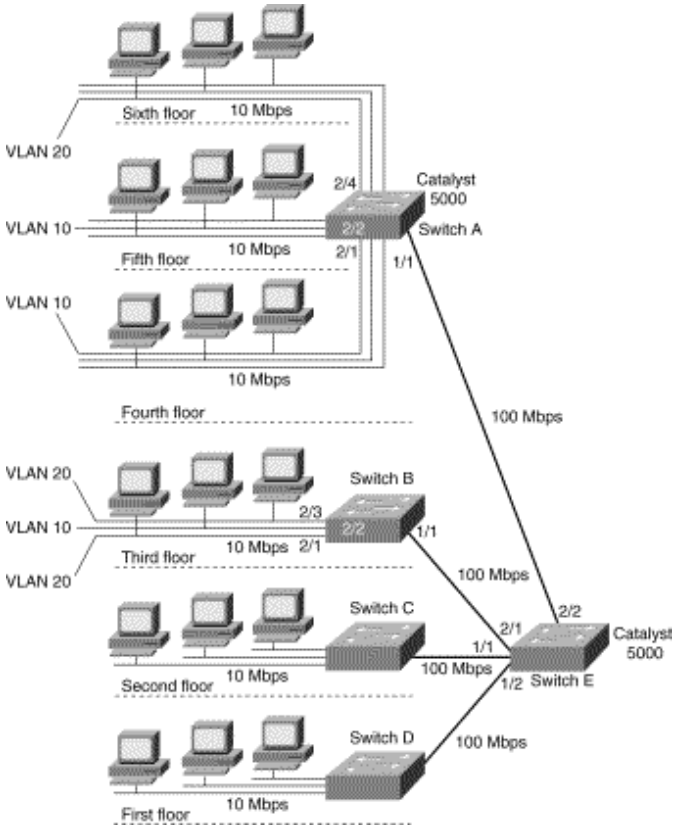
Slika 6.1. Virtualne lokalne mreže na podatkovnoj razini

Okviri univerzalne adrese (broadcast) rasprostiru se segmentima virtualne lokalne mreže, što je izrazito bitno za funkcioniranje protokola više razine koji koriste te okvire za objavljivanje dostupnosti svojih usluga, pa korisnici mogu automatski ostvariti pristup određenoj usluzi. Okviri univerzalne adrese prosljeđuju se

tehnikom razapinjućeg stabla, i posebno upravljanje nije potrebno. Omogućeno je i kontrolirano prosljeđivanje okvira grupne adrese (multicast). Uz ovu pogodnost, razlozi za primjenu VLANova su i: dodatne mjere sigurnosti, povećana učinkovitost rasterećenjem mreže, te olakšano upravljanje mrežom.

Virtualne lokalne mreže na podatkovnoj razini (Layer 2 VLANs) ostvaruju se logičkim grupiranjem priključaka prospojnika između kojih će se razmjenjivati promet za članove grupe. Uređaji korisnika jedne radne grupe na jednoj lokaciji spajaju se na jedan mrežni segment koji se zatim spaja na jedan priključak prospojnika kojem se definira pripadnost određenom VLANu, slika 6.1.

Prvi korak u uspostavi VLANova jest logička organizacija mreže na segmente prema uređajima i/ili korisnicima koji trebaju činiti istu radnu grupu. Zatim slijedi konfiguracija mrežne opreme (prospojnika). Primjer topologije prospajane lokalne mreže u kojoj su konfigurirani VLANovi prikazan je na slici 6.2.



Slika 6.2. - Tipična VLAN topologija

Prospojnik najčešće ima više kartica (slot) koje imaju više priključaka (port), a mjesto spajanja segmenta mreže na karticu označava se s "kartica/priključak". Na primjer, 2/4 označava priključak 4 na kartici 2.

Prema slici 6.2. VLAN 20 sastoji se od priključka 4 na kartici 2 prospojnika A (2/4) i priključka 1 i 3 na kartici 2 na prospojniku B (2/1 i 2/3). Okviri koji se razmjenjuju između priključaka 2/1 i 2/3 prospaja prospojnik B. Prospojnici A-D spojeni su s prospojnikom E vezom propusnosti do 100 Mbps (Fast Ethernet) i njihova međusobna komunikacija odvija se preko ISL protokola.

Na prospojniku B, okvirima koje generiraju priključci 2/1 i 2/3 i koji nisu namjenjeni priključcima 2/1 i 2/3 dodaje se ISL zaglavlje od 30 okteta koje sadrži identifikaciju VLANa 20 i šalje se prospojniku E. Prospojnik E ispituje ISL zaglavlje i kad odredi da je okvir namjenjen VLANu 20, šalje okvir preko svog priključka 2/2 do prospojnika A. Prospojnik A ispituje ISL zaglavlje kako bi odredilo kojem je VLANu okvir namijenjen, uklanja zaglavlje i prosljeđuje okvir. Ako je okvir namijenjen jednom odredištu (unicast) prosljeđuje se priključku 2/4, a ako sadrži univerzalnu adresu odredišta (broadcast) ili je namijenjen grupi primatelja (multicast) prosljeđuje se svim priključcima VLANa 20.

Primjer: konfiguracija VLANova na LAN prospojnicima Cisco Catalyst 5000. Konfiguriranje VLANa na prospojniku **A** obavlja se naredbama:

```
set vlan 10 2/1, 2/2
set vlan 20 2/4
set trunk 1/1 10,20
```

Prva naredba definira VLAN 10 i dodjeljuje mu priključke 1 i 2 na kartici 2. Druga naredba definira VLAN 20 i dodjeljuje mu priključak 4 na kartici 2. Treća naredba konfigurira priključak 1 na kartici 1 kao izlaz prema drugom prospojniku (trunk) i dodaje mu VLANove 10 i 20. Komunikacija između prospojnika odvija se prema ISL protokolu, a podrška tom protokolu ugrađena je u Cisco IOS. Za detekciju i uklanjanje petlji koristi se protokol razapinjućeg stabla (Spanning-Tree Protocol).

Slično je potrebno postaviti na prospojniku **B**. Na prospojniku **E** potrebno je postaviti naredbe:

```
set trunk 2/1 10,20
set trunk 2/2 10,20
```

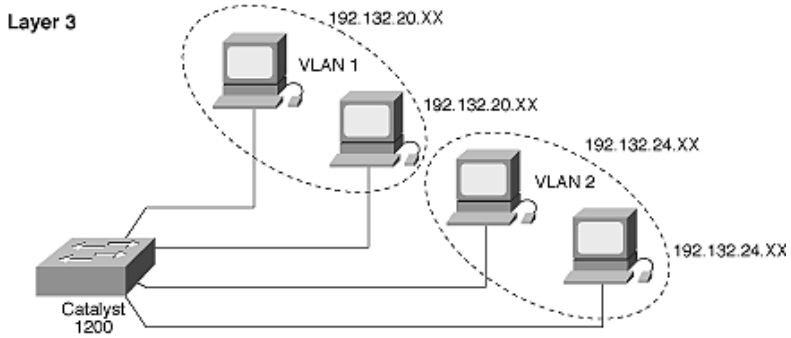
Prva naredba konfigurira priključak 1 kartice 2 kao vezu prema drugom prospojniku i dodaje joj VLANove 10 i 20. Ova veza koristi se za komunikaciju s prospojnikom B. Slično je s drugom naredbom, s tim što ona definira komunikaciju prema A.

Prilikom podjele mreže na segmente koji čine virtualne lokalne mreže moguće je da svaki VLAN ima svoje poslužitelje mrežnih usluga i da ne postoji potreba korištenja poslužitelja na drugim segmentima. Međutim, moguće je i postojanje zajedničkih poslužitelja za cijelu lokalnu mrežu. Ti se poslužitelji mogu staviti na jedan mrežni segment za koji se definira da pripada svim VLANovima koji trebaju koristiti njegove usluge. Također, svi poslužitelji mogu se nalaziti na jednom mrežnom segmentu (server farming) koji može biti veće propusnosti, ili nad njim mogu biti definirane posebne sigurnosne mjere zaštite.

Kad se VLANovi formiraju unutar jedne lokalne mreže, za realizaciju je dovoljna pravilna konfiguracija prospojnika uz primjenu ISL protokola. Ako je, međutim, potrebno povezati više VLANova na različitim lokacijama međusobno odvojenih drugim mrežama, temeljenih možda i na ATM tehnologiji, tad su za realizaciju potrebni i usmjernici, a uz ISL primjenjuje se i IEEE 802.10 protokol, te ATM LANE - standardizirani protokol za emulaciju virtualnih lokalnih mreža preko ATM okosnice.

6.3.2 Virtualne lokalne mreže na mrežnoj razini

Virtualne lokalne mreže na mrežnoj razini formiraju se na osnovu informacija o tipu protokola i adresi podmreže sadržanih u zaglavlju paketa mrežne razine. To znači da se narušava striktna hijerarhijska struktura. Takav tip podjele mreže zahtjeva logičko povezivanje adresa podmreže i oznake VLANa. Na osnovu adrese podmreže, prospojnik pridružuje MAC adresu krajnjeg uređaja pripadajućem VLANu, te određuje druge mrežne priključke čiji uređaji pripadaju istom VLANu.



Slika 6.3. Virtualne lokalne mreže na mrežnoj razini

6.4 KONFIGURACIJA MREŽNIH SERVISA

6.4.1 Domain Name System

Sustav područnih naziva DNS omogućava određivanje FQDN naziva uređaja na mreži na osnovu njegove IP adrese i obratno. Temelji se na modelu klijent/poslužitelj, a realiziran je kao distribuirani sustav baza podataka o uređajima na mreži. Klijent je najčešće ugrađen u programske alate mrežnih usluga, i ne treba ga posebno konfigurirati.

Konfiguracija domenskog poslužitelja koji se nalazi na UNIX sustavu obuhvaća definiranje nekoliko datoteka. Potrebno je definirati osnovni domenski poslužitelj za danu domenu, te upisati podatke o uređajima u bazu podataka. Najčešće se osnovna konfiguracija DNS poslužitelja obavlja prilikom instalacije

poslužitelja, a naknadno se mijenjaju jedino zapisi u bazi podataka dodavanjem uređaja na mrežu, promjenom postojećih konfiguracija mrežnih parametara ili odspajanjem uređaja s mreže.

Razmještaj i naziv konfiguracijskih datoteka, te način upisa potrebnih parametara, može se razlikovati u različitim verzijama UNIX operacijskog sustava, stoga će izgled konfiguracijskih datoteka biti pokazan na primjeru Sun Solaris 7 verzije UNIX opeacijskog sustava.

Primjer: Konfiguracija DNS poslužitelja na Sun Solaris 7 UNIX operacijskom sustavu.

Sve datoteke za konfiguraciju domenskog poslužitelja nalaze se u direktoriju **/etc**. U datoteci **named.conf** definirano je da se preostale konfiguracijske datoteke nalaze u direktoriju **/etc/namedb**, zatim koje datoteke čine bazu podataka DNS sustava (**hosts.db** i **hosts.rev**), koja je inicijalna datoteka za pokretanje procesa spremanja informacija o drugim domenskim poslužiteljima u privremenu memoriju (**named.ca**), te datoteku povratne petlje mreže (**named.local**) u koju je upisana adresa koju uređaji koriste za usmjeravanje prometa unutar mreže. Povezivanje naziva i IP adresa upisanih uređaja obavlja procesa **named**.

Datoteka **named.ca** sadrži podatke o glavnim domenskim poslužiteljima vršnih domena, a služi za inicijalizaciju procesa spremanja zapisa u privremenu memoriju. Sadržaj datoteke može se preuzeti s nekog od javnih ftp poslužitelja, a zapisi koje sadrži su oblika:

```
; formerly NS.NASA.GOV
;
.                        3600000                 NS      E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.      3600000                 A       192.203.230.10
```

tj. sadrže naziv poslužitelja zaduženog za neku domenu, odgovarajuću IP adresu, te vrijeme koliko taj zapis može ostati u privremenoj memoriji (u ovom primjeru 3600000).

Podaci o uređajima na mreži upisuju se u datoteke baze podataka. Datoteka **hosts.db** povezuje naziv uređaja i njemu dodjeljenu IP adresu, a zapis ima oblik:

```
delta           IN    A      178.113.42.8
```

Jedan uređaj može imati više od jednog naziva, npr. ako se radi o WWW ili proxy poslužitelju, što se definira oznakom CNAME:

```
www             IN    CNAME  178.113.42.5
proxy           IN    CNAME  178.113.42.5
```

Moguće oznake zapisa su:

SOA	definira tko je zadužen za domenu (Start of Authority)
NS	naziv imeničkog poslužitelja za tu domenu (Name Server)
Other records	podaci o drugim uređajima u toj domeni
A	povezivanje imena s adresom (Name-to-address mapping)
PTR	povezivanje adrese s imenom (Address-to-name mapping)
CNAME	zamjenski, simbolički naziv (Canonical name)
MX	poslužitelj elektroničke pošte (Mail Exchanger)

U primjeru je također prikazano i kako izgledaju zapisi kad se unutar osnovne dodijeljene domene (rac.velst.hr) definira poddomena (hvar.rac.velst.hr) s jednim upisanom računalom (jelsa) koje je istovremeno domenski poslužitelj te domene (NS) i poslužitelj elektroničke pošte za cijelu domenu (MX):

```
hvar    IN      NS      jelsa.hvar.rac.velst.hr.
hvar    IN      MX      10 jelsa.hvar.rac.velst.hr.
jelsa.hvar.rac.velst.hr.    IN      A       178.113.45.28
```

U istom direktoriju /etc/named treba postojati i datoteka **hvar.db** sadržaja:

```
jelsa                   IN      A               178.113.45.241
```

U datoteci **hosts.rev** nalaze se zapisi pomoću kojih se na osnovu IP adrese određuje naziv uređaja, a uz pomoć posebne poddomene unutar in-addr.arpa domene. U primjeru, ta domena je 42.113.178.in-addr.arpa, a jedan zapis ima oblik:

```
8.42.113.178.in-addr.arpa.      IN      PTR     delta.rac.velst.hr.
```

Datoteke hosts.db i hosts.rev sadrže redni broj Serial i svaki put kad se mijenja sadržaj datoteke potrebno je upisati veću vrijednost od prethodne. To može biti bilo koji broj, a u primjeru je upisan kao datum promjene i broj promjene tog dana (ggggmmddbr).

Datoteke baze podataka (hosts.db i hosts.rev) nisu osjetljive na velika i mala slova, ali se preporuča nazive uređaja pisati malim slovima. Također, te datoteke ne smiju sadržavati prazne retke, komentari se označavaju s ";", a stupci se odvajaju tabovima.

Upisane promjene postaju aktivne tek nakon ponovnog pokretanja **named** procesa.

Administratorima sustava preporuča se davanje naziva uređaja na mreži slijedeći neku logiku, kao i praćenje i evidentiranje svih dodijeljenih naziva i IP adresa, ne samo kroz DNS sustav.

DNS konfiguracijske datoteke na UNIX OS (Sun Solaris 7)

```
%> more /etc/named.conf

options {
        directory        "/etc/namedb";
        forwarders       { 161.53.2.70; };

};

zone "rac.velst.hr" in {
        type master;
        file "hosts.db";
};

 zone "42.113.178.in-addr.arpa" in {
        type master;
        file "hosts.rev";
};

 zone "0.0.127.in-addr.arpa" in {
        type master;
        file "named.local";
};

 zone "." in {
        type hint;
        file "named.ca";
};
```

```
%> more /etc/namedb/named.local
;
; BIND data file for local loopback interface.
;
@       IN      SOA     alpha.rac.velst.hr. postmaster.alpha.rac.velst.hr. (
                        3       ; Serial
                        43600   ; Refresh
                        4300    ; Retry
                        3600000 ; Expire
                        3600 )  ; Minimum
        IN      NS      alpha.rac.velst.hr.
1       IN      PTR     localhost.
```

```
%> more /etc/namedb/named.ca
;
; formerly NS.INTERNIC.NET
;
.                       3600000         IN      NS      A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000                 A       198.41.0.4
;
; formerly NS.NASA.GOV
;
.                       3600000                 NS      E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000                 A       192.203.230.10
;                               ....
; End of File
```

Datoteke DNS baze podataka

```
%> more /etc/namedb/hosts.db
; Data file of hostnames in this zone.
;
@       IN      SOA     alpha.rac.velst.hr. postmaster. alpha.rac.velst.hr. (
                        2000031601      ; Serial
                        28800   ; Refresh
                        7200    ; Retry
                        604800  ; Expire
                        86400 ) ; Minimum
        IN      NS      alpha.rac.velst.hr.
        IN      NS      beta.velst.hr.
;
hvar   IN      NS      jelsa.hvar.rac.velst.hr.
hvar   IN      MX      10 jelsa.hvar.rac.velst.hr.
jelsa.hvar.rac.velst.hr.    IN      A       178.113.45.28
;
; %HOSTS_START%
localhost               IN      A               127.0.0.1
alpha                   IN      A               178.113.42.5
bindmaster              IN      CNAME           alpha
www                     IN      CNAME           alpha
proxy                   IN      CNAME           alpha
;
; Host Database
delta                   IN      A               178.113.42.8
omega                   IN      A               178.113.42.253
;
rac.velst.hr.           IN      MX      10      alpha.rac.velst.hr.
; %HOSTS_END%
```

```
%> more /etc/namedb/hosts.rev
; Data file for reverse address to hostname.
; Data file of hostnames in this zone.
;
@       IN      SOA     alpha.rac.velst.hr. postmaster.alpha.rac.velst.hr. (
                        2000031601      ; Serial
                        28800   ; Refresh
                        7200    ; Retry
                        604800  ; Expire
                        86400 ) ; Minimum
                IN      NS      alpha.rac.velst.hr.
                IN      NS      beta.velst.hr.
; %HOSTS_START%
5       IN      PTR     alpha.rac.velst.hr.
8.42.113.178.in-addr.arpa.          IN      PTR     delta.rac.velst.hr.
253.42.113.178.in-addr.arpa.        IN      PTR     omega.rac.velst.hr.
;
; %HOSTS_END%
```

```
%> more /etc/namedb/hvar.db
; Data file of hostnames in this zone.
;
@       IN      SOA     alpha.rac.velst.hr. postmaster.alpha.rac.velst.hr. (
                        1999060901      ; Serial
                        28800   ; Refresh - 5 minutes
                        7200    ; Retry - 1 minute
                        604800  ; Expire - 2 weeks
                        86400 ) ; Minimum - 12 hours
        IN      NS      alpha.rac.velst.hr.
;
; %HOSTS_START% - entries added by make_hosts
;localhost               IN      A               127.0.0.1
jelsa                    IN      A               178.113.45.241
; %HOSTS_END%
```

7 PROJEKTIRANJE I ODRŽAVANJE RAČUNALNIH MREŽA SA STANOVIŠTA SIGURNOSTI

7.1 UVOD

Prednost koju korisnicima pruža povezivanje u računalnu mrežu jest otvorenost prema drugim računalima i drugim mrežama, te mogućnost pristupa informacijama bez obzira na fizičku razdvojenost. Računalnoj opremi moguće je pristupiti s brojih i udaljenih lokacija koje najčešće uopće nisu pod nadzorom vlasnika ili administratora računala. Iz tog je razloga puno zahtjevnija i ozbiljnija zadaća zaštiti umreženi, nego izolirani, nepovezani sustav. Osnovni ciljevi zaštite sustava jesu osigurati konzistentnost i funkcionalnost sustava, te integritet i pouzdanost podataka. Mjere zaštite sustava često uvode dodatne restrikcije, što može utjecati na smanjivanje dostupnosti ili kvalitete usluga. Razina zaštite sustava najčašće je kompromis potreba korisnika za zaštitom vlastitih podataka i slobode pristupa uslugama sustava.

Planiranje zaštite sustava temelji se na ispitivanju poznatih prijetnji, te prijedloga rješenja kao rezultat kompromisa. Sustav se štiti od aktivnosti nedobronamjernih osoba koji mogu, ali ne moraju biti ovlašteni korisnici resursa lokalne mreže, kao i od nedovoljno upućenih ili neobrazovanih korisnika čije pogreške mogu na bilo koji način ugroziti rad sustava (na primjer, brisanjem podataka onemogućiti rad nekog drugog korisnika na sustavu ili neke usluge i slično). Potrebno je zaštiti mrežnu opremu, poslužitelje, radne stanice i podatke korisnika.

Bitna činjenica u planiranju zaštite sustava jest temeljnost mrežnih usluga na modelu klijent-poslužitelj. Poslužitelji su stalno spojeni na mrežu i pružaju usluge korisnicima na ili izvan lokalne mreže. Kako se većina podataka nalazi upravo na poslužiteljima, to oni postaju glavna točka koju na sustavu treba štititi.

7.2 SIGURNOSNE PRIJETNJE I NAČINI ZAŠTITE SUSTAVA

Mogući ciljevi napada na sustav su:

- neovlašteni pristup podacima ili sustavu
- promjena ili brisanje podataka
- generiranje netočnih ili krivih podataka
- onemogućavanje usluge (denial of service)

a postupak projektiranja zaštite sustava može se znatno olakšati ako su poznati putevi i načini na koji neki sustav može biti ugrožen. Iz tog je razloga napravljena sistematizacija mogućih prijetnji kroz nekoliko razina koje su usporedive s ISO-OSI komunikacijskim modelom, te modelom Interneta (TCP/IP). Prvi korak u zaštiti sustava je fizička zaštita opreme.

7.2.1 Fizička zaštita mrežne opreme

Fizička zaštita mrežne opreme podrazumijeva zaštitu od neovlaštenog pristupa ili krađe. Osnovni oblik zaštite sastoji se u ograničenju, nadzoru i kontroli fizičkog pristupa komunikacijskoj opremi (modemima, prospojnicima, usmjerivačkim uređajima) i računalima u nadležnosti mrežnog administratora, a zatim i računalima i terminalima namijenjenim ovlaštenim korisnicima.

Zaštita od elementarnih nepogoda ili ublažavanje njihovih posljedica moguće je uvođenjem dodatnih uređaja. Na primjer, moguće je uvesti uređaje za neprekidno napajanje (UPS), prenaponske zaštite, uređaje za otkrivanje i zaštitu od požara, a potrebno je i redovito praviti zaštitne kopije podataka (backup). Zaštitne kopije omogućavaju obnavljanje oštećenih ili izbrisanih datoteka, a moraju biti redovito održavane i obnavljane tako da sadrže sve bitne izmjene i prave verzije datoteka. Također, posebne mjere mogu se primjeniti na pohranu zaštitnih kopija (čuvati na dva odvojena mjesta) s ciljem sprječavanja oštećivanja, neželjenih promjena sadržaja ili krađe.

Neke od ovih mjera oslabljenje su samom činom povezivanja u lokalnu ili globalnu računalnu mrežu.

7.2.2 Fizička razina

Mjere sigurnosti na fizičkoj razini bliske su fizičkoj zaštiti komponenti mreže, uglavnom komunikacijskih kanala. U tablici 7.1, kao prijetnje prepoznate su i izdvojene prisluškivanje medija, uništavanje medija i uništavanje ili oštećenje opreme. Predložene mjere zaštite jesu fizička zaštita, razmještaj prijenosnih medija i mrežne opreme, kao i strukturna organizacija mreže.

RAZINA	NAPAD	OBRANA	NAPOMENA
Fizička	Neovlašten pristup fizičkom mediju	Odspojiti utičnice koje se ne koriste	onemogućava neovlašteno spajanje opreme, a time i postavljanje uređaja za prisluškivanje
		Zaštititi pristup aktivnim utičnicama	
		Koristiti optičke kablove gdje je to moguće	
	Uništavanje fizičkog medija ili prekid veza	Zaštititi kanalice	povećati pouzdanost veza
		Osigurati alternativne puteve	
	Oštećenje opreme (kroz utičnice)	Odspojiti utičnice koje se ne koriste	
	Interferencija signala	Odspojiti mrežne segmente sa smetnjama	

Tablica 7.1. - Prijetnje i zaštite na fizičkoj razini

Dobro organizirana i izvedena zaštita na fizičkoj razini ograničava mogućnost pristupa mrežni s neprovjerenom opremom, čime je pružena osnova za zaštitu na višim razinama.

7.2.3 Podatkovna razina

Sigurnosne prijetnje na podatkovnoj razini prikazane su u Tablici 7.2., a obuhvaćaju hvatanje podataka na lokalnoj mreži i generiranje prevelikog nepotrebnog prometa, kao i neovlašteni pristup preko javne telefonske mreže.

RAZINA	NAPAD	OBRANA	NAPOMENA
Podatkovna	Neovlašteni pristup kroz javnu telefonsku mrežu	Provjera identifikacije i autorizacija korisnika	
	Hvatanje paketa podataka (data capture)	Onemogućiti pokretanje programa za hvatanje paketa	(npr. programa kao što je tcpdump)
		Pratiti stanje mrežnih priključaka opreme	s ciljem detekcije promiskuitetnog načina rada što upućuje na prisluškivanje
		Koristiti LAN prospojnike	omogućavaju nadzor distribucije okvira dijeljenjem mreže na više zona kolizije
		Koristiti šifriranje na višim razinama	uhvaćeni podaci postaju beskorisni
	Preplavljivanje lokalne mreže podacima	Pratiti promet po lokalnoj mreži	u tom slučaju treba koristiti programe za hvatanje paketa
		Koristiti LAN prospojnike	koji omogućavaju selektivno uskraćivanje usluga nepovjerljivim ili nekorektnim korisnicima

Tablica 7.2. - Prijetnje i zaštite na podatkovnoj razini

Mjere zaštite na podatkovnoj razini obuhvaćaju identifikaciju korisnika na modemskim poslužiteljima, praćenje prometa na lokalnoj mreži i mrežnoj opremi, te segmentaciju mreže ovisno o prometu. Poput definiranja korisničkih računa na poslužiteljima koji podržavaju višekorisnički rad, mogu se definirati korisnici i na modemskim poslužiteljima. Korisnik je predstavljen svojim korisničkim imenom i lozinkom. Prilikom postavljanja zahtjeva za pristup, na postavljeni upit odgovara svojim podacima čime prolazi proces identifikacije (prepoznavanja korisnika) i autorizacije (potvrđivanja lozinke). Uz ispravno upisane podatke korisniku se dozvoljava uspostava veze s modemskim poslužiteljem. Nakon toga, korisnik može uspostaviti vezu s drugim poslužiteljima (i vjerojatno prolaziti sličan proces autentifikacije), te koristiti mrežne usluge.

7.2.4 Mrežna razina

Na mrežnoj razini, javlja se problem mogućnosti pristupa i napada s udaljenih dijelova mreže. Od posebnog su značaja tehnike zaštitnog kodiranja, kao i postavljanje vatrenog zida s ciljem zaštite pristupa mreži.

Zaštitno kodiranje (šifriranje, kriptiranje) predstavlja postupak tranformaciju podataka iz jednog oblika u drugi nečitljivi, s ciljem prikrivanja informacije. Izvorni podaci se kombiniraju s drugim podacima (ključem)

primjenom nekog od algoritama, a kao rezultat dobijaju se nečitljivi - šifrirani podaci. Postupak zaštitnog kodiranja može se provoditi na razini aplikacije, ili s kraja na kraj komunikacijske veze čime se omogućava zaštita prijenosa svih podataka preko takve veze.

Vatreni zid (firewall) ograničava komunikaciju jednog dijela mreže s drugim, ili jedne mreže s drugim mrežama. Temelji se na ograničenom i selektivnom propuštanju paketa upućenih nekom od uređaja na vlastitoj mreži. Kako je pristup mreži moguć isključivo preko vatrenog zida, to on predstavlja osnovnu točku koju na sustavu treba štiti, a puno je jednostavnije dobro osigurati jednu točku u sustavu, nego sve komponente sustava. Stoga je primjena vatrenog zida česti tip zaštite osjetljivih dijelova sustava.

Vatreni zid po funcijama koje obavlja i načinu na koji radi dijelom pripada mrežnoj, a dijelom prijenosnoj razini. Pojam IP vatreni zid obuhvaća tehnike filtriranja i maskiranja IP paketa, kao i izgradnju privatnih mreža (intraneta). Filtriranje je selektivno propuštanje paketa na osnovu informacija koje sadrže, najčešće informacija o izvorišnom ili odredišnom računalu i tipu usluge, a maskiranje je postupak zamjene parametara komunikacije - adresa i priključnih brojeva usluge, s ciljem prikrivanja informacija o štićenoj mreži. Tablica 7.3. daje pregled prepoznatih mogućih napada na sustav, i primjer obrane sustava.

RAZINA	NAPAD	OBRANA	NAPOMENA
Mrežna	krivo ili lažno predstavljanje (IP spoofing, false identification)	Koristiti šifriranje; onemogućiti usluge koje provjeru identiteta korisnika temelje na podacima IP razine	na taj način onemogućava se ubacivanje krivih ili hvatanje izvornih podataka na višim razinama
	Preuzimanje uspostavljene veze (Connection hijacking)		
	Neovlašteni pristup računalima	Koristiti IP vatreni zid (filtriranje paketa i privatne mreže)	kako bi se onemogućili svi pokušaji spajanja s nepovjerljivih računala
	preplavljivanje IP paketa (s udaljenih mreža)	Koristiti IP vatreni zid	sprječava se neželjeni dotok paketa
	Neovlašeno mijenjanje tablica usmjeravanja	Ograničiti pristup i prava administriranja usmjerivačkih uređaja	npr. omogućiti pristup i mogućnost konfiguriranja samo preko konzole

Tablica 7.3. - Prijetnje i zaštite na mrežnoj razini

7.2.5 Prijenosna razina

Na prijenosnoj razini, sigurnosni aspekti su slični onima na mrežnoj, a zaštita sustava ostvaruje se preko posrednika (proxy) koji vezu uspostavljaju umjesto samog korisnika.

RAZINA	NAPAD	OBRANA	NAPOMENA
Prijenosna	krivo predstavljanje i preuzimanje TCP veza (TCP spoofing and hijacking)	Isto kao i na mrežnoj razini	
	Neovlašteni pristup računalima	Koristiti vatreni zid na prijenosnoj razini i koncept privatnih mreža.	npr. proxy SOCKS za uspostavu TCP veza umjesto korisnika
		Definirati listu računala koja imaju pravo pristupiti štićenom računalu	

Tablica 7.4. - Prijetnje i zaštite na prijenosnoj razini

7.2.6 Korisnička razina

Na korisničkoj razini zastupljene su mrežne usluge koje zbog svoje transparentnosti i raspoloživosti postaju posebno izložene napadima. Zlouporabu mrežnih usluga i neovlašteni pristup sustavu omogućavaju nedostaci u programskoj podršci koji se svakodnevno otkrivaju. U Tablici 7.5., dan je pregled prijetnji za osnovne mrežne usluge - telnet, ftp i elektroničku poštu. Mjere zaštite sastoje se uglavnom od pravilne konfiguracije operacijskog sustava, programske podrške poslužitelja i klijenta, te isključivanje usluga koje se ne koriste.

USLUGA	NAPAD	OBRANA	NAPOMENA
Telnet	Neovlašteni pristup korisnika (uporaba, mijenjanje ili uništavanje korisnikovih podataka)	Definiranje pravila na izbor i duljinu trajanja lozinke. Korištenje jednokratnih lozinki. Zabrana pristupa s nepovjerljivih računala.	do lozinke se može doći hvatanjem paketa na nižim razinama, pogađanjem na osnovu poznavanja korisnika ili korisnikovih podataka
	Neovlašteni pristup u ime administratora sustava (s ciljem promjene podataka samog sustava ili instalacije programske podrške štetne za sustav)	Pravila o lozinkama	cilj je onemogućiti neovlašteno sticanje administratorskih prava
		Pristup kao administrator sustava dozvoliti samo sa konzole i biranog terminala.	
		Otklanjati nedostatke programske podrške	
		Praćenje rada sustava i aktivnosti korisnika na sustavu kroz datoteke koje bilježe pristup i korištenje resursa sustava	otkrivanje nedozvoljenih aktivnosti
FTP	Neovlašteni pristup korisnika (kopiranje, stavljanje, zamjena ili brisanje podataka)	Kao i za Telnet; Provjeravati datoteke sumnjivog sadržaja	postavljene datoteke mogu sadržavati viruse, crve ili trojanske konje
	Zlouporaba pristupa javnim FTP poslužiteljima	Pažljiva uspostava javnog FTP poslužitelja	cilj je izbjeći pristup datotečnom sustavu koji nije namjenjen običnom korisniku
E-mail	Krivo predstavljanje (slanje elektroničke pošte pod tuđim korisničkim imenom)	Zabrana uporabe SMTP protokola. Pravilna konfiguracija programa za razmjenu elektroničke pošte (sendmail)	
	Neovlašteni pristup e-mail porukama korisnika	Koristiti šifriranje	npr. PGP
	Zasipanje porukama (E-mail spamming)	Nema učinkovite obrane	primjenjuju se dopuštene tehnike slanja e-mail poruka

Tablica 7.5. - Prijetnje i zaštite na korisničkoj razini

Mrežnu uslugu World Wide Web (WWW) karakterizira vrlo brz i dinamičan razvoj. S obzirom na mogućnst dohvata i prikazivanja multimedije, postaje najčešće korištena usluga uvodeći nove standardne prezentacije informacija. Zbog jednostavnosti uporabe, koristi se za i pristup brojnim drugim mrežnim uslugama. Sigurnosni aspekti WWW-a prikazani su u Tablici 7.6.

USLUGA	NAPAD	OBRANA	NAPOMENA
WWW	Pregled sadržaja direktorija	Zabraniti pristup ili postaviti datoteku index.html	sprječava uvid u sadržaj direktorija
	Zlonamjerni cgi-bin programi	Dozvoljavati samo provjerene cgi programe	zaštita WWW poslužitelja od neovlaštenog pristupa ili zlouporabe
	Loše napisane cgi-bin i Java script komandne datoteke	Temeljita provjera kôda uz ispravljanje pogrešaka	
	Zlonamjerni Java appleti	Web pregledniku zabraniti izvršavanje Java programa	zaštita računala klijenta
	Neovlašteno hvatanje podataka	Primjenjivati šifriranje	za prijenos tajnih podataka (npr. brojevi kreditnih kartica)

Tablica 7.6. - Prijetnje i zaštite WWW usluge

Dinamika razvoja HTML jezika, jezika u kojem su pisane WWW stranice, te uvođenje interaktivnih elemenata programskim alatima, dovode do čestih promjena u konfiguracijama programske podrške na strani poslužitelja i klijenta i pojave novih verzija programa. Iako je cilj omogućiti korisniku sve prednosti novih promjena, često sa sobom nosi sigurnosne probleme nastale kao posljedica previda u izradi programa. U sljedećim verzijama, otkriveni problemi se otklanjaju, ali se nehotice mogu pojaviti novi. Kako je i ova usluga temeljena na modelu klijent - poslužitelj, upravo su programska podrška klijenta i poslužitelja točke koje treba štititi. Uz to, sigurnost sustava ovisi i o programima koji omogućuju interaktivnost i stranicama daju dodatnu dinamiku (cgi i Java komandne datoteke, Java programi), a temelje se na dodatnim obradama na strani poslužitelja ili na strani klijenta.

7.2.7 Razina operacijskog sustava i sigurnost korisnika

Na razini operacijskog sustava i korisnika potrebno je primjenjivati slične mjere zaštite kao i na korisničkoj razini. Dodatak predstavlja instalacija novih verzija operacijskog sustava, te programskih dodataka (patch) namjenjenih otklanjanju otkrivenih nedostataka ili pogrešaka.

Sadržaj kojeg korisnik dohvati putem računalne mreže može sadržavati zlonamjerne programe. Primjer takvih programa su **virusi** - programski kôd koji se dodaje nekoj datoteci, **crvi** (worms) - programi koji djeluju kao samostalne datoteke i **trojanski konji** - programi koji naizgled rade nešto korisno, a u sebi sadrže skrivene zlonamjerne odsječke. Svima je zajedničko svojstvo kopiranje i prenošenje na druge sustave. Akcije koje virusi, crvi i trojanski konji obavljaju mogu biti usmjerene na postojeće datoteke na sustavu koje mijenjaju i/ili uništavaju, te na onemogućavanje korištenja resursa. S tim problemima korisnik se može susresti i kod preuzimanja podataka nekim od vanjskih memorijskih medija (diskete, CD), pa iste principe provjere i mjere zaštite treba primjeniti i kod prihvata podataka računalom mrežom. S obzirom da je učinak uvijek štetan, prijeko je potrebno provjeravati ispravnost svih preuzetih datoteka. Programi koji automatski provjeravaju nove datoteke nazivaju se antivirus programi. Zadaća je administratora sustava brinuti da sva računala imaju instalirane takve programe, te da se redovito osvježava baza podataka o virusima koje antifirus program moći otkriti i otkloniti.

	NAPAD	OBRANA	NAPOMENA
Operacijski sustav	Korištenje programskih manjkavosti sustava za neovlašteni pristup i stjecanje administratorskih prava	Redovito i ažurno instalirati dodatke op. sustavu	najnovije informacije dostupne su putem distribucijskih lista ili na Web stranicama
Korisnički programi		Redovito instalirati nove verzije programa	
Preuzimanje datoteka	Virusi, crvi, trojanski konji itd	Provjeravati primljeni sadržaj. Primjenjivati antivirus programe	zastupljeno kod mrežnih usluga: WWW, FTP, e-mail

Tablica 7.7. - Operacijski sustav i sigurnost korisnikovih podataka

7.3 TIPOVI RADNIH GRUPA PREMA ZAHTJEVANOJ RAZINI ZAŠTITE

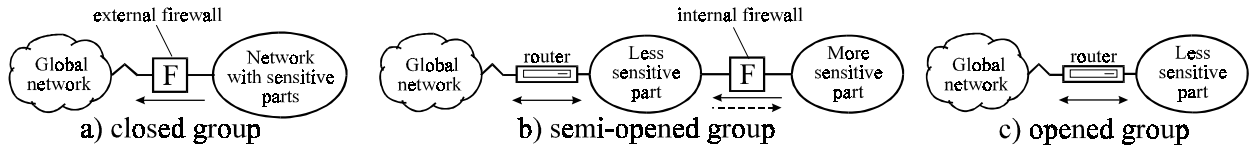
Kao dio projektiranja informatičkog sustava u cjelini, projektiranje računalne mreže sa stanovišta sigurnosti temelji se na primjeni organizacijskih i strukturnih mjera. Organizacijske mjere su skup pravila koje korisnici trebaju poštivati tijekom uporabe mrežnih resursa. Strukturne mjere utječu na topologiju mreže, definiranje i izbor mrežne opreme, kao i odluke o tipu i verziji primjenjene programske podrške.

Razmatrajući strukturne i organizacijske mjere, mreže se temelje na konceptu radnih grupa. Sa stanovišta sigurnosti, radne grupe mogu se klasificirati u zatvorene, poluotvorene i otvorene.

Zatvorena grupa ne objavljuje podatke na javnu mrežu. Pristup podacima preko javne mreže strogo je zabranjen, čak i članovima grupe. Članovima zatvorene grupe može se dozvoliti pristup informacijama preko javne mreže jedino ako ne ugrožava njihovu lokalnu sigurnost. Primjena vatrenog zida je obvezna.

Poluotvorene grupe objavljuju podatke na javnu mrežu, ali i dalje zahtjevaju visoku razinu zaštite za ostatak operacija. Neke poluotvorene grupe dozvoljavaju provjerenim korisnicima i/ili računalima pristup tajnim podacima. To se može postići primjenom vatrenog zida.

Otvorene grupe objavljuju sve svoje podatke na javnu mrežu. Najčešće postoje kao dio poluotvorene mreže, ali se nekad mogu stvarno i uspostaviti, npr. grupa studenata.



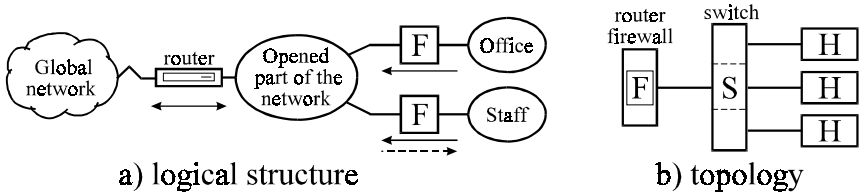
Slika 7.1. - Struktura podmreža grupa

Logička struktura podmreže za te tri grupe prikazana je na slici 7.1. Zatvorena grupa spaja se preko vanjskog vatrenog zida čime se ograničava i kontrolira komunikacija i (najčešće samo dolazni) promet. Osjetljivi dio mreže poluotvorene grupe štiti se primjenom internog vatrenog zida, čime se čuvani resursi izoliraju od ostatka mreže. Otvorena grupa ne treba imati vatreni zid. Može se zaključiti da je struktura poluotvorene grupe univerzalna, jer se eliminacijom vanjske podmreže prelazi u zatvorenu, a unutarnje u otvorenu mrežu.

Primjer: Organizacija računalne mreže akademske ustanove sa stanovišta sigurnosti

Sukladno specifikaciji posla i potrebi za razmjenama informacija, definirane su četiri grupe: referada, računovodstvo, nastavno osoblje i studenti. Prve dvije grupe imaju povjerljive podatke koji bi smjeli biti dostupni malom broju korisnika, najvjerojatnije samo s računala iz lokalne mreže. Stoga njihovi podaci moraju biti zaštićeni, a pristup ograničen. Referada može imati podatke koji moraju biti javno dostupni svima i, za razliku od računovodstva, više je otvorena prema drugim sustavima i drugim korisnicima. Nastavno osoblje i studenti su znatno više usmjereni prema vanjskom svijetu, ali se razlikuje tip podataka koje te dvije skupine razmjenjuju. Stoga je potrebno djelomično razdvojiti te dvije skupine.

U svakom slučaju, nedvojbeno je da mreža treba biti organizirana kao poluotvorena grupa. Slika 7.2. prikazuje logičku strukturu podmreže, kao i mogući način realizacije takve lokalne mreže.



Slika 7.2. - Struktura i topologija podmreža za akademsku ustanovu

U ovom slučaju, optimalna struktura sastojala bi se od jedne vanjske i dvije unutarnje podmreže. Potrebno je formirati tri segmenta mreže, a poželjno je i ostvariti tri virtualne lokalne mreže. To se može realizirati primjenom prospojnika i usmjernika. Na usmjerniku je moguće definirati pristupne liste kojim se ograničava pristup uslugama i/ili dijelovima mreže i to predstavlja prvu razinu zaštite u pristupu mreži. Prospojnik s definiranim virtualnim lokalnim mrežama omogućava razdvajanje prometa, a time i dodatne zaštite unutar same lokalne mreže. Ovaj način zadovoljava principe strukturnog kabliranja.

Drugi, lošiji, način realizacije bio bi primjenom usmjernika koji može obavljati funkcije vatrenog zida.

Ako ustanova ima više poslužitelja, sukladno predstavljenoj organizaciji, mogući raspored poslužitelja dan je u Tablici 7.8.

POSLUŽITELJ	**Otvoreni**	**Nastavnici**	**Službe**
zajedničke mrežne usluge (DNS, WWW proxy, WWW, FTP)	x		
nastavnici (korisnički računi, pošta, osobne WWW stranice)		x	
studenti (korisnički računi, pošta, osobne WWW stranice)	x		
referada - glavni poslužitelj (interni)			x
referada - javni poslužitelj	x		
opće službe - poslužitelji			x
odjeli (ustrojbene jedinice)		x	
radne stanice (računala) nastavnika		x	
radne stanice (računala) - opće službe			x
računalne učionice	x		

Tablica 7.8. - Razmještaj poslužitelja (podataka i usluga)

Svaka ustanova mora definirati svoja pravila korištenja mrežnih resursa i dosljedno ih provoditi. Uz mogućnost zajedničkog korištenja, briga za ispravnim radom i funkcionalnošću računalne mreže postaje briga svih njezinih korisnika. Administratori računalne mreže trebaju stalno pratiti rad mreže i aktivnosti korisnika, s ciljem presretanja, što bržeg otkrivanja i otklanjanja problema ili nedostataka sustava. Zatim, treba pratiti promjene mrežnih tehnologija i sukladno tome instalirati nove verzije operacijskih sustava i programa, posebno onih kojih ispravljaju uočene sigurnosne nedostake sustava. Korisnici sustava trebaju biti što više obrazovani i što bolje informirani o specifičnosti sustava, pravima, te načinu korištenja raspoloživih im usluga. U tome im pomaže administrator sustava. Uz brigu za računalima i mrežnom opremom, posebno mjesto zauzima i briga o korisničkim podacima, pa tu značajnu ulogu igra redovito spremanje zaštitnih kopija podataka.

DODATAK **A**

IP adresa mreže: _____

Mrežna maska: _____

Domena mreže: _____

Default gateway _____

DNS server _____

Proxy server _____

r.br.	naziv računala	IP	soba	oznaka utičnice	port na hubu	radna grupa
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						
17.						
18.						
19.						
20.						
21.						
22.						
23.						
24.						
25.						