Sveučilište u Splitu

**Fakultet elektrotehnike, strojarstva i brodogradnje**

# Računalne mreže

Upute za laboratorijske vježbe

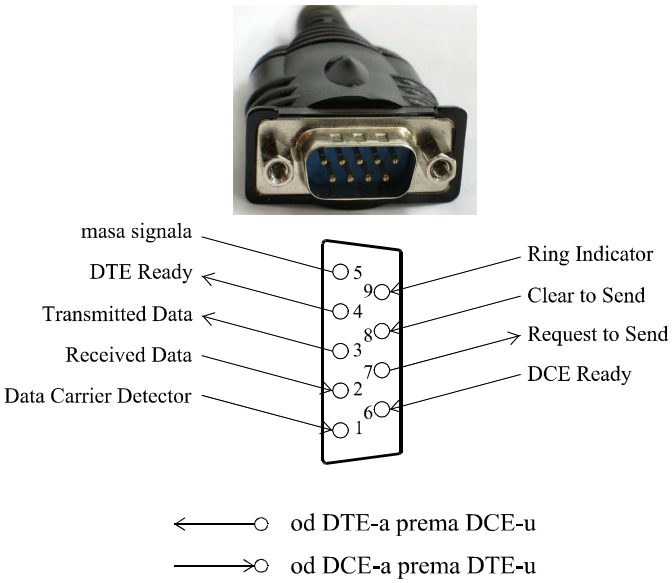
(radni materijal)

**Split, 2010.**

# 1. SUČELJE DTE/DCE

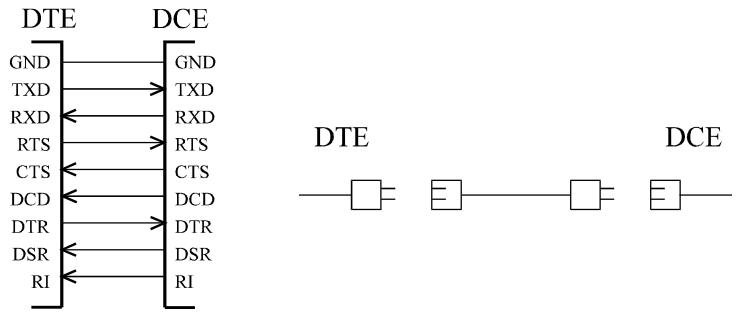
Sučelje između terminala (Data Terminal Equipment - DTE) i modema tj. uređaja za zaključenje kanala (Data Circuit Terminating Equipment - DCE) danas ima veliki značaj, jer je ugrađeno u svako osobno računalo. Ovo je sučelje opisano standardom RS232 američke organizacije EIA, odnosno ekvivalentnim preporukama ITU-T-a V.28 i V.24. RS232 standard obuhvaća električne, funkcionalne i mehaničke karakteristike sučelja, dok ITU-T za električne karakteristike donosi preporuku V.28, za funkcionalne V.24, a mehaničke su karakteristike specificirane standardom ISO 2110.

Veza između DTE-a i DCE-a ostvaruje se kabelom između dva uređaja. Na DTE-u je muški konektor, a na DCE-u ženski konektor. Obično se koristi 9-pinski D konektor, a rijetko i 25- pinski konektor.



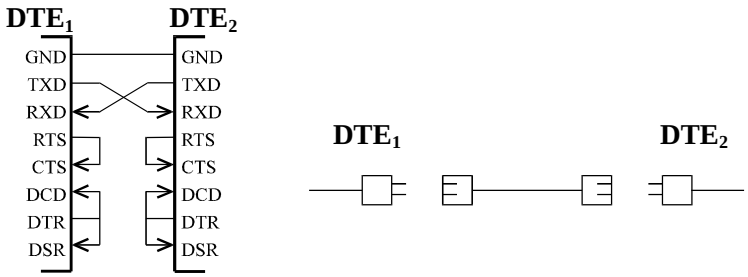

**Sl.1 . Muški 9-pinski konektor i njegovi signali**

Računalo se s modemom spaja modemskim kabelom prikazanim na Sl. 2.



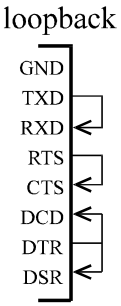

**Sl. 2. Modemski kabel**

Ukoliko se želi uspostaviti direktna terminalska veza dvaju računala, dovoljno blizu smještenih, upotrebljava se nul-modemski kabel, prikazan na Sl. 3.




**Sl. 3. Nul-modemski kabel**

Cilj ove vježbe je provjeriti karakteristike signala V.24/V.28, odnosno RS232 sučelja. Promatraju se signali na osnovnim linijama sučelja: TXD, RXD, RTS, CTS, DTR, DSR, DCD i RI. Mjerenje se izvodi na modificiranom RS232 konektoru (loopback) koji ima izvode za priključak osciloskopa (TXD-RXD, GND), a ostali su konektori prespojeni kao kod nulmodemskog kabela, tako da uz TXD-RXD spoj imamo situaciju kao da je na serijski port računala spojeno drugo računalo koje svaki oktet podataka koji primi po RXD liniji odmah i šalje natrag po TXD liniji.

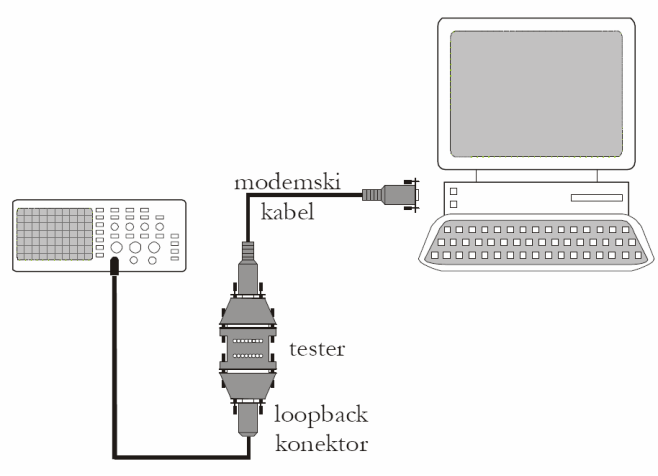



**Sl. 4. Loopback konektor**

**Prvi zadatak** u sklopu vježbe je povezivanje dvaju računala nul-modemskim kabelom i prijenos podataka među njima.

**Drugi zadatak** je osciloskopom snimiti signale u loopback načinu rada.

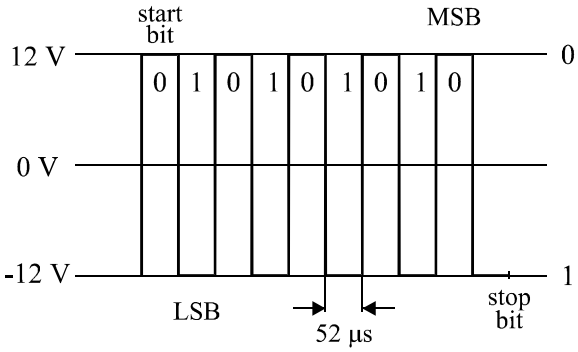
Podatke na serijsko sučelje računala najlakše je slati korištenjem tzv. terminalskih programa od kojih je jedan uključen i u Windows operacijski sustav (Hyper Terminal). Terminalski program znakove unesene s tipkovnice šalje u ASCII obliku na odabrano serijsko sučelje (najčešće COM 1), a podatke primljene sa sučelja prikazuje u ASCII obliku u prozoru terminala. U drugom dijelu vježbe na muški D konektor konvertera se priključuje loopback konektor. Sonda osciloskopa se priključuju na TXD (RXD) – GND izvode loopback konektora, te očitavamo oblik signala. Za svaki utipkani znak može se uočiti start bit, stop bit, te ASCII kod samog znaka.




**Sl. 5. Mjerenje u loopaback načinu rada**

### *Mjerenje signala u loopback načinu rada*

Budući da je prijenos između računala i modema asinkron, a serijski port računala je podešen da podatke šalje u formatu 1 start bit, 8 podatkovnih bita, 1 stop bit, na osciloskopu se za svaki znak utipkan na tipkovnici dobije upravo taj format podataka. Prvi je bit u logičkoj nuli i predstavlja start bit, a zadnji je bit u logičkoj jedinici i predstavlja stop bit, a između njih se nalazi ASCII kod utipkanog znaka. Ovo se mjerenje izvršava na podatkovnim linijama TXD i RXD, na kojima se koristi negativna logika, tj. negativni napon predstavlja logičku jedinicu, a pozitivni napon predstavlja logičku nulu. Podaci na podatkovnim linijama se prenose počevši od najmanje značajnog bita (Least Significant Bit - LSB), a završavaju najznačajnijim bitom (Most Significant Bit - MSB). Na Sl. 6. prikazan je signal dobiven na osciloskopu za znak U, čiji je ASCII kod 01010101.




**Sl. 6. Prikaz slova U na osciloskopu**

Mjerenja je moguće provesti i na ostalim linijama, no dovoljna je i LED signalizacija ugrađena u RS 232 tester spojen između serijskog sučelja računala i loopback konektora. Budući da su to upravljački signali koji koriste pozitivnu logiku, vrijednost ON je aktivna vrijednost i za nju se koristi napon od 12V, a za vrijednost OFF napon od -12V. Hyper Terminal, kao i ostali komunikacijski programi, pri pokretanju postavi DTR signal u ON stanje, stoga je isto stanje i na DSR te DCD liniji. Identična je situacija i kod RTS-CTS linija.

## *1.1 MODEMI I DIREKTNO POVEZIVANJE KOMUTIRANJEM KANALA*

Modemska veza donedavno je bila najčešći način spajanja malih korisnika na Internet. Danas se koristi rijetko, ili kod bežičnog pristupa Internetu GSM/UMTS mrežom. Uređaj koji omogućuje komunikaciju na fizičkoj razini naziva se modem. Povezivanje modema i računala zahtijeva vrlo malo podešavanja i prektično se svodi na povezivanje na računalo serijskim USB ili PCMCIA priključkom kod vanjskih (eksternih) modema, ili PCI priključkom kod internih modema. Modemi se i dalje masovno koriste za niz primjena (mobilni telefoni, sustavi daljinskog nadzora i sl.) a princip rada im je ostao jako jednostavan i praktički nepromijenjen dugi niz godina.

Modem s operativnim sustavom komunicira korištenjem Hayes AT jezika. Naredbe modemu kao i odgovori modemu prenose se kao niz ASCII znakova koji završavaju CR-LF (0x13 0x10) znakovima. Naredbe modemu počinju s "AT" ASCII znakovima. Komunikacija s modemom danas najčešće nije vidljiva jer se realizira na razini pogonskog programa modema (drivera) koji zahtjeve aplikacijskog programa prevodi u niz AT stringova koji se šalju modemu. Izravna komunikacija moguća je korištenjem terminalskih programa, slično kao u prvom dijelu vježbe.

Modem se može nalaziti u jednom od dva načina rada: upravljačkom ili podatkovnom. U upravljačkom načinu rada pomoću AT naredbi se postavljaju sadržaji pojedinih registara modema, određuju početni parametri rada modema, te uspostavlja i raskida veza. Pod uspostavom veze podrazumijeva se prospajanje telefonskog kanala do udaljenog modema i postizanje sinkronizacije među modemima u smislu detekcije vala nosioca, sinkronizacije miješanja (scramblera) i poništenja jeke, prilagodbe brzine prijenosa stanju (kvaliteti prijenosne linije), itd, a kod digitalnih sustava (GSM, ISDN) uspostava veze još je jednostavnija.

Postoji niz modemskih protokola za prijenos datoteka, od kojih su najpoznatiji XMODEM, YMODEM i ZMODEM. XMODEM protokol ne omogućuje prijenos imena datoteke, a greške su nešto češće zbog korištenja checksum metode detekcije greški. YMODEM osigurava prijenos imena datoteke i pouzdaniji prijenos zahvaljujući CRC zaštiti od pogreški. ZMODEM povećava brzinu prijenosa veća zahvaljujući većim paketima podataka i streaming načinu prijenosa.

Skup komandi koje pojedini modem razumije i može izvršiti naravno ovisi o tipu modema.

- ATE1Q0 instrukcija uključuje echo funkciju modema, koja svaki poslani znak modemu odmah i vraća nazad terminalskom programu, pa "vidimo što pišemo", što je u biti softverska verzija loopback konektora upoznatog u prethodnoj vježbi.

- ATI0-ATI9 naredbe ispisuju parametre modema (proizvođač, model, verzija firmwarea, itd.).

- ATX3 naredba modemu naređuje modemu da ne čeka na signal slobodne linije

• Uspostava veze s udaljenim računalom može se inicirati korištenjem ATDT<broj>. Drugo računalo prihvaća poziv, automatski ili ručno. Za automatsko prihvaćanje, potrebno je u registru S0 podesiti broj zvonjenja prije nego se modem javi. Za ručno prihvaćanje postavimo S0=0, te kasnije operater komandom ATA prihvaća poziv. Nakon uspostave veze modem prelazi u podatkovni način rada (chat mode, prijenos datoteka..).

• +++ je "escape sequence" za prelazak iz podatkovnog moda natrag u komandni

• AT0 naredba je za povratak iz komandnog moda u podatkovni (nakon izdavanja naredbe +++)

• ATH0 je "hang" naredba za prekidanje veze

Bitno je uočiti da je jedna od AT komandi ATX3 koja se odnosi na signal slobodne linije. Većina modema je u osnovi rađena za američko tržište, a tamo je standard drugačiji nego u Europi. Ukoliko se ne isključi čekanje na signal slobodne linije, modem neće prepoznati europski standard i neće izvršiti biranje. Naredba ATX3 određuje da modem ne čeka na signal slobodne linije, već da počne odmah birati broj.

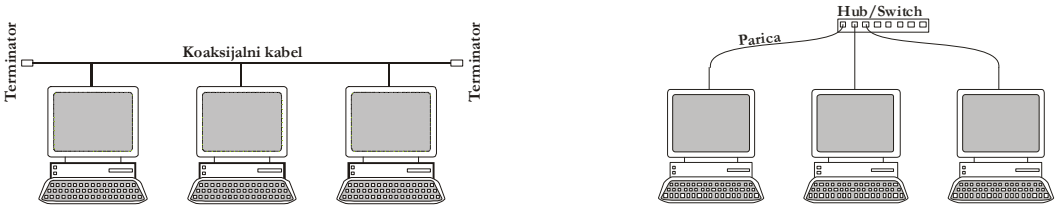
U drugom dijelu vježbe jedno računalo zove drugo (ATDT), ono odgovara (ATA), te se veza uspostavlja. Uspostavljena veza identična je nul-modemskoj vezi, osim po brzini prijenosa, koja je u prvom dijelu vježbe bila ograničena karakteristikama serijskog porta i nul-modemskog kabela, dok je sada ograničena karakteristikama modema i telefonske linije, koji su po brzini daleko ispod brzine serijskog porta ( omjer ~910 kbps / ~56kbps).

Prikazani skup AT naredbi samo je mali podskup naredbi koje postoje kod različitih modema. GSM modemi koji su sastavni dio mobilnih telefona posjeduju AT komande za rukovanje telefonskim (SIM) imenikom, slanje i čitanje SMS poruka, itd.

**Zadatak** u ovom dijelu vježbe je izvršiti spajanje dva računala modemskom vezom. Parovi računala u laboratoriju povezani su USB (Universal Serial Bus) modemima. USB veza danas je najčešće sučelje za povezivanje većine vanjskih uređaja na računalo, no u biti se radi o tzv. virtualnom serijskom portu, koji se fizički oslanja na USB sučelje, ali se rukovanje njime bitno ne razlikuje od klasičnog serijskog porta opisanog u prethodnoj vježbi. Modemi su povezani na telefonsku centralu koja omogućuje uspostavu lokalnih veza.

# 2. LOKALNE MREŽE ETHERNET

Lokalna mreža omogućuje veliku brzinu prijenosa podataka i malo kašnjenje, a ograničena je na računala unutar prostorije ili zgrade (kratak doseg). Najčešće se koriste lokalne mreže tipa Ethernet, s daleko najviše instalacija brzine 100 MB/s, dok su instalacije 10 MB/s (starije) ili 1000MB/s rijetkost. Osim po brzini, lokalne mreže Ethernet mogu se podijeliti i po vrsti komunikacijskog medija koji se koristi za prijenos podataka (fizička razina ISO-OSI modela) pa postoje Ethernet na parici (Base-T) koji je daleko najčešća instalacija, dok su varijante s koaksijalnim kablovima (Base5 i Base2) korištene u prošlosti, a varijanta s optičkim vlaknima (Base-F) je dosta skuplja i stoga se rijeđe koristi. Slijedi prikaz dvije karakteristične lokalne mreže:



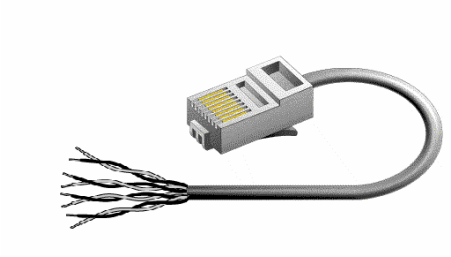

**Sl. 1 B5/2 LAN i BT LAN**

Prva mreža temelji se na koaksijalnim kabelima. Mrežne kartice sadrže koaksijalni konektor, na koji se priključuje tzv. T koaksijalni konektor, koji omogućuje spajanje svih računala u lokalnoj mreži u niz, pri čemu je bitno uočiti da sva računala koriste isti komunikacijski kabel (višespojni medij). Posljedica je takve organizacije da u određenom trenutku samo jedno od računala može slati podatke na lokalnu mrežu. Te podatke primaju sva računala koja su priključena na višespojni medij, a ako neko od računala u tom trenutku pokuša poslati podatke na mrežu nastupa kolizija (collision), stoga se koristi i termin *domena kolizije* za skup računala koji koriste isti višespojni medij.

Protokol na kojem se temelji dijeljenje zajedničkog medija u Ethernet mreži je MAC protokol (Media Access Control). Mrežna kartica koja želi poslati podatke na medij osluškuje stanje medija i čeka trenutak kada medij postane slobodan (Carries Sense). Kako više uređaja osluškuje zajednički medij ovaj pristup se naziva *Carrier Sense Multiple Access* (CSMA). Budući da signalu kojeg šalje jedna stanica treba određeno vrijeme da stigne do ostalih stanica, može se dogoditi da neka stanica počne slati podatke iako neka druga stanica već šalje, te dolazi do sudara (kolizije). Nastanak kolizije očituje se kroz nagli porast napona na vodu, a podaci koji su trenutno na mediju su izgubljeni i potrebna je retransmisija. Postupak otkrivanja sudara se naziva *Colision Detection* (CD). Ethernet mreže koriste oba navedena postupka, odnosno **CSMA/CD**.

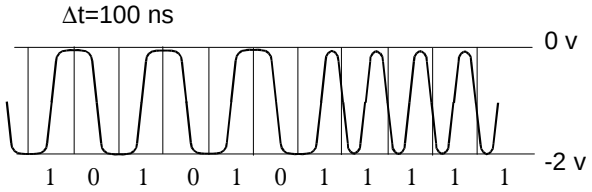
Koaksijalni kabel obavezno je zaključen karakterističnom impedancijom (50 Ω). Zbog ispravne detekcije kolizije duljine segmenata kabela ograničene su ovisno o brzini mreže. Iz istog razloga minimalna duljina okvira lokalne mreže je ograničena na 64 bajta. Okvir je naziv za PDU (Protocol Data Unit) druge, tj. podatkovne, mrežne razine. Maksimalna duljina okvira također je ograničena (podaci do 1500 bajta), ali to ograničenje nema posebnog tehničkog uporišta već je uzrokovano cijenom memorija prvih računala na Ethernetu.

Druga mreža temelji se na paricama. Mrežne kartice sadrže RJ-45 konektor preko kojeg se spajaju na UTP kabel s osam vodova (4 parice). 10 i 100 Mbit/s mreže koriste dvije parice (1-2 prijem, 3-6 predaja). Drugi kraj kabela spojen je na *hub* ili *switch.*



**Sl. 2 UTP kabel i RJ45 konektor**

HUB (zvjezdište) je elektronički uređaj koji signal (niz bitova kodiranih MANCHESTER II kodom) koji dobije na prijemnoj parici nekog od priključenih računala proslijedi na predajne parice ostalih priključenih računala, eventualno ga i pojača i očisti od šuma, ali nema inteligentnih funkcija u smislu čitanja podataka iz niza bitova koje primi. REPEATER (obnavljač) je uređaj sličan hubu, ali ima samo dva ulaza, pa se koristi za obnovu signala kod dužih prijenosnih linija. Hub i repeater rade na fizičkom sloju mreže. Segment lokalne mreže u kojem je povezivanje računala ostvareno samo hubovima i repeaterima čini jednu domenu kolizije.



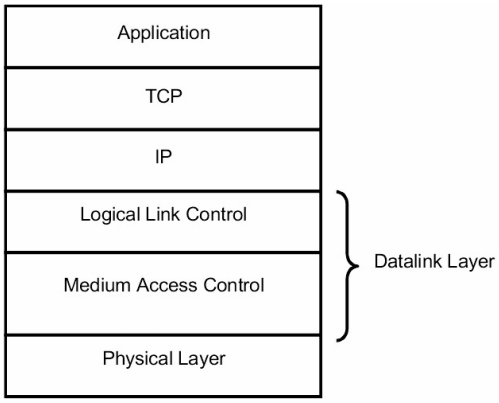

**Sl. 3 Manchester II kodiranje na Ethernet mreži**

SWITCH (prospojnik) je inteligentniji od HUB-a, budući da čita podatke iz primljenih paketa (okvira) i na temelju njih određuje na koji od svojih priključaka će poslati paket. Pritom ne može nastupiti kolizija jer se okvir ne prosljeđuje na sve priključke kao kod HUB-a, već samo onom računalu kojem su podaci namijenjeni. Kako nema kolizije, nema ni problema s njenom detekcijom koji su određivali maksimalne duljine segmenata kabela, pa su oni sada isključivo ograničeni gušenjem signala. *Broadcast* okvire, naravno, switch prosljeđuju na sve svoje portove, osim dolaznog. Njihovo prosljeđivanje ograničava se uređajima više razine (router, gateway), tj. ovi uređaji odvajaju tzv. *broadcast domene*.

Ova arhitektura se gotovo isključivo koristi kod 1000 Mbit/s mreža, koja osim toga koristi sve 4 parice, jer je takt od 1 ns previsok za parice, pa se koristi prijenos po dva bita po taktu (5 naponskih razina) i takt od 125 MHz, što razultira traženom brzinom 1 Gbit/s.

Današnje lokalne mreže 100 Mbit/s organizirane su najčešće kao na slici 1, uz korištenje switcha, i iznimno rijetko huba. Kod mreža koje se rasprostiru na više prostorija obično dio opreme čini i komunikacijski ormar sa switchevima i *patch panelom*. Na patch panel su spojeni dolazni kabeli iz utičnica razmještenih po prostorijama koje pokriva lokalna mreža. Računala su spojena na utičnice u zidu, utičnice kabelima na patch panel, a iz patch panela se tzv. *patch kabelima* povezuju sa switchevima.

## *2.1 Protokoli lokalne mreže Ethernet*




**Sl. 4. Ethernet podrazine u TCP/IP skupu protokola**

Fizička razina kod Ethernet mreža definira kodiranje/dekodiranje i prijem/predaju električnog signala, generiranje prembule.

Podatkovna razina (datalink layer) podijeljena je u dva dijela:

- MAC podrazina implementira funkcije pristupa mediju;
- LLC razina prihvaća podatke od nadređene razine (najčešće IP), formira okvire lokalne mreže, popunjava polja adresa i kontrolne sume, a kod prijema okvira testira njegovu ispravnost, odvaja podatkovni dio od zaglavlja okvira i prosljeđuje ga nadređenoj razini.

Ethernet okvir prikazan je na sljedećoj slici:

| 8 okteta | 6 okteta | 6 okteta | 2 okteta | 46 do 1500 okteta | 4 okteta |
|---|---|---|---|---|---|
| Preambula | Odredišna adresa | Izvorišna adresa | Tip okvira | Podaci i dopuna | CRC |

**Sl. 5 Ethernet okvir**

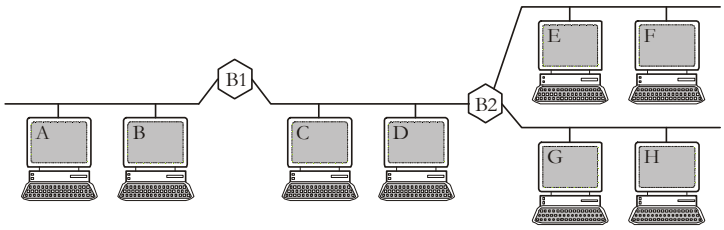
Dva su polja iz zaglavlja jako bitna: Destination i Source Address adresiraju dva računala (mrežne kartice) koji izmjenjuju okvire. Svaka kartica unutar svoje ROM memorije ima upisanu adresu, koja je jedinstvena, tj. ne postoje dvije kartice koje imaju identičnu (MAC) adresu. Ona je duljine 6 oketa, pri čemu su gornja tri okteta identifikacija proizvođača kartice, a donja tri su vrijednost koju dodjeljuje proizvođač. Ukoliko je mreža kreirana uz korištenje huba ili koaksijalnih kabela, svaki okvir koji se pojavi na mreži prihvati svaka kartica, ali se nadređenoj razini (najčešće IP) prosljeđuju podaci samo u tri slučaja:

- ako je odredišna adresa jednaka adresi kartice,
- ako je odredišna adresa broadcast (OxFFFFFFFFFFFF),
- bezuvjetno, ako je kartica u tzv. promiskuitetnom modu, kod testiranja.

Polje Tip okvira (Frame Type) definira protokol korišten na mrežnoj razini, i kod najčešćeg protokola mrežne razine (IP) iznosi 0x0800. Preambula služi za sinkronizaciju po bitu i okviru, a sastoji se od 7 okteta oblika 10101010 te zadnjeg okteta oblika 10101011.

Sada je moguće detaljnije opisati radi switcha. Switch analizira promet preko svojih ulaza i gradi tablicu, koja mu omogućuje da Ethernet okvir proslijedi na onaj svoj priključak na koji je spojena mrežna kartica s MAC adresom koja se nalazi u polju Odredišna adresa (Destination Address) zaglavlja okvira. Spomenuta switch tablica ili tablica MAC adresa sadrži parove MAC adresa - port. Svakom priključku switcha može biti pridruženo više MAC adresa ukoliko je na njega spojen hub s više priključenih računala. Ukoliko je mreža kreirana uz korištenje switcha, okviri koji dolaze do mrežne kartice bit će samo oni koji imaju odredišnu MAC adresu identičnu MAC adresi kartice, ili broadcast okviri.

BRIDGE (premosnik) je uređaj sličan switchu te se ta dva pojma često zamjenjuju: switch najčešće ima mnogo priključaka jer služi povezivanju računala na mrežu, dok bridge najčešće povezuje dvije ili više lokalnih mreža koje ne moraju biti istovrsne (koristiti iste protokole). Primjer četiri lokalne mreže povezane s dva bridgea prikazan je na sljedećoj slici:




**Sl. 6. Lokalne mreže povezane bridgevima**

Četiri mreže povezane su s dva bridgea B1 i B2. Bridge radi na temelju tri jednostavna pravila, koja se, naravno, temelje na MAC adresama izvorišta i odredišta Ethernet okvira:

- Ukoliko je MAC adresa i izvorišta i odredišta na istom LAN-u paket se odbacuje (filter). Ovo je situacija kada npr. komuniciraju računala A i B, te će bridge B1 odbaciti takav paket.

- Ukoliko je MAC adresa izvorišta i odredišta različita paket se prosljeđuje (forward) na segment na kojem se nalazi odredišna MAC adresa. Ovo je situacija kada npr. komuniciraju računala A i C.

- Ukoliko je adresa odredišta nepoznata, obavlja se prosljeđivanje na sve priključene LAN-ove, osim na izvorišni (flooding).

Na temelju izvorišnih adresa okvira koji dolaze do njega, bridge saznaje na kojem se LAN-u nalazi mrežna kartica s određenom MAC adresom, te taj podatak sprema u tablicu i koristi kada je potrebno proslijediti paket na tu MAC adresu.

Osim učenja, te filtriranja i prosljeđivanja, switchevi/bridgevi posjeduju i funkcionalnost sprječavanja petlji koju im omogućava Spanning Tree Protocol (STP). Naime, redundantne veze među bridgevima služe boljoj dostupnosti dijelova LAN-a, ali gašenjem pojedinih portova STP sprječava međusobno prosljeđivanje okvira među bridgevima u beskonačnoj petlji.

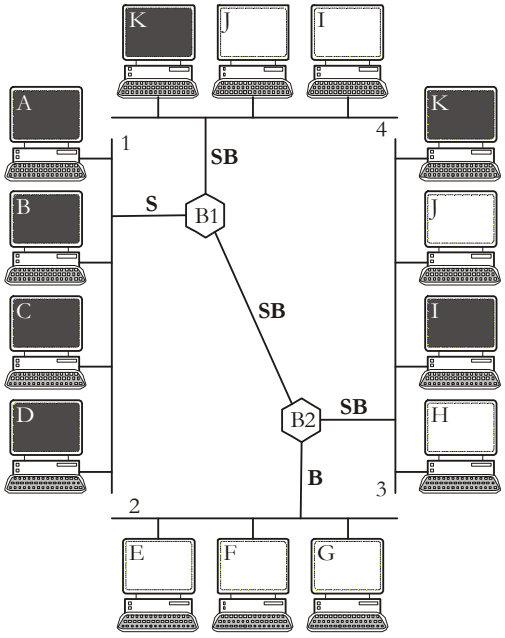
## *2.2 VLAN mreže*

*Virtual LAN*, tj. virtualne lokalne mreže su one kod kojih je logička organizacija mreže različita od fizičke organizacije. Klasična organizacija podrazumijeva da su npr. na slici 6 računala A i B na istoj mreži i fizički i logički, npr. jedan odjel u tvrtki. Ukoliko postoji potreba da se samo npr. računala A i C povežu u logičku cjelinu, koriste se VLAN bridgevi ili switchevi, koji imaju mogućnost konfiguracije svakog ulaza (porta) kao dijela određenog VLAN-a. Dodatna funkcionalnost koju VLAN bridge ili switch ima je tablica koja povezuje svako računalo s pripadajućim VLAN-om. Veza VLAN-računalo može biti izvedena na tri načina:

- svakom portu pridjeljena je oznaka VLAN-a, što je dobro rješenje ukoliko su fizički i virtualni LAN identični (LAN 1 i 2 na sl.7). Nedostatak ovog načina je što, ako se računalo premjesti s jednog porta na neki drugi, administrator mora rekonfigurirati VLAN;

- svakoj MAC adresi mrežne kartice pojedinog računala pridjeljena je oznaka pripadajućeg VLAN-a, što je sasvim dobro rješenje za većinu situacija;

- adresi mrežne razine! (razina 3!) je pridjeljena oznaka pripadajućeg VLAN-a, što je "hack" rješenje koje se koristi u situacijama kada MAC adresa ne odgovara uvijek istom računalu, pa ga se može identificirati jedino po adresi s mrežne razine (npr. IP, AppleTalk...). Mana rješenja je kršenje neovisnosti razina ISO-OSI modela)




**Sl. 7 VLAN mreže**

Primjer na prethodnoj slici prikazuje 4 fizička LAN-a organizirana u dva logička VLAN-a (sivi i bijeli). Jedan priključak bridgea B1 u njegovoj tablici označen je oznakom prvog VLAN-a (S, sivi), dok su druga dva označena oznakom SB (sivi, bijeli), dakle na taj priključak proslijeđuju se okviri s odredišnim MAC adresama i iz S i B VLAN-a. Bridge B2 konfiguriran je slično: Dva ulaza označena su sa SB, dok je jedan označen s B, jer se na fizičkom LAN-u 2 nalaze samo računala iz bijelog VLAN-a.

Okvir koji računalo A šalje računalu B, bit će odbačen na bridgeu B1; okvir koji računalo B šalje računalu K bit će proslijeđen preko B1 i B2 na LAN 3, odnosno računalu K, itd. Svaki VLAN čini jednu *broadcast domenu*, a komunikacija računala smještenih u različite VLAN-ove omogućava se uređajima više razine.

Nazivi (vrste) portova na switchu/bridgeu s definiranim VLAN-ovima su:

- Trunk port - na koji se spaja drugi switch/bridge (uređaj koji podržava VLAN). Okviri koji ulaze/izlaze iz ovog porta najčešće imaju dodatna polja u zaglavlju 2. razine koja identificiraju pripadni VLAN (označeni okviri), prema protokolu 802.1Q;

- Access port - na koji se spaja hub ili računalo (uređaj koji ne podržava VLAN). Okviri koji ulaze/izlaze iz ovog porta su neoznačeni.

**Zadatak** u ovoj vježbi je povezati računala u laboratoriju na switch, grupirati računala u zasebne VLAN-ove, te testirati mogućnost komunikacije unutar pojedinog VLAN-a, kao i između zasebnih VLAN-ova.

# 3. Internet protokol (IP)

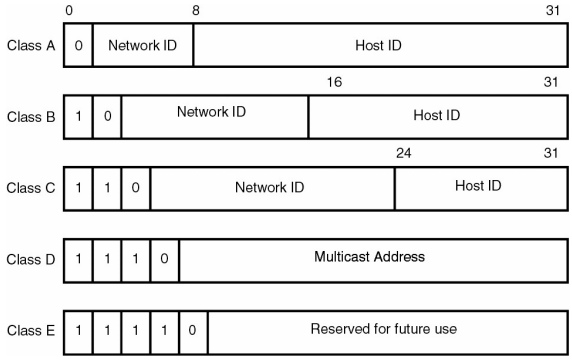
S razvojem Interneta kao globalne mreže, razvijao se i skup protokola koji se koriste za komunikaciju između računala. Budući da je ovaj skup protokola od početka bio namijenjen spajanju raznorodnih mreža, sloj pristupa mreži kod Interneta je otvoren. Osim vlastitih protokola, on uključuje bilo koju funkcionalnu mrežnu tehnologiju. Ovaj skup protokola je i najčešći izbor kod današnjih lokalnih mreža, čak i onih koje nisu vezane na Internet mrežu.

Internet protokol IP je protokol mrežne razine koji je temelj Internet mreže i većine današnjih lokalnih mreža. Namjena mu je osigurati prijenos podataka (IP datagrama) između raznorodnih mreža, što uključuje dva zadatka: adresiranje i usmjeravanje. Adresiranje omogućuje identificiranje izvorišta i odredišta datagrama, dok usmjeravanje omogućuje dostavu datagrama do odredišta najoptimalnijim putem.

IP protokol je nepouzdani bespojni protokol, dakle ne uspostavlja logički kanal kao spojevni protokoli, pa ne nudi zaštitu od gubitka datagrama. Kako je rukovanje datagramima zasebno za svaki od njih, kao i zbog drugih karakteristika Internet mreže, moguće je da niz datagrama poslan prema odredištu stigne do njega redoslijedom različitim od onog kod slanja, a moguća je i pojava višestrukih kopija istog datagrama. Trenutno su u upotrebi dvije varijante IP protokola: IPv4 je starija verzija protokola koja se zbog brzog rasta Interneta zamjenjuje novom varijantom: IPv6.

## *3.1 Adresiranje po IP protokolu*

Adresiranje ima ulogu identificirati svako računalo, odnosno čvor u IP mreži. Stoga adresa mora sadržavati identifikaciju mreže u kojoj se čvor nalazi, kao i samo računalo unutar mreže (čvor). IP adrese u IPv4 protokolu su duljine 32 bita (~4 milijarde mogućih adresa). Dio IP adrese identificira mrežu, a ostatak identificira računalo unutar mreže. Ovisno o tome koliki dio IP adrese predstavlja mrežu, a koliko dio računalo uvedena je podjela na klase IP adresa:




**Sl. 2. Klase IPv4 adresa**

Klasa A namijenjena je jako velikim mrežama s do $2^{24}$-2 računala. Klasa B može imati do $2^{16}$-2 računala. Klasa C namijenjena je mrežama s do $2^{8}$-2 = 254 računala. Po dvije IP adrese iz svakog raspona su rezervirane: adresa računala koja binarno ima sve jedinice je tzv. broadcast adresa za dotičnu mrežu, a ona sa svim nulama identificira mrežu. Klasa D se koristi za multicast adresiranje (slanje jednog paketa na više adresa), a klasa E za eksperimentalnu upotrebu.

IP adrese se najčešće zapisuju u tzv. *dotted quad* formi, gdje se svaki oktet iz 32 bita adrese predstavlja svojim decimalnim ekvivalentom, npr. 161.53.168.12. je decimalni ekvivalent binarne

adrese 10100001 00110101 10101000 00001100. Iz ovog zapisa lako možemo zaključiti kojoj klasi pripada određena IP adresa:

| | | | |
|---|---|---|---|
| **0.0.0.0** | **-** | **127.255.255.255** | **A klasa** |
| **128.0.0.0** | **-** | **191.255.255.255** | **B klasa** |
| **192.0.0.0** | **-** | **223.255.255.255** | **C klasa** |
| **224.0.0.0** | **-** | **239.255.255.255** | **D klasa** |
| **240.0.0.0** | **-** | **255.255.255.255** | **E klasa** |

Neke od ovih adresa imaju posebnu namjenu. Mreža 0.0.0.0 predstavlja default mrežu i ove adrese se koriste za rutiranje. Posebna je i adresa 255.255.255.255, koja služi za broadcast poruka cijeloj mreži na kojoj se neko računalo nalazi. Raspon 127.0.0.0-127.255.255.255 je rezerviran za tzv. *loopback adresu*. Datagram upućen na tu adresu vraća se računalu koje ga je poslalo. Koristi se za testiranje i debuggiranje softvera i hardvera. Odvojeni su i blokovi tzv. privatnih IP adresa radi interne upotrebe na računalima koja nisu direktno spojena na Internet.

## *3.2 ICMP*

ICMP – *Internet Control Message Protocol* razvijen je za komuniciranje usmjernika (računala koja usmjeravaju datagram od izvorišta do odredišta), međusobno, kao i s izvorišnim računalima da bi se izvijestilo o eventualnoj pogreški nastaloj u obradi paketa (nedostupnost mreže, zagušenje, ...). Neke ICMP poruke su:

- Echo request - šalje se da bi se dobila informacija o dostupnosti nekog odredišta.
- Echo reply - odgovor na Echo request.
- Redirection – preusmjeravanje, kada se u tablici nađe kraći put do odredišta.
- Destination Unreachable - nedostupnost računala, mreže, porta ili protokola.
- Time Exceeded - obavještava izvorište da je paketu isteklo "vrijeme života" (TTL=0).
- Parameter Problem - usmjernik je naišao na nekonzistentnost unutar zaglavlja.
- Source Quench - zahtjev izvorištu za smanjenjem brzine slanja paketa, paket odbačen.

Progam Ping koristi ICMP Echo Request poruku da bi odredio da li je odredište aktivno i dostupno. Svako računalo koje podržava IP protokol podržava i ICMP protokol, te se ispravnost IP konfiguracije računala u lokalnoj mreži može testirati naredbom ping <IP adresa>:

```
H:\>ping 161.53.168.96

Pinging 161.53.168.96 with 32 bytes of data:

Reply from 161.53.168.96: bytes=32 time<1ms TTL=128
Reply from 161.53.168.96: bytes=32 time<1ms TTL=128
Reply from 161.53.168.96: bytes=32 time<1ms TTL=128
Reply from 161.53.168.96: bytes=32 time<1ms TTL=128

Ping statistics for 161.53.168.96:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

## 3.3 DNS

Kako je i decimalna notacija IP adresa nezgodna za pamćenje uvedena je usluga DNS (*Domain Name Service*) koja IP adrese zamjenjuje hijerarhijski organiziranim sustavom imena: IP adresa 161.53.168.12 ima svoj DNS ekvivalent epic1.fesb.hr; .hr je top-level (vrhovna) domena, .fesb je sekundarna, itd. Imena vrhovnih domena su standardizirana (.com, .org, .edu, itd + domene država). Računala koja pružaju DNS uslugu su DNS poslužitelji, koji su također organizirani hijerarhijski. DNS poslužitelj sadrži zapise o određenom broju računala unutar jedne ili više lokalnih mreža (DNS zone). Ukoliko se želi saznati IP adresa računala izvan zone, DNS poslužitelji kontaktira poslužitelj iz zone traženog računala i formira odgovor. Npr. internet web aplikacija koja kontaktira npr. www.hr web poslužitelj, u prvom koraku će kontaktirati DNS poslužitelji iz zone klijenta. Ovaj će mu odgovoriti IP adresom web (http) poslužitelji www. hr (161.53.166.1) koja će se koristiti u daljnoj komunikaciji s www.hr poslužiteljem. DNS imena računala koriste se u najvećem broju mrežnih aplikacija. Izravan kontakt se DNS poslužiteljem moguć je naredbom nslookup <IP ili DNS zapis>:

```
H:\>nslookup epic1.fesb.hr
Name:    duje.st.carnet.hr
Address:  161.53.30.3

Name:    epic1.fesb.hr
Address:  161.53.168.12
```

Ukoliko se upit postavlja za računalo izvan zone DNS servera (potpis servera je u prve dvije linije odgovora), odgovor je "Non-authoritive" tipa, odnosno dobiven je od DNS servera van zone računala koje je postavilo upit.

## 3.4 ARP protokol

ARP-*Adress Resolution Protocol* je protokol koji omogućuje dostavu datagrama mrežne razine (IP) računalu koje se nalazi na lokalnoj mreži Ethernet. ARP protokol uspostavlja vezu IP-MAC adresa, tako da ako je poznata IP adresa računala kojem se dostavlja IP datagram, ARP protokolom se doznaje njegova MAC adresa, formira Ethernet okvir s IP datagramom u podatkovnom dijelu okvira i MAC adresom odredišnog računala u zaglavlju Ethernet okvira. Svako računalo koje se nalazi na lokalnoj mreži održava listu parova IP-MAC adresa (ARP cache), koja je dostupna naredbom arp –a. Kod formiranja Ethernet okvira najprije se pretražuje ARP cache, ukoliko se tu ne pronađe tražena MAC adresa, emitira se broadcast upit, na kojeg će odgovoriti ono računalo koje ima traženu IP adresu. Odgovor se sastoji od para IP-MAC adrese i sprema se u ARP cache, jer je velika vjerojatnost da će nam uskoro opet trebati. RARP - reverzni ARP protokol ima suprotnu ulogu: za danu MAC adresu traži odgovarajuću IP adresu. DHCP protokol spomenut kasnije u vježbi je poboljšanje RARP protokola koje omogućuje automatsku konfiguraciju računala kod spajanja na mrežu.

```
H:\>arp -a

Interface: 141.29.126.45 --- 0x10003
  Internet Address      Physical Address      Type
  141.29.126.20         00-03-47-b2-2e-df     dynamic
  141.29.126.21         00-03-47-b2-2e-ca     dynamic
  141.29.126.22         00-02-b3-c8-64-8a     dynamic
  141.29.126.254        00-0c-ce-98-b7-00     dynamic
```

Prethodni primjer prikazuje primjer sadržaja ARP cachea. Vidimo da je u prethodne dvije minute (Windows 2000/XP životni vijek ARP zapisa) računalo slalo IP pakete na IP adrese 141.29.126.20, .21, .22 i .254.

## *3.5 Podmreže*

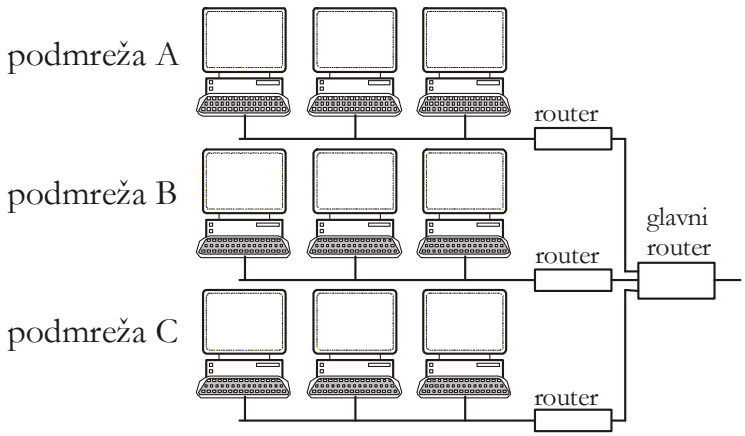
Funkcioniranje velikih mreža (klase A, B), kao i upravljanje njima, pojednostavnjuje se razbijanjem na podmreže. Princip je jako jednostavan: Dio IP adrese koji identificira računalo razdvaja se u dva dijela, od kojih gornji dio predstavlja podmrežu, a ostatak adresu računala.

Uzmimo za primjer B klasu: 16 bita koji adresiraju računalo možemo razbiti na dva dijela tako da npr. 8 važnijih bita predstavljaju podmrežu, a ostalih 8 bita dresu računala: Na taj način smo veliku mrežu B klase s do 64k računala razbili na 256 podmreža s do 254 računala. Parametar koji definira podjelu na podmreže je mrežna maska: 32-bitna varijabla koja se sastoji od bloka jedinica i nula: dio s jedinicama definira dio IP adrese koji definira mrežu i podmrežu, a dio s nulama adresu računala. I ona se jednostavno zapisuje u dotted quad formatu, ili još jednostavnije brojem "mrežnih bita", npr. 161.53.0.0/24.

| | | | | |
|---|---|---|---|---|
| 161 | 53 | 168 | 12 | IP adresa |
| 255 | 255 | 255 | 0 | mrežna maska |
| 161 | 53 | 168 | 0 | adresa podmreže |

**Sl. 2. Podjela na podmreže**

Slika prikazuje opisani slučaj: AND operacijom između IP adrese i mrežne maske dobije se rezultat - adresa podmreže, koja se koristi kod usmjeravanja paketa na lokalnoj mreži. Postupak je potpuno transparentan, odnosno IP adrese se ne mijenjaju, već se samo olakšava rukovanje paketima na mreži.




**Sl. 3. Primjer mreže podijeljene na tri podmreže**

Prikazana mreža sastoji se od tri podmreže A, B i C. Svaka podmreža sadrži router, koji je povezan na glavni router. Router (usmjernik) je mrežni uređaj koji ima dva ili više priključaka, i tablicu usmjeravanja na temelju koje određuje na koji će od svojih priključaka proslijediti (forward) pridošli IP datagram. Kada paket dođe na glavni router on obavlja AND operaciju odredišne IP adrese i mrežne maske. Dobiveni rezultat određuje podmrežu na kojoj se nalazi odredišno računalo.

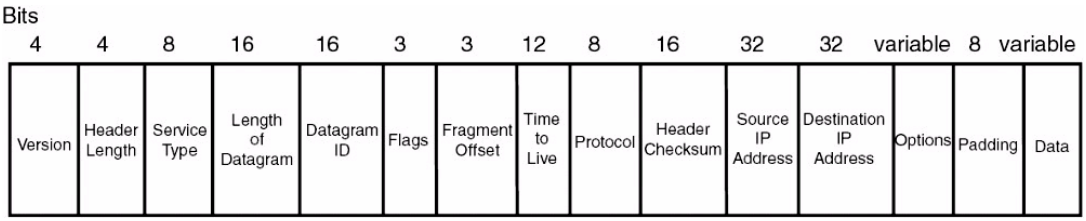
Podjela na klase izabrana je u počecima razvoja Interneta, pri čemu su odluke o broju računala u pojedinoj klasi donesene po kriterijima koji su tada bili aktualni: podjela po oktetima

omogućuje jednostavnu obradu paketa kod usmjeravanja. no problemi su nastali kod naglog rasta mreže. Većina organizacija kod spajanja na Internet je uzimala B klasu jer im se ograničenje od 254 adrese činilo premalenim. B klasa nudi ~64 k adresa koje su najčešće ostale slabo iskorištene (po nekim starijim istraživanjima više od polovice mreža B klase imale su manje od 50 priključenih računala. Tako smo došli do situacije da je adresni raspon od 32 bita IPv4 adresa skoro potrošen, a nije ni približno iskorišten.

Do prelaska na IPv6 protokol i 128 bitno adresiranje koriste se dva rješenja nedostatka IP adresa: CIDR adresiranje i NAT protokol. CIDR se temelji na dodjeljivanju IP adresa u manjim blokvima (1024, 2048...) što je prikladno rješenje, ali jako otežava usmjeravanje paketa, dok je NAT protokol, koji će detaljnije biti opisan u sljedećim vježbama, "hack" koji se masovno koristi, ali krši neke osnovne principe ISO-OSI modela.

## *3.6 IPv4 protokol*

Zaglavlje IPv4 protokola prikazano je na sljedećoj slici:




**Sl. 4 IPv4 datagram**

Karakteristična polja:

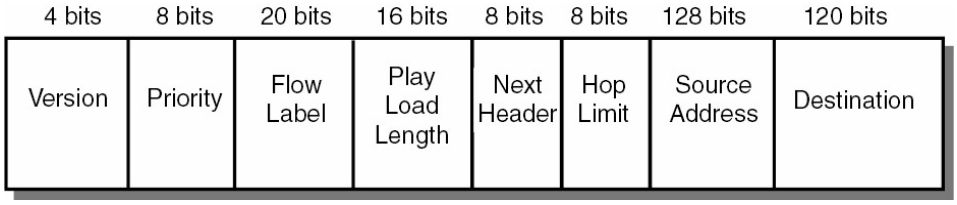
- Version – verzija IP protokola (4)
- Header Length – duljina zaglavlja (ovisi o postojanju opcija)
- Service type – definira kvalitetu usluge
- Length of datagram – ukupna duljina datagrama, maksimalno do 65535 okteta.
- Identification – identifikacija datagrama koja omogućuje sastavljanje fragmentiranih datagrama.
- Flags: DF – dont fragment - zabrana fragmentiranja datagrama; MF – more fragments - postavljen za sve osim posljednjeg fragmenta.
- Fragment offset – Pomak fragmenta unutar originalnog datagram omogućuje spajanje fragmentiranih datagrama.
- Time-to-live – datagram se emitira s vrijednošću 255 i na svakom se čvorištu umanjuje za 1, kako bi se zaustavilo datagrame koji kruže mrežom bez prestanka.
- Protocol – definira protokol prijenosne razine (najčešće TCP ili UDP).

## *3.7 IPv6 protokol*

IPv4 protokol koji je u upotrebi već 30-tak godina osim problema s adresiranje ima i znatna ograničenja vazana uz aplikacije koje se danas koriste na Internet mreži, u prvom redu pitanje sigurnosti i real-time usluga (audio i video sadržaji koji zahtijevaju konstantno, a ne varijabilno kašnjenje u prijenosu podataka). Treći problem je složena obrada IP opcija (dodaci IP zaglavlju koji se koriste kod različitih upravljačkih funkcija koje nije moguće riješiti unutar IP zaglavlja).

IPv6 adrese su 128 bitne što omogućava otprilike $3.4\times10^{38}$ različitih adresa. Ne koristi se dotted format već se adrese zapisuju kao 8 grupa od po 4 heksadecimalne znamenke, odvojene dvotočkama (npr. 2001:0db8:85a3:08d3:1319:8a2e:0370:7334) i DNS ekvivalentom. Kada se IPv6 adresa piše u sklopu URL-a, stavlja se u kvadratne zagrade radi izbjegavanja zamjene s brojem porta (prijenosna razina), koji se od IP adrese odvaja također dvotočkama (npr. http://[2001:0db8:85a3:08d3:1319:8a2e:0370:7344]:443/)

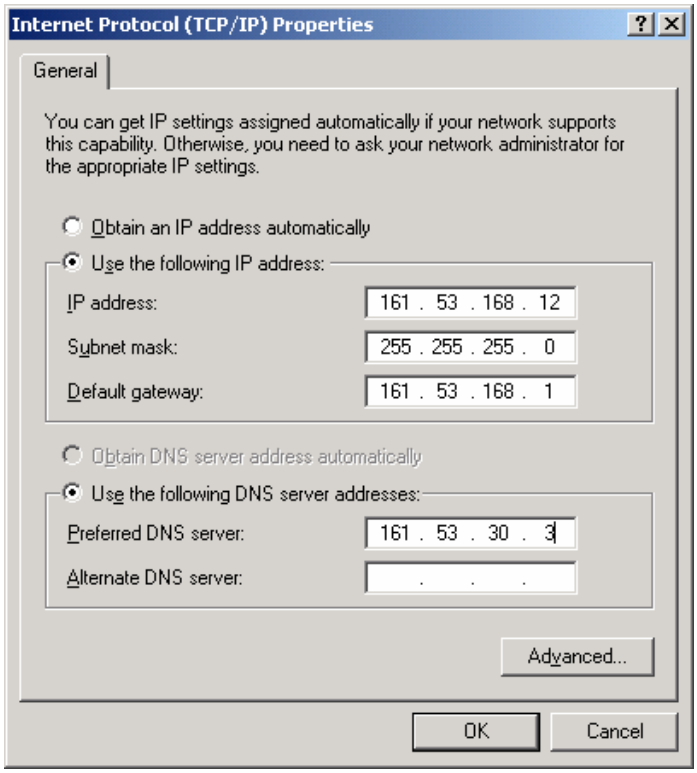
Kao posebnost, IPv6 protokol ne koristi polje zaštitne sume (checksum) jer zahtijeva dosta vremena kod obrade datagrama, a i smatra se suvišnim, jer se koristi i na nižim (npr. 802.x) ali i na višim slojevim (npr. TCP).




**Sl. 5 IPv6 zaglavlje**

## 3.8 Podešavanje postavki mreže računala u lokalnoj mreži

Konfiguracija računala u lokalnoj mreži može se obaviti ručnim podešavanjem parametara IP adrese, mrežne maske, itd ili automatski kod priključenja računala na lokalnu mrežu koja podržava takav način rada (DHCP – Dynamic Host Configuration Protocol).




**Sl. 6 Statička konfiguracija mrežnih parametara**

Default gateway IP adresa je adresa usmjernika koji usmjerava pakete koji nisu dio prometa na lokalnoj mreži (Internet promet). DNS server je IP adresa lokalnog DNS poslužitelja.

Dinamička konfiguracija sastoji se u uključivanju "Obtain an IP address..." opcije (vidi sliku 6.). Kod priključenja računala na mrežu kontaktirati će se DHCP server koji će nam proslijediti parametre koje bi inače podesili ručno. Ova konfiguracija koristi se kod npr. modemskog, GPRS, UMTS, ... pristupa Internetu i lokalnih mreža koje sadrže računalo koja obavlja konfiguraciju ostatka mreže (DHCP server).

Dodatna podešavanja eventualno su potrebna ovisno o konfiguraciji mreže: čest je slučaj da je izlaz na Internet riješen preko "proxy" računala, koje sprema često korištene podatke i na taj način smanjuje opterećenje mreže. Osim toga druge funkcije proxy računala su zaštita od neželjenih sadržaja, kontrola prometa koji generiraju korisnici i sl.

## 3.9 Radne grupe i domene

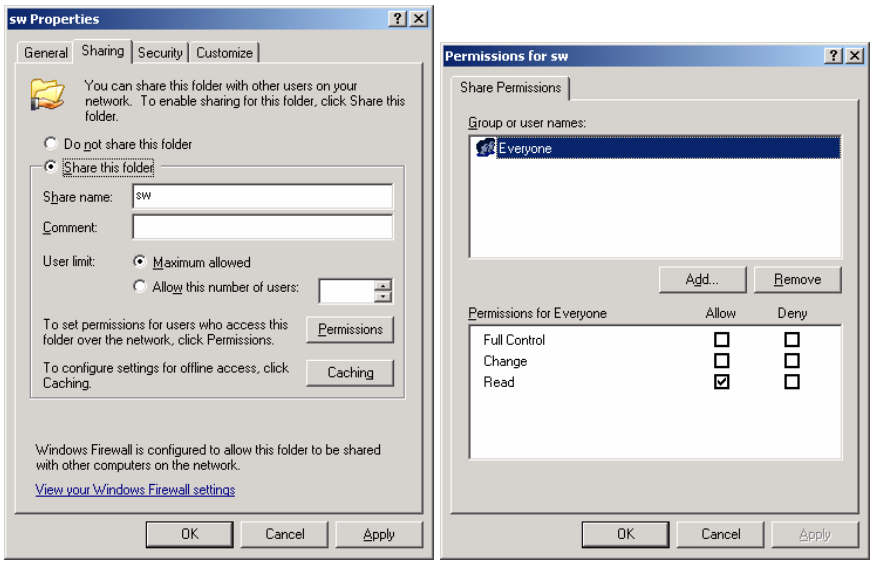
Dva dominantna načina organizacije računala s Windows operativnim sustavom su radne grupe (WORKGROUP) i domene (DOMAIN).

Ukoliko se radi o radnim grupama, korisnikov profil (razne postavke njegovog računa poput lozinaki, raspored menija i sl.) se nalazi na samom računalu. Osim workgroup ovakva organizacija se često naziva i pee-to-peer.

Kod domenske organizacije jedno od računala u mreži (domenski kontroler) drži podatke o korisnicima te se korisnik može koristiti bilo kojim od računala u mreži s svojim korisničkim imenom i lozinkom).

## *3.10 Dijeljenje resursa računala na lokalnoj mreži*

Dijeljenje resursa (direktoriji, pisači, itd) može biti slobodno (public) ili ograničeno. Primjer pokazuje definiranje direktorija na lokalnim hard disku koji će biti dostupan ostalim korisnicima iz lokalne mreže. Odabirom Sharing And Security opcije direktrorija otvara se izbornik za definiranje opcija dijeljenog direktorija:




**Sl. 7 Dijeljenje lokalnog direktorija na lokalnoj mreži**

Početne *Permissions* postavke dozvoljavaju dijeljenje direktorija svim korisnicima, no moguće je ograničavanje po korisnicima i načinu spajanja (samo čitanje, čitanje i pisanje, itd). Pristup računalima u lokalnoj mreži i njihovim dijeljenim resursima moguć je pretraživanjem lokalne mreže (My Windows Places -> Workgroups -> Ime računala), ili izravno preko IP adrese: \\<IPadresa>.

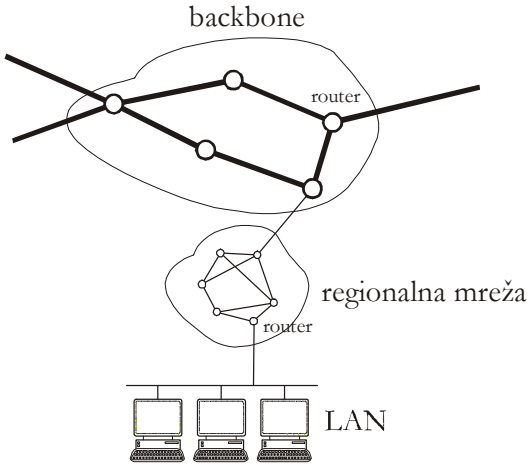
# 4. Usmjeravanje na Internetu

Usmjeravanje kod paketskih mreža ima primarnu ulogu osigurati dostupnost od izvorišta do odredišta toka podataka, a sekundarnu pri tome utjecati na optimalno iskorištenje mreže i kvalitetu usluge. *Usmjernik* (router) je sustav s više mrežnih priključaka, koji svoj rad temelji na *algoritmu/protokolu, usmjeravanja* (routing algorithm/protocol), Algoritam usmjeravanja određuje na koji od priključaka proslijediti datagram koji pristigne na jedan od njih (forwarding). Odluka o usmjeravanju donosi se na temelju sadržaja *tablice usmjeravanja* (routing table).

## *4.1 Arhitektura usmjeravanja na Internetu*

Prvobitno su usmjernici unutar Interneta bili organizirani hijerarhijski, što je bilo naslijeđe ranije ARPANET arhitekture. Postojao je centralni sustav (jezgra) mreže, kroz čije su usmjernike (core gateways) prolazile informacije o usmjeravanju među svim mrežama Interneta. Rastom Interneta, naglo je rasla i količina usmjerivačkih informacija koje je jezgra trebala obraditi, te je to postao i glavni nedostatak hijerarhijskog modela.

Novi model usmjeravanja zasniva se na ravnopravnim nezavisnim (autonomnim) sustavima. Svaki nezavisni sustav sastoji se od grupe mreža koje su pod istom administrativnom upravom.




**Sl. 8 Arhitektura Internet mreže**

- **osnovna mreža** (Backbone), povezuje vanjske usmjernike i predstavlja najvišu razinu. Paketi IP protokola isporučuju se optimalnim putem do usmjernika preko kojega je dostupna osnovna podmreža odredišta.
- **osnovna podmreža** (Autonomous system) predstavljena je s jednom ili više adresnih klasa, a karakterizirana je vlastitom administracijom adresa. Dijeli se na podmreže s fiksnom (klase) ili varijabilnom (adresna maska) mrežnom adresom. Najčešće je ostvarena jednostavnom do srednje složenom mrežom unutrašnjih usmjernika na koje su povezane podmreže. IP paketi se usmjeravaju optimalnim putem do usmjernika preko kojega je dostupna podmreža odredišta.
- **podmreža** (Subnetwork) je dio Interneta koji obuhvaća jednu zonu prostiranja (broadcast domain) lokalne mreže, a čija je mrežna IP adresa određena klasom ili mrežnom maskom. Podmreža je s osnovnom podmrežom povezana najčešće samo jednim usmjernikom, koji za računala podmreže predstavlja *osnovni usmjernik* (Default Gateway). Pakete koji dolaze na

podmrežu osnovni usmjernik pakira u okvire s MAC adresom odredišta i prosljeđuje ih lokalnom mrežom. Pakete koji idu van iz podmreže, izvorište pakira u okvire s MAC adresom osnovnog usmjernika, koji će ih proslijediti dalje kroz osnovnu podmrežu. Paketi kojima je izvorište i odredište na istoj podmreži (unutar granica zone prostiranja), odredište pakira u okvir s MAC adresom odredišta i šalje ga direktno odredištu. U sva tri slučaja, pripadnost paketa podmreži određuje se na osnovu mrežnog dijela IP adrese, a pretvorba IP adrese odredišta ili usmjernika u MAC adresu obavlja se korištenjem ARP protokola.

S obzirom na takvu podjelu razlikujemo sljedeće vrste usmjernika:

- **vanjske usmjernike** koji obavljaju usmjeravanje i razmjenjuju informacija o usmjeravanju između različitih nezavisnih sustava. Takvi sustavi koriste vanjske usmjerivačke protokole (npr. BGP-*Border Gateway Protocol,* ).
- **unutrašnje usmjernike** koji usmjeravaju pakete unutar nezavisnih sustava. Takvi sustavi koriste unutrašnje usmjerivačke protokole (npr. RIP-*Routing Information Protoco,* OSPF-*Open Shortest Path First,* EIGRP-*Enhanced Interior Gateway Routing Protocol*).

Algoritmi/protokoli usmjeravanja se također mogu podijeliti u sljedeće dvije grupe:

- **statički (neadaptivni) algoritmi** ne uzimaju u obzir topologiju mreže, njeno opterećenje i sl. već se put paketa od točke A do točke B određuju unaprijed i postavlja kod pokretanja usmjernika.
  - *Shortest Path algoritam* - Veze između usmjernika opisuju se karakterističnim parametrima: udaljenost, brzina, kašnjenje, cijena, i sl. Mijenjanjem težine koja se pridaje jednom od ili više navedenih parametara određuje se najkraći put po zadnim parametrima.
  - *Flooding* - Ovaj algoritam se sastoji u prosljeđivanju primljenog paketa na sve priključke osim izvorišnog. Kako se na taj način generira golem promet kopija datagrama, koriste se razne optimizacije kako bi se taj problem smanjio.
- **adaptivni algoritmi** uzimaju u obzir parametre rada mreže, te u skladu s njima mijenjaju sadržaj tablice usmjeravanja.
  - *Distance Vector Routing* - Svaki usmjernik održava tablicu vektora, koja sadrži "udaljenost" do odredišta i preko kojeg priključka ga je moguće dosegnuti. Usmjernici međusobno komuniciraju i mijenjaju tablicu vektora u skladu s promjenama u radu mreže. Primjeri ovog algoritma su EIGRP, te RIP - prvotni algoritam usmjeravanja Interneta, koji se i danas koristi, ali na manjim mrežama.
  - *Link State routing* - "Udaljenost" iz prethodnog algoritma podrazumijevala je duljinu reda čekanja (queue) u određenom smjeru. S uvođenjem više linija različitih brzina, ali i njegovih drugih slabosti 1979. se prelazi na Link State Routing algoritme (npr. OSPF), kod kojeg svaki usmjernik ima nekoliko zadataka:
    - upoznati susjedne usmjernike i njihove adrese, odrediti kašnjenje ili cijenu do svakog od njih,
    - konstruirati paket s podacima iz prvog zadatka i poslati ga ostalim usmjernicima (flooding)
    - odrediti najkraću putanju do svakog svih ostalih usmjernika.

## *4.2 Tablice usmjeravanja i RIP*

Da bi olakšali traženje optimalnog puta usmjernici održavaju tablice usmjeravanja. One sadrže niz informacija potrebnih za usmjeravanje i odabir najboljeg puta, primjerice:

- parove *adresa_odredišta-sljedeći_usmjernik* koji kazuju usmjerniku da se odgovarajuće odredište može dosegnuti na optimalan način ako se pošalje na navedeni slijedeći usmjernik. Dakle, usmjernici ne drže informacije o potpunom putu paketa već sadrže samo prvi slijedeći korak na tom putu. Odredište može biti mreža, računalo ili posebna oznaka koja označava osnovni usmjernik.
- mrežnu masku za određeno odredište
- metriku - koja definira mehanizam za uspoređivanje kakvoće pojedinih smjerova.
- ime mrežnog sučelja koje koristi navedeni smjer
- da li je smjer ispravan, koristi li usmjernike ili je vezan izravnom vezom i sl.
- vrijeme kada je pojedini smjer posljednji put ažuriran

Unutar tablice usmjeravanja postoji posebna adresa kojom se definira osnovni smjer (default route) i najčešće je to adresa koja sadrži sve nule (0.0.0.0). Na osnovni smjer šalju se svi paketi za koje se ne može pronaći odredište unutar tablice usmjeravanja (bilo bi nepraktično da svaki usmjernik ima u tablici usmjeravanja sva moguća odredišta). Osnovni smjer definiran je adresom osnovnog usmjernika (default gateway). Dakle, kada paket stigne na neki usmjernik, on provjerava tablicu usmjeravanja ne bi li našao odgovarajuću odredišnu adresu (računala ili njegovu mrežnu adresu) i ako je ne pronađe, šalje je na vlastiti osnovni usmjernik.

**RIP** (Routing Information Protocol) se početkom 80-ih godina počeo isporučivati s BSD inačicom UNIX operativnog sustava (routed program). Danas je to još vrlo popularan unutrašnji protokol za usmjeravanje. Verzija 1 je formalno definirana u RFC 1058, a posljednja, verzija 2, u RFC 2453. Postoji i verzija RIPng predviđena za upotrebu s IPv6 protokolom.

RIP omogućuje usmjernicima i računalima razmjenu informacija o usmjerivačkim smjerovima unutar Internet mreže. Zasniva se na algoritmu "vektora udaljenosti" i to tako da odabire smjer s najmanjim "brojem koraka" (brojem usmjernika koje paket treba proći na putu do odredišta) kao najbolji. Najduži prihvatljivi smjer unutar RIP usmjerivačke tablice može imati najviše 15 koraka (za >15 RIP smatra da se odredište ne može doseći). RIP pamti samo najbolji put do odredišta, tj. ako nova informacija nudi bolji smjer (manji broj koraka), nova informacija zamjenjuje staru. Kada neki RIP usmjernik detektira prekid jedne od svojih vlastitih veza on ažurira svoju tablicu (postavlja broj koraka za taj smjer na 16) i susjednim usmjernicima šalje vlastitu usmjerivačku tablicu. Svaki usmjernik koji primi ovu poruku ažurira vlastitu tablicu i šalje je dalje - promjena se propagira mrežom.

Za prijenos dijelova vlastite usmjerivačke tablice RIP koristi UDP datagrame. Svako računalo koje koristi RIP mora imati usmjerivački proces koji šalje i prima datagrame s UDP priključne točke 520. Svaki RIP IP paket može sadržavati do 25 vrijednosti iz tablice usmjeravanja, pa je maksimalna veličina paketa MTU=512. Ukoliko računalo nije usmjernik ono također može motriti ove RIP poruke, ali ne šalje vlastitu tablicu. To je tzv. "tihi " RIP proces (silent RIP). RIP ne osigurava mehanizam za prijavu pogreški izvorišnom računalu kada dođe do pogreški pri usmjeravanju. Tu funkciju obavlja ICMP protokol.

RIP proces svakih 30 sekundi šalje čitavu usmjerivačku tablicu svojim susjedima. Ako nakon 180 sekundi usmjernik nije dobio potvrdu smjera u tablici, on proglašava smjer neispravnim (broj koraka postavlja >15)., a ukoliko nakon daljnjih 120 sekundi (najčešće) ne dobije potvrdu smjera, on ga briše iz tablice usmjeravanja. Ukoliko usmjernik detektira prekid neke veze on, po ažuriranju vlastite tablice, odmah šalje svoju tablicu susjednim usmjernicima ne čekajući istek 30 sekundi (triggered update).

Osim ograničavanja najvećeg broja koraka na 15, RIP protokol uključuje i niz dodatnih svojstava koja omogućuju stabilniji rad:

- *Podijeljena obzorja (Split Horizons)* - Ovo svojstvo proizlazi iz činjenice da nije korisno slati informaciju o smjerovima u onom smjeru iz kojeg smo tu informaciju i primili. Ovim sprječavamo stvaranje usmjerivačkih petlji između 2 usmjernika.
- *Ažuriranje prekinutih smjerova (Poison Reverse Updates)* - Ovo svojstvo namijenjeno je nalaženju i sprječavanju usmjerivačkih petlji između tri ili više računala, a temelji se na tome da povećavanje broja koraka za pojedini smjer obično ukazuju na pojavu usmjerivačke petlje. Stoga se pri uočavanju ovakvih smjerova šalju paketi (Poison reverse update poruke) koje brišu takve smjerove iz usmjerivačkih tablica.
- *Zadržavanje promjene izbrisanih smjerova (Hold-downs)* - Budući da ažuriranje smjerova koji su prekinuti ne dolazi istovremeno na svaki usmjernik, može se dogoditi da usmjernik koji još nije obaviješten o prekidu veze šalje redovite poruke u kojima navodi da je takav smjer još ispravan. Usmjernik koji primi takvu poruku, a već je obaviješten o prekidu tog smjera, neće odmah takav smjer staviti u svoju tablicu već će određeno vrijeme zadržavati promjenu.

Praćenje putanje datagrama do odredišta moguće je u jednostavnijim slučajevima naredbama tracert (traceroute) ili pathping. Primjer prikazuje praćenje putanje paketa sa računala spojenog preko UMTS mobilne veze na CARNet prema web serveru www.hr. U donjem dijelu prikazana su kašnjenja na pojedinom dijelu putanje paketa. Pathping i tracert koriste ICMP poruke ping, koje se na nekim mrežama (npr, CMU) blokiraju pa nije moguće praćenje putanje na ovaj način.

```
H:\>pathping www.hr

Tracing route to www.hr [161.53.19.201]
over a maximum of 30 hops:
  0  193.198.165.17
  1  192.168.2.1
  2  192.168.2.12
  3  vipnet26-167.mobile.CARNet.hr [193.198.167.26]
  4  CN-FER-ES.zg.core.CARNet.hr [193.198.229.10]
  5  161.53.16.14
  6  www.hr [161.53.19.201]

Computing statistics for 150 seconds...
            Source to Here   This Node/Link
Hop  RTT    Lost/Sent = Pct  Lost/Sent = Pct  Address
  0                                           193.198.165.17
                                     0/ 100 =  0%   |
  1  196ms     0/ 100 =  0%     0/ 100 =  0%  192.168.2.1
                                     0/ 100 =  0%   |
  2  193ms     0/ 100 =  0%     0/ 100 =  0%  192.168.2.12
                                     0/ 100 =  0%   |
  3   197ms         0/  100  =    0%         0/  100  =    0%   vipnet26-167.mobile.CARNet.hr
[193.198.167.26]
                                     0/ 100 =  0%   |
  4   196ms         1/  100  =    1%         1/  100  =    1%   CN-FER-ES.zg.core.CARNet.hr
[193.198.229.10]
                                     0/ 100 =  0%   |
  5  212ms     2/ 100 =  2%     2/ 100 =  2%  161.53.16.14
                                     0/ 100 =  0%   |
  6  189ms     0/ 100 =  0%     0/ 100 =  0%  www.hr [161.53.19.201]

Trace complete.
```

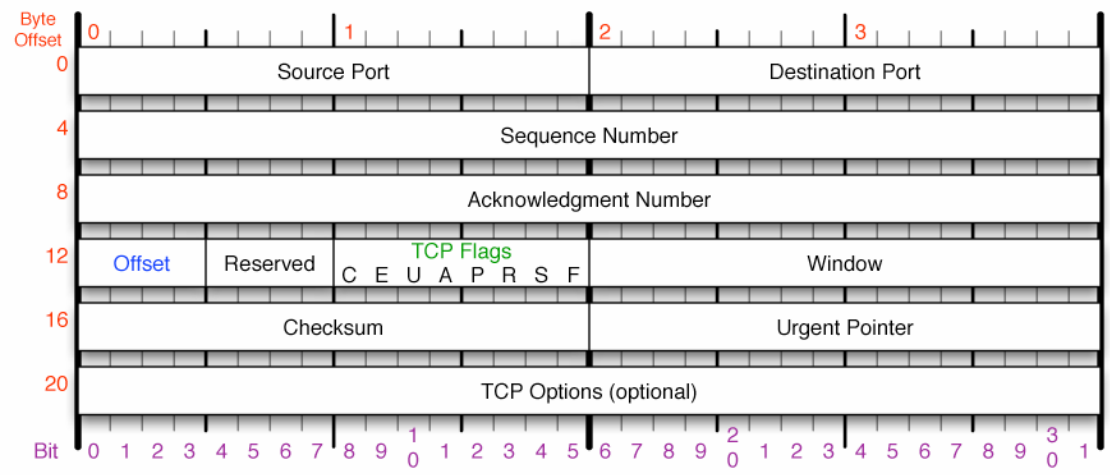
# 5. Prijenosna razina TCP/IP skupa protokola

Prijenosna razina TCP/IP skupa protokola koristi usluge IP razine za realizaciju protokola prijenosne razine. Dva najčešća protokola u upotrebi su TCP i UDP. U okviru ove vježbe simulacijom će se pokazati ponašanje različitih varijanti TCP protokola.

## *5.1 TCP*

TCP (*Transmission Control Protocol*) je spojevni protokol koji omogućuje pouzdanu komunikaciju Internet aplikacija korištenjem nepouzdanog (best-effort) IP protokola. TCP procesi na dva računala u Internet mreži komuniciraju razmjenom segmenata. Računalo koje šalje segment podataka formira segment određene veličine i prosljeđuje ga IP razini koji ga eventualno razdijeli na više IP datagrama i šalje ga odredištu. TCP proces na prijemnom računalu ima zadatak formirati originalni segment od jednog ili više primljenih datagrama i proslijediti ga aplikaciji.

TCP veza između dva računala na Internetu uspostavlja se korištenjem krajnjih točaka na oba računala. Ove krajnje točke nazivamo **priključnicama (socket)**. Svaka priključnica jedinstveno je određena *IP adresom računala* i *priključnom točkom (port)*. Priključna točka identificira proces koji šalje ili prima podatke. Veza je jedinstveno određena parom priključnica.




**Sl. 1 TCP zaglavlje**

Polja **Source port** i **Destination Port** u TCP zaglavlju su duljine 16 bita, dakle omogućuju 64k vrijednosti. Portovi 0-1023 su *statički* (well-known) i pridruženi su najčešćim Internet uslugama; portovi 1024-49151 su registrirani (registered), a 49151-65535 su *dinamički*/privatni potrovi.

Uzmimo za primjer WEB (HTTP) preglednik: Klijentskoj aplikaciji dodjeljuje se dinamička priključna točka, koja zajedno s IP adresom klijenta određuje klijentovu priključnicu. DNS uslugom određuje se IP adresa poslužitelja iz dane web adrese (http://www...). Vrijednost priključne točke na poslužitelju postavi se sukladno korištenoj usluzi (80 za http). Time je određena i priključnica na strani poslužitelja. Dakle, u TCP zaglavljima segmenata koje klijent

šalje poslužitelju nalazi se vrijednost Destination Port 80, a Source Port vrijednost dodijelio je operativni sustav (dinamički port).

| Port | Protokol | Usluga |
|---|---|---|
| 21 | FTP | Prijenos datoteka |
| 22 | SSH | Razmjenu podataka preko "sigurnog kanala" |
| 23 | Telnet | Rad na udaljenom računalu |
| 25 | SMTP | e-mail |
| 80 | HTTP | World Wide Web |
| 110 | POP3 | udaljeni e-mail pristup |

**Sl. 2 Primjeri portova za često korištene usluge**

Polje **Sequence Number** (SEQ) označava poziciju segmenta u originalnom bloku podataka, a **Acknowledgement Number** (ACK) se koristi za potvrdu ispravnog prijema paketa u suprotnom smjeru. Ukoliko računalo 1 šalje računalu 2 segment od 100 bajta podataka sa SEQ = 0 (dakle, radi se o početnih 100 bajta podataka), računalo 2 će odgovoriti s ACK = 101, odnosno potvrđuje ispravan prijem segmenta s prvih 100 bajta podataka i očekuje od računala da slijedeći segment sadrži podatke od 101 bajta nadalje. Ako se pozitivna potvrda ne primi do isteka vremena retransmisije, podatak se automatski ponovo šalje.

Sequence number i Acknowledgement Number polja TCP-u omogućuju:

- detekciju i oporavak od gubitka u prijenosu,
- da ispravno poreda segmente kod poruka koje se prenose u više datagrama i mogu stići do odredišta redoslijedom različitim od redoslijeda kod slanja ,
- eliminiranje dupliciranih segmenata (koji nastaju kao posljedica Flooding algoritma usmjeravanja na nekoj od mreža preko kojih datagram prođe).

Polje **TCP flags** sadrži podatke o vrsti i sadržaju segmenta. Polje se sastoji od 8 zastavica (flag) - bitova koji kada su postavljeni u jedinicu označavaju:

URG paket sadrži hitnu poruku, a polje Urgent Pointer pokazuje na kraj hitnih podataka

ACK segment nosi potvrdu čiji se broj nalazi u polju Acknovledgement Number

PSH predajnik zahtijeva trenutnu isporuku pristiglih podataka na prijemnoj strani (push)

RST resetiranje veze

SYN sinhronizacija Sequence Number polja

FIN pošiljatelj nema više podataka za slanje

Najčešće se TCP segment formira od 1460 bajta podataka kako bi stao unutar jednog Ethernet okvira standardne veličine 1500 bajta. 40 bajta razlike čine TCP i IP zaglavlja. Slanje manjih količina podatka moguće je postavljanjem URG (Urgent) bita. Veličina bloka podataka koji se šalje definirana je **Urgent Pointer** poljem.

TCP omogućava prijemniku upravljanje količinom podataka koje smije odaslati predajnik. Poljem **Window,** koje služi za *kontrolu toka*, određuje se količina podataka koju prijemnik može primiti bez gubitaka. Sa svakom potvrdom (ACK), prijemnik šalje i veličinu prozora (RWIN, receiver window). Najveći prozor je 65536 okteta (polje ima 16 bita).

TCP protokol implementiran je u operacijskom sustavu, te aplikacijama (korisničkim procesima) nudi određeni skup funkcija. Funkcije se razlikuju kod poslužitelja i klijenta.

Na poslužitelju, kod uspostave TCP veze:

1. SOCKET funkcija kreira socket. Vrijednost porta ovisi o vrsti usluge koju će poslužitelj nuditi klijentima.
2. Nakon poziva BIND funkcije socket je povezan s IP adresom i omogućava spajanje klijenata.
3. LISTEN funkcija obrađuje pozive jednog ili više klijenata koji pokušavaju uspostaviti vezu s poslužiteljem.
4. Nakon dolaska zahtjeva (CONNECT) od klijenta ACCEPT funkcija uspostavlja vezu s klijentom.

Na klijentskoj strani:

1. SOCKET funkcijom kreira se socket. Vrijednost Port dodjeljuje operativni sustav iz raspona 1023 – 64k.
2. CONNECT pozivom uspostavlja se veza na udaljeni poslužiteljski socket.

Uspostava TCP veze zahtijeva razmjenu ukupno tri paketa između računala koja komuniciraju (***three way handshaking***). Obično ovaj postupak pokreće jedno računalo, dok drugo odgovara na njega (slika 3):

- Računalo 1 koje inicira vezu šalje segment podataka sa postavljenim SYN bitom i određenom vrijednošću SEQ=x polja.

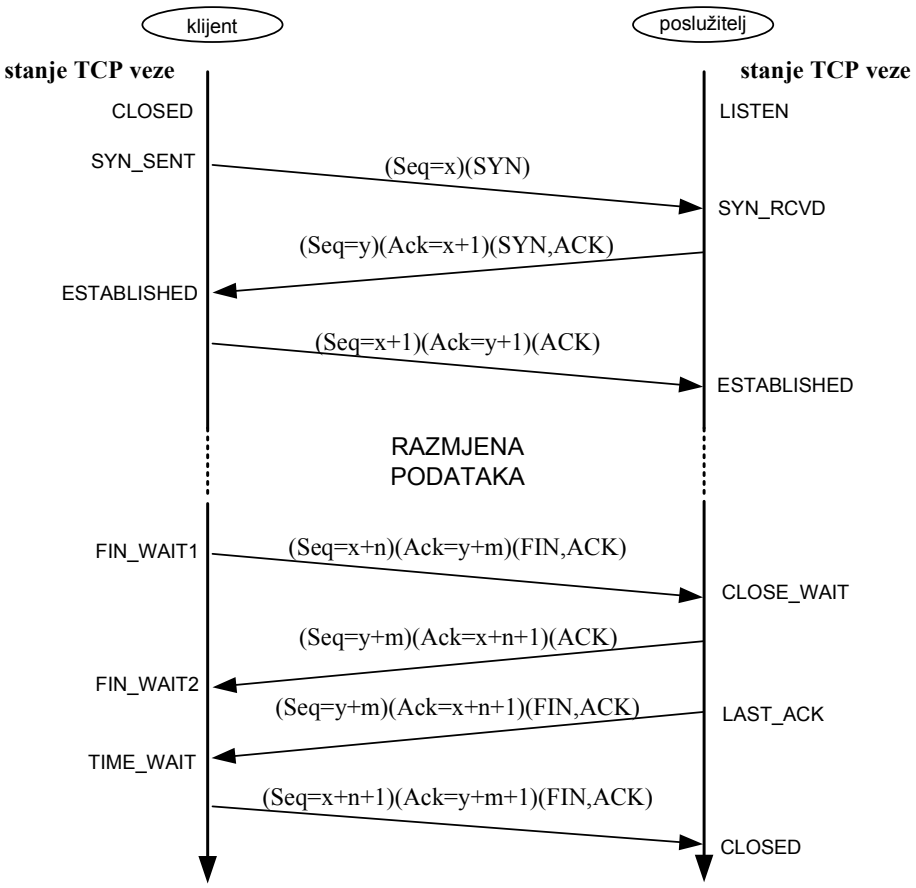
- Računalo 2 odgovara slanjem segmenta s postavljenim SYN i ACK bitom, vlastitom vrijednošću SEQ = y i potvrdom prijema prethodnog segmenta ACK = x+1.

- Računalo 1 odgovara slanjem segmenta sa SEQ = x+1, i potvrđuje prijem prethodnog segmenta postavljenim ACK = y+1.

Nakon uspostave veze klijent i poslužitelj razmjenjuju podatke SEND i RECEIVE funkcijama.

Po završetku slanja podataka, TCP veza se raskida razmjenom 3 ili 4 segmenta (slika 3). Strana koja želi prekinuti vezu šalje segment s postavljenom FIN zastavicom. Uobičajena je situacija da klijent želi prekinuti vezu, a kasnije i poslužitelj prekida vezu. Nakon zatvaranja klijentske strane poslužitelj i dalje može slati podatke. U trenutku kada i poslužitelj želi zatvoriti vezu ponavlja istovjetan postupak, tj. šalje segment s postavljenom FIN zastavicom.

Poslužitelj (npr. HTTP poslužitelj) najčešće prihvaća više klijenata odjednom. U tom slučaju pojedine klijente poslužitelj razlikuje po (IP adresi i) polju Source Port, čiju vrijednost na klijentskoj strani dodjeljuje operacijski sustav među vrijednostima >1023 (dinamičke priključne točke).




**Sl. 3 Uspostava, prijenos podataka i prekid veze TCP protokola**

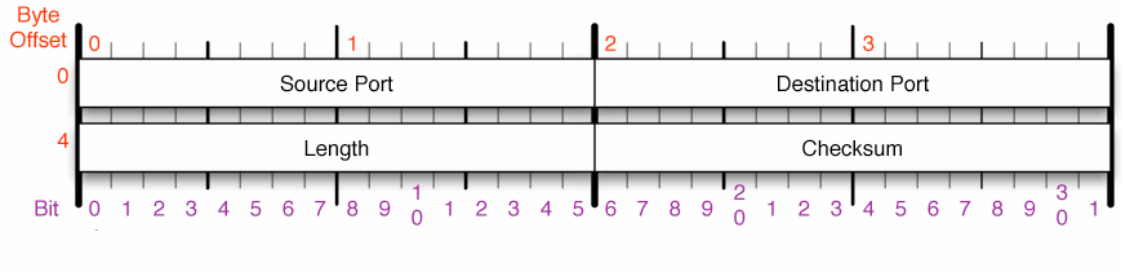
TCP veza može biti u jednom od sljedećih stanja:

| **Stanje:** | **Značenje:** |
|---|---|
| CLOSED | Veza je neaktivna (raskinuta) |
| LISTEN | Stanje čekanja zahtjeva za vezu |
| SYN-SENT | Poslan je zahtjev za vezu; čeka se da druga strana odgovori zahtjevom za vezu |
| SYN-RECEIVED | Primljen je zahtjev za vezu; čeka se potvrda zahtjeva za vezu |
| ESTABLISHED | Stanje normalnog prijenosa podataka |
| FIN-WAIT-1 | Odaslan je zahtjev za raskidanje veze |
| FIN-WAIT-2 | Čeka se zahtjev za raskidanje veze od udaljenog TCPa |
| CLOSE-WAIT | Čekanje na zahtjev za raskidanje veze od lokalnog korisnika |
| CLOSING | Čeka se potvrda na poslani zahtjev za prekid veze |
| LAST-ACK | Čeka se potvrda na zahtjev za raskid veze od udaljenog TCPa |
| TIME-WAIT | Čeka se dva maksimalna vremena života segmenta (MSL), kako bismo se uvjerili da su svi zaostali segmenti stigli do udaljenog TCPa. Za to vrijeme se ne može ponovo uspostaviti veza između ove dvije priključnice. |

Održavanje TCP veze zahtijeva pamćenje više varijabli. One se pohranjuju u strukturi nazvanoj TCB (Transmission Control Block). TCB sadrži informacije o identifikatorima lokalne i udaljene priključnice, prioritetima i sigurnosti veze, pokazivačima na red za retransmisiju i tekući segment, te o varijablama vezanim za redne brojeve predaje i prijema podataka.

## 5.2 UDP

UDP (*User Datagram Protocol*) je bespojni protokol, dakle omogućava slanje podataka bez uspostave logičke veze između dva računala koja komuniciraju. Stoga se koristi za usluge kod kojih je bitnija jednostavnost rukovanja i brzina, od pouzdanosti prijenosa (npr. audio-video prijenos). UDP zaglavlje duljine je 8 bajta i osim polja za izvorišni i odredišni port ima još samo polje duljine i zaštitne sume.




**Sl. 4 UDP zaglavlje**

Primjer aplikacije koja koristi UDP je DNS usluga opisana u prethodnim vježbama. Klijent šalje DNS upit DNS poslužitelju, koji odgovara IP adresom za traženi DNS upit, ukupno dva segmenta podataka.

Lista trenutno otvorenih veza (UDP ili TCP) na obje strane komunikacije, kao i pripadajuće priključnice mogu se dobiti naredbom netstat. Primjer pokazuje ispis netstat naredbe s aktivnom vezom web pretraživača na www.hr stranice.

```
H:\>netstat

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    lab325.fesb.hr:1416    www.hr:http            ESTABLISHED
```

Prvi stupac prikazuje protokol prijenosne razine. Local i Foreign adrress su dvije priključnice (socket) koje međusobno komuniciraju. Priključnica na klijentu lab325.fesb.hr ima vrijednost priključne točke 1416 (dinamički port), a na poslužitelju 80 (http). Ukoliko se pokrene još jedan proces web pretraživača na istu adresu (www.hr), on će se spojiti na priključnu točku 80 na istom poslužitelju, ali s različitom vrijednošću priključne točke u Local Adress polju i to je parametar koji omogućava ispravnu razmjenu segmenata između poslužitelja i dva klijenta s iste IP adrese.

netstat naredba ima nekoliko zanimljivih opcija:

/b povezuje otvoreni socket s aplikacijom/procesom koji ga je kreirao;

/e ispisuje statistiku Ethernet prometa

/o ispisuje PID procesa koji koristi danu vezu

/s ispisuje statistiku po protokolima (IP, TCP, ICMP...)

## *5.3 RAZVOJ KONTROLE TOKA TCP PROTOKOLA*

U stanju uspostavljene veze prijenos podataka se obavlja razmjenom podatkovnih segmenata. Uslijed greške ili zagušenja na mreži može doći do gubitka segmenta. Stoga TCP koristi mehanizam *retransmisije* kako bi osigurao dostavu svakog segmenta. Potvrde su *kumulativne*, što znači da potvrda x-tog okteta podrazumijeva i potvrdu svih prethodnih.

Ako u određenom vremenu (**RTO, Retransmission Timeout**) ne dobije potvrdu, TCP ponovno šalje segment, računajući da je izgubljen. Zbog raznolikosti mreža u sustavu i širokog raspona uporabe TCP veza, ovo vrijeme se računa dinamički. Kvalitetan proračun tog vremena od ključnog je značenja za učinkovitost TCP veze. Proračuni se zasnivaju na vremenu potrebnom da stigne potvrda za odaslani paket. To se vrijeme naziva **vrijeme obilaska, RTT (Round Trip Time)**. RTT se stalno mijenja i ovisi o trenutnoj opterećenosti mreže.

Nazivni kapacitet mreže predstavlja maksimalnu količinu podataka koju mreža može prenijeti, a da ne nastupi zagušenje (congestion). *Relativno opterećenje mreže* opisuje faktor ρ:

$$\rho = \frac{ponudjeni\_promet}{kapacitet\_mreze}$$

**Zagušenje** nastaje kada faktor ρ u nekom vremenskom intervalu $[t_1, t_2]$ poprimi vrijednost $\rho \geq 1$. U ovisnosti o periodu trajanja, razlikujemo *trajna, periodična, privremena i trenutna zagušenja*.

**Kontrola toka** je osnovni mehanizam za izbjegavanje zagušenja kod mreža s prospajanjem paketa. Usmjeravanje prometa je za paketne mreže pomoćni postupak izbjegavanja zagušenja. *Prozorska kontrola* toka ograničava broj paketa u mreži, ali dozvoljava slanje praskova (burst) paketa. Nasuprot tome, *kontrola brzine* garantira jednoliki tok paketa, ali ne garantira broj paketa u mreži. Kontrola toka TCP protokola postiže se mehanizmom prozorske kontrole.

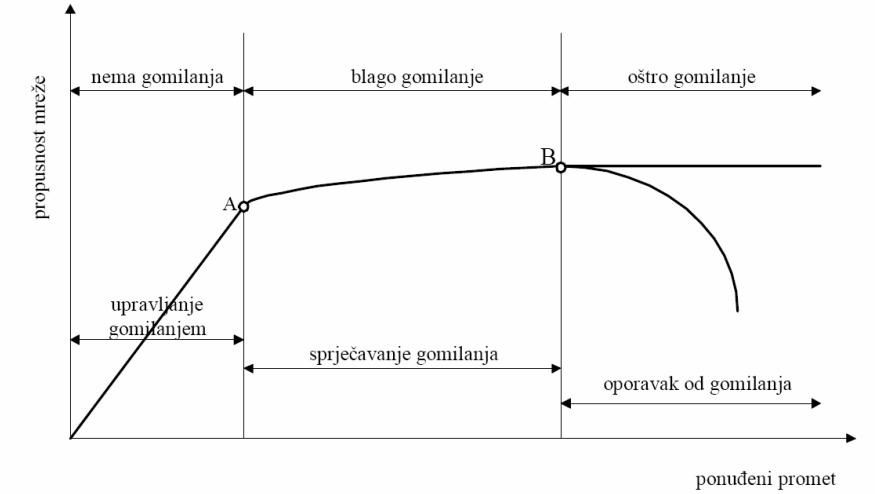
Suština mehanizma prozorske kontrole toka je u tome da se širinom prozora ograniči broj paketa koje izvorište može poslati dok ne primi potvrdu za prvi poslani paket. Paketi podataka putuju od izvorišta ka odredištu, dok potvrde putuju kroz mrežu u suprotnom smjeru. Ukupno vrijeme potrebno da paket prođe kroz mrežu (tj. da se njegova potvrda vrati u izvorište) jednako je vremenu obilaska RTT. Tek kada je jedan paket napustio mrežu, izvorište može poslati sljedeći. Za velike mreže slanje pojedinog paketa nema utjecaja, pa su varijacije RTT dovoljno male. Odavde slijedi važna pretpostavka o konstantnom vremenu obilaska. Ako je W širina prozora, a RTT vrijeme obilaska, brzina *predaje predajnika* dana je formulom:

$$R = \frac{W}{RTT} \ [broj\ paketa/sek]$$

jer kroz vrijeme RTT u mrežu uđe cijela širina prozora W. Ograničavanjem širine prozora W može se kontrolirati brzina predaje R, uz pretpostavku da je RTT približno konstantno.

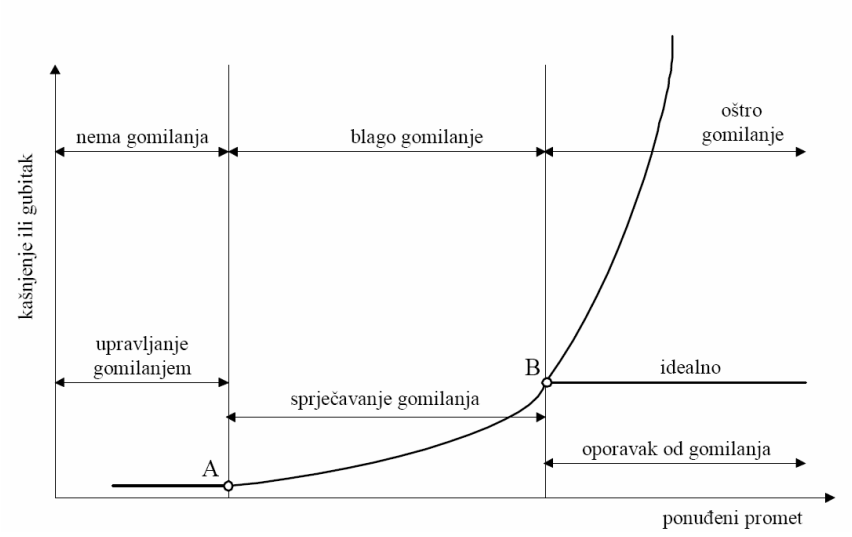
Posljedice zagušenja vidljive su iz dijagrama na slikama 5 i 6. Ovi dijagrami prikazuju funkcijske ovisnosti propusnosti mreže i prosječnog kašnjenja/gubitka o ponuđenom prometu. Vidljivo je da propusnost, a time i iskorištenje mreže, pri relativno malom opterećenju mreže raste s povećanjem ponuđenog opterećenja do točke A (tzv. koljeno, eng. knee). Pri daljnjem povećanju opterećenja povećanje propusnosti mreže je sporije, jer mreža ulazi u stanje *blagog*

*gomilanja*. Povećava se i kašnjenje. Kada ponuđeni promet dostigne vrijednost koja odgovara točki B (tzv. greben, eng. cliff), mreža ulazi u stanje *oštrog gomilanja*. Propusnost mreže se naglo smanjuje pri daljnjem povećanju opterećenja, jer zbog konačne veličine međuspremnika u čvorovima mreže dolazi do gubitaka paketa i retransmisija.. Tako u području oštrog gomilanja dolazi do degradacije kvalitete usluge, što se ogleda u povećanju kašnjenja ili gubitaka.




**Sl. 5 Funkcijska ovisnost propusnosti mreže o ponuđenom prometu**

Djelotvornost neke sheme kontrole zagušenja može se procijeniti na osnovi kašnjenja ili gubitka do kojega dolazi kada je ponuđeni promet veći od najvećeg dozvoljenog prometa.




**Sl. 6 Funkcijska ovisnost kašnjenja ili gubitka o ponuđenom prometu**

Optimalna radna točka mreže je točka A. U teoriji bismo nastojali održati mrežu što bliže toj točki. No u praksi algoritmi koji se primjenjuju otkrivaju raspoloživi kapacitet mreže upravo uvođenjem u zagušenje (tj. do točke B), te naknadnim smanjivanjem ponuđenog prometa.

TCP koristi gubitak segmenta kao indikaciju zagušenja, pa održava mrežu u radnoj točki oko točke B. Za postupke upravljanja prometom i sprječavanje zagušenja TCP raspolaže s nekoliko algoritama koji su često puta mijenjani i nadograđivani, u skladu s razvojem protokola TCP.

**Nagle-ov algoritam**: Kod nekih aplikacija uočeno je vrlo neučinkovito iskorištenje kanala. Primjer za to je TELNET veza, gdje se šalje znak po znak s tipkovnice. To znači da svaki pojedinačni znak putuje u svom paketu, dakle 1 oktet podataka i 40 okteta zaglavlja (20 okteta TCP zaglavlja + 20 okteta IP zaglavlja). Učinak se svodi na samo 2.4% korisne informacije po paketu, što nepotrebno opterećuje mrežu.

J. Nagle je 1984. godine ponudio adaptivno rješenje. On je predložio zadržavanje slanja novih korisnikovih podataka dok se ne potvrde svi prethodno odaslani paketi ili dok se ne skupi dovoljno podataka za slanje segmenta maksimalne veličine (MSS – Maximum Segment Size).

**Silly Window Syndrome algoritam:** Sljedeći problem koji se može pojaviti je *sindrom besmislenih prozora*, kada aplikacija na prijamnoj strani dobiva samo jedan po jedan oktet podataka. U početnom stanju spremnik prijemnika je pun i pošiljatelj to zna - oglašena je veličina prozora RWIN jednaka nuli. Kada se iščita jedan oktet na prijamnoj strani, odmah se oglašava prozor veličine jednog okteta. Pošiljatelj šalje jedan oktet podataka, te dolazi do ponavljanja ciklusa. Ovo rezultira slanjem svih podataka u paketima koji sadrže samo po 1 oktet podataka.

1982. godine je Clark predložio rješenje ovog problema. Potrebno je spriječiti prijemnik da oglašava prozor veličine jednog okteta. Prijemnik treba oglasiti prozor veličine maksimalnog segmenta koji je oglašen kod uspostave veze. Do tog trenutka on bi morao biti u stanju čekanja da se isprazne međuspremnici koji bi mu dozvolili da napravi taj korak.

**Slow start:** Algoritam usporenog starta služi za otkrivanje raspoloživog kapaciteta mreže, a koristi se na početku prijenosa ili kod oporavka od gubitka. Jednostavno se implementira pomoću dvije varijable. To su *prag Slow Starta SSTHRESH* (Sow Start Treshhold) i *prozor zagušenja CWND* (Congestion Window). SSTHRESH označava vrijednost na kojoj veza izlazi iz Slow Start faze i ulazi u fazu izbjegavanja zagušenja. SSTHRESH ima početnu vrijednost od 64 kB (toliko iznosi maksimalna veličina prijemnog prozora udaljenog TCPa).

Nakon uspostave veze, prozor zagušenja se postavlja na jedan segment. *Proces funkcionira tako da se primitkom svake potvrde CWND uvećava za jedan.* Prijenos započinje odašiljanjem jednog paketa i čekanjem potvrde za taj paket. Kada se primi potvrda, prozor zagušenja se poveća s jednog na dva segmenta, što znači da se sada mogu poslati dva segmenta. Na taj način CWND se udvostručuje primitkom svih potvrda iz prethodnog prozora. Ukoliko je vrijeme obilaska konstantno, prozor zagušenja raste eksponencijalno.

Rast prozora zagušenja CWND ograničen je s dva mehanizma. Prvo, manjom od dvije vrijednosti RWIN (Receiver Window) i SSTHRESH, nakon čega se automatski prelazi u fazu izbjegavanja zagušenja. Drugo, eksponencijalni rast prometa može dovesti do gubitka segmenta. Ukoliko je u fazi usporenog starta došlo do gubitka, ažuriraju se vrijednosti:

$$SSTHRESH = \max(2; CWND/2) \quad , \quad CWND = 1$$

Time nanovo započinje usporeni start, ali sada do polovičnog prozora CWND/2 u odnosu na prozor koji je uzrokovao zagušenje. Postupak se ponavlja sve dok faza usporenog starta ne prođe bez gubitaka. Postignuti CWND smatra se optimalnim u tom trenutku, te TCP prelazi u fazu izbjegavanja zagušenja.

**Congestion avoidance**: Izbjegavanje zagušenja je faza u kojoj TCP treba ispitivati mogućnost povećanja prozora kako bi iskoristio kapacitet mreže oslobođen eventualnim završetkom prijenosa drugih korisnika. Stoga se u ovoj fazi CWND povećava za 1 svakih RTT vremena, odnosno po algoritmu:

$$CWND = CWND + 1/CWND$$

Ova faza traje sve do ponovnog gubitka segmenta. Tada se ponavlja faza usporenog starta, pri čemu se koristi SSTHRESH = max(2; CWND/2) i CWND = 1, kao gore. U obje faze, prijemnik mora slati potvrdu za svaki primljeni paket.

TCP s ugrađenim usporenim startom i izbjegavanjem zagušenja poznat je kao **osnovni TCP**.

**Fast retransmit**: Čekanje na istek vremena retransmisije RTO je dugotrajno i traje RTT+4D. Za to vrijeme će svi paketi napustiti mrežu i ona ostaje neiskorištena. Brza detekcija gubitka moguća je ako prijemnik za svaki prekoredno primljeni segment (nakon gubitka) ponavlja posljednju poslanu kumulativnu potvrdu. Predajnik nakon druge duplicirane potvrde još nije siguran da li se radi o gubitku ili samo poremećaju redoslijeda isporuke. Međutim, nakon što primi tri duplicirane potvrde, predajnik zaključuje da je došlo do gubitka segmenta i obavlja ponovno slanje daleko prije isteka RTO. To je algoritam brze retransmisije.

TCP s ugrađenom brzom retransmisijom poznat je od 1989. kao **TAHOE TCP**.

**Fast recovery**: Algoritam brzog oporavka je uveden kako bi se što bolje iskoristile prednosti brze retransmisije. Naime, nakon gubitka paketa TCP normalno mora ići u fazu usporenog starta. Algoritam brzog oporavka izbjegava ovu fazu na način da se kod brze retransmisije parametri postave:

$$SSTHRESH = CWND/2 \quad ; \quad CWND = SSTHRESH+3$$

čime se uzimaju u obzir paketi koji su izašli iz mreže (tri duplicirane potvrde). Primitkom potvrde novih podataka ulazi se u fazu izbjegavanja zagušenja s polovičnim prozorom:

$$CWND = SSTHRESH.$$

Algoritam brzog oporavka efikasan je samo za jednostruke pogreške.

TCP s ugrađenim brzim oporavkom poznat je od 1990. kao **RENO TCP**.

**Djelomične potvrde:** Da bi se ubrzao izlazak iz faze brzog oporavka za slučaj višestrukog gubitka segmenta, uvedeno je razlikovanje novih i *djelomičnih (parcijalnih) potvrda*. Djelomična potvrda se bazira na karakteristikama kumulativne potvrde: kod jednostrukog gubitka, prijemnik će, nakon što primi brzom retransmisijom ponovljeni segment, potvrditi sve segmente poslane do popune nedostajućih podataka. Ukoliko prijemnik potvrdi smo dio podataka, predajnik može zaključiti da se radi o višestrukom gubitku segmenata. Takva potvrda se zove djelomična potvrda. Ona istovremeno znači da je određeni broj segmenata izašao iz mreže, te da je još neki od ranije poslanih segmenata izgubljen. Taj segment je moguće odmah ponovno poslati.

TCP s ugrađenim djelomičnim potvrdama poznat je kao **NEW-RENO TCP**.

## *5.4 SIMULACIJSKA MJERENJA NA PAKETNIM MREŽAMA*

Simulacija pomoću računala je disciplina određivanja modela nekog stvarnog ili teoretskog sustava, pokretanje takvog modela na digitalnom računalu, te analiza dobivenih rezultata. Simulacija je nužna u slučajevima: kada je model kompleksan s mnogo međusobno povezanih varijabli stanja, kada je model nelinearan, ili kada model sadrži varijable koje su slučajne prirode.

Značaj simulacije naročito dolazi do izražaja u projektiranju računalnih mreža. Korištenjem simulacije možemo mijenjati parametre pojedinih čvorišta u mreži bez skupih intervencija na samim uređajima.

Simulatori paketnih mreža su jako zahtjevni u pogledu obrade podataka. Kada čvorište prosljeđuje paket, generiraju se najmanje dva događaja: jedan određuje vrijeme dostavljanja paketa fizičkom mediju, a drugi vrijeme u kojem susjedni čvor prihvati paket. Ako je riječ o izvorišnom čvorištu, postoji još i događaj koji određuje slijedeći paket za retransmisiju. Ovi su simulatori jednako tako zahtjevni i u pogledu memorije. Broj paketa koji prolaze kroz mrežu raste linearno s povećanjem umnoška pojasne širine i kašnjenja.

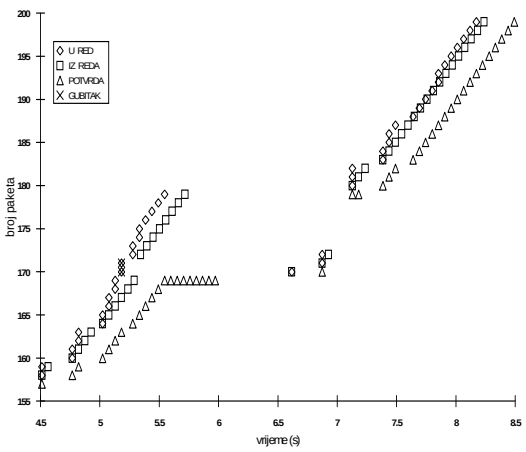
U ovoj vježbi koristi se simulator paktenih mreža NS 2, novija verzija simulatora NS (Network Simulator), razvijenog 1989. godine u Lawrence Berkeley National Laboratory (LBL) SAD kao varijanta već postojećeg simulatora REAL.

NS je mrežni simulator koji radi na principu liste događaja, a ugrađen je u Tool Command Language (Tcl) UNIX sustava. Struktura simulatora je izvedena u programskom jeziku C++, a može se upravljati i definirati pomoću Tcl sučelja. NS je organiziran kao interpreterska ljuska koja razumije naredbe pisane u Tcl jeziku, te naredbe samog simulatora. Naredba *ns* poziva određene funkcije NS simulatora unutar Tcl skripte. Pomoću naredbe *ns* definira se mrežna topologija, podešavaju se izvorišta i odredišta i starta se simulacija. Izvršavanje traje sve dok postoje događaji koji se trebaju izvršiti, ili dok ga sami ne prekinemo naredbom u skripti *ns stop*.

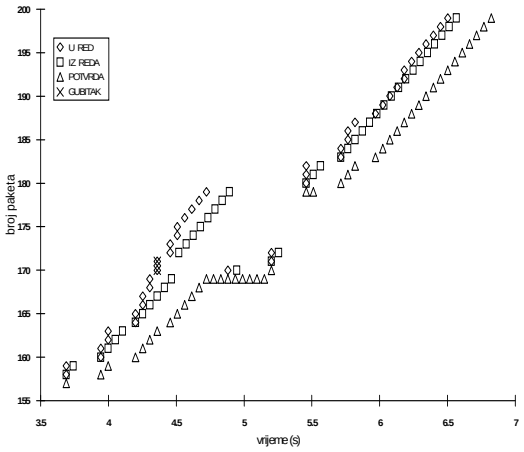
**Zadatak** u ovom dijelu vježbe je simulirati ponašanje različitih varijanti TCP protokola na jednostavnoj mreži i komentirati rezultate.

**PRIMJER:**

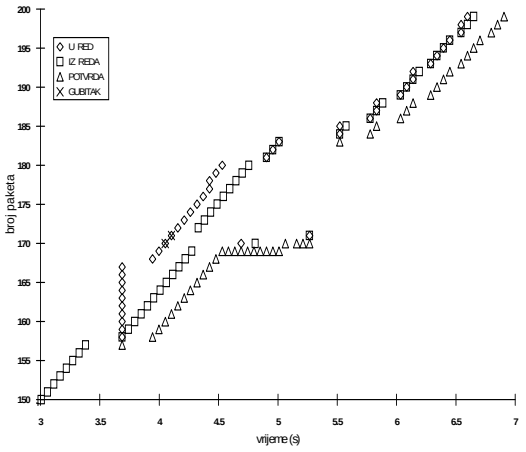
Na kanalu kapaciteta 150 kb/s i kašnjenja 100 ms izazvan je gubitak segmenata 70 i 71. Snimke slanja segmenta (U RED), emitiranja segmenta (IZ REDA) i prijema potvrde (POTVRDA), te gubitaka (GUBITAK) dane su na vremensko-prostornim grafovima, gdje je dimenzija prostora redni broj paketa, slika 7.



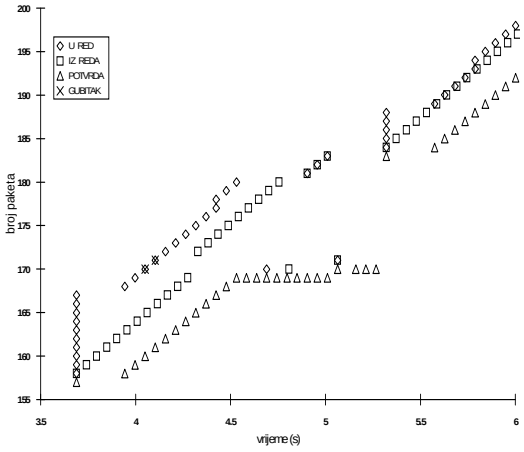

Osnovni TCP




Tahoe TCP




Reno TCP




NewReno TCP

**Sl. 7 Veza 150 kb/s, 100 ms, 70/2 gubitka**

Samo NEW-RENO TCP uspijeva retrasmitirati izgubljene segmente bez gubitka kapaciteta kanala.

# 6. Privatne mreže i vatrozidi

## *6.1 Privatne mreže (Intranet)*

Privatne mreže (Intranet) su mreže organizirane na TCP/IP tehnologiji, ali ne koriste javne, već privatne IP adrese. Za privatne mreže rezervirane su adrese 10.0.0.0/8, 172.16.0.0/16 i 192.168.0.0/16, dakle jedna A, jedna B i blok od 256 uzastopnih C klasa. Usmjernici Interneta pakete s ovim IP adresama odbacuju bez pokušaja daljnjeg usmjeravanja.

Postojanje Intranet mreža ima jedno od tri opravdanja:

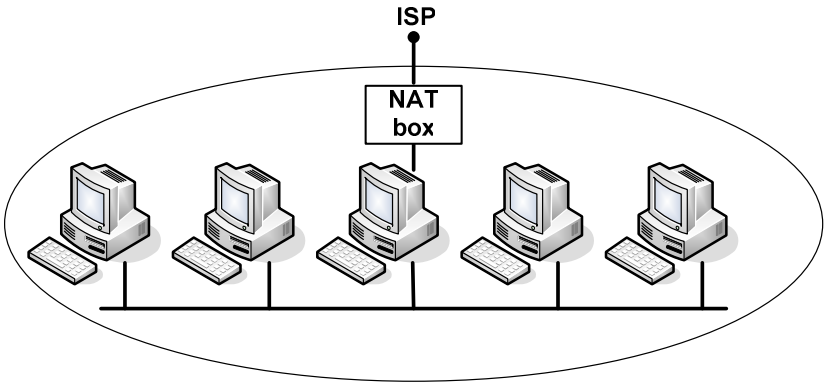
- mreža nije povezana na Internet - **nepovezane podmreže** trebaju koristiti privatne adrese kako bi kod naknadnog povezivanja na Internet bili izbjegnuti poremećaji u usmjeravanju, mogući za slučaj dupliciranja već iskorištenih adresa.

- mreža je povezana, ali zbog sigurnosti koristi privatne adrese - **sigurne podmreže** (Intranet) koriste privatne adrese, a povezane su na Internet preko jednog usmjernika koji prema Internetu djeluje kao krajnje računalo. Na taj način vanjskom učesniku komunikacije nije poznat broj ni nazivi računala unutar sigurne podmreže. Veze s javne mreže prenose se na privatnu (unutarnju) tehnikama maskarade i uslužnih veza, odnosno NAT-*Network Address Translation* i PAT-*Port Address Translation* protokolom (termin PAT se rjeđe koristi, radi jednostavnosti se pod NAT-om često podrazumijevaju oba protokola).

- mreža je povezana, ali zbog nedostatka/uštede IP adresa koristi privatne adrese.

Uobičajene lokalne mreže najčešće su preko usmjernika povezane na npr. zakupljeni vod odnosno njime na Internet. Usmjernik obavlja prevođenje s Ethernet na PPP protokol se koji koristi na zakupljenom vodu. IP datagram, njegovo zaglavlje sa IP adresama i njegov podatkovni dio (TCP, HTTP, ...) prenose se transparentno, bez obrade, budući su razine Internet modela nezavisne. Ethernet zaglavlje se odbacuje.

NAT protokol funkcionira dosta drugačije. Unutar lokalne mreže koristi se adresiranje s IP adresama iz raspona za privatne mreže, a prema Internetu je mreža predstavljena samo usmjernikom, koji se sada ponekad naziva i NAT kutija (NAT box).




**Sl. 1 Network Address Translation Protocol na lokalnoj mreži**

Kako smo vidjeli, većina aplikacija koristi TCP ili UDP na prijenosnoj razini te se svaka uspostavljena veza može identificirati priključnicom (socket) na dvije strane komunikacije (najčešće klijent i poslužitelj). Kada računalo iz Intranet lokalne mreže uspostavlja vezu prema poslužitelju izvan lokalne mreže, ono se spaja na priključnicu na poslužitelju, pri čemu odredišna priključna točka (Destination port) ovisi o usluzi na poslužitelju. Izvorišna priključna točka se dodjeljuje praktički nasumično iz raspona 1024 – 64k.

Ideja NAT protokola je jako jednostavna, ali nije "ISO/OSI kompatibilna". Kako je cjelokupna mreža predstavljena samo usmjernikom, izvorišna IP adresa paketa će pri prolasku kroz NAT kutiju biti zamijenjena IP adresom usmjernika. TCP ili UDP polje Source Port bit će također zamijenjeno vrijednošću po izboru NAT kutije, i ta će se vrijednost zapamtiti u memoriji NAT kutije, zajedno s Intranet IP adresom datagrama i originalnom vrijednošću polja Source port. Dakle, NAT box radi mapiranje između para *{internal address, internal port}* i *{external address, external port}*. Zamjena vrijednosti Source Port TCP/UDP polja pri slanju je nužna jer je zbog slučajnog karaktera tog polja moguće da dva ili više Intranet računala pokušaju uspostaviti vezu s istom vrijednošću Source Port.

Kada dođe odgovor od poslužitelja kojem je datagram upućen, NAT kutija će pogledati TCP/UDP Destination Port, zatim u svojoj tablici pogledati kojoj Intranet IP adresi on odgovara, obaviti zamjene IP adrese i Destination porta i pustiti datagram na Intranet mrežu. Ovo rješenje funkcionira dobro i masovno se koristi ali ima i značajnih mana. Neke od njih su:

- Prijenosna razina adresira računala, dakle radi posao mrežne razine;
- IP adresa više ne identificira jedinstveno računalo na Internet mreži, jer, mada prekriveno, može postojati više računala s istom IP adresom iz privatnog skupa adresa;
- Povećano je kašnjenje;
- Nemogućnost praćenja puta paketa s kraja na kraj; itd.

## *6.2 Vatrozid*

**Vatrozid (firewall)** je uređaj ili program koji nadzire mrežni promet na računalu ili mreži. Njegova uloga je kontroliranje prometa po kriteriju IP adrese, TCP/UDP porta, odredišne usluge, protokola, TTL vrijednosti, aplikacije i dr. Na taj je način moguće ograničiti različite zloupotrebe mreže i ograničiti djelovanje virusa preko mreže.

Koji promet se propušta, a koji blokira, definiraju pravila u tablicama filtriranja. Dvije su uobičajene politike filtriranja:

- blokira se sav promet koji nije eksplicitno dozvoljen - najsigurnija i najpreporučljivija politika kod koje administrator posebno dozvoljava ono što je potrebno.

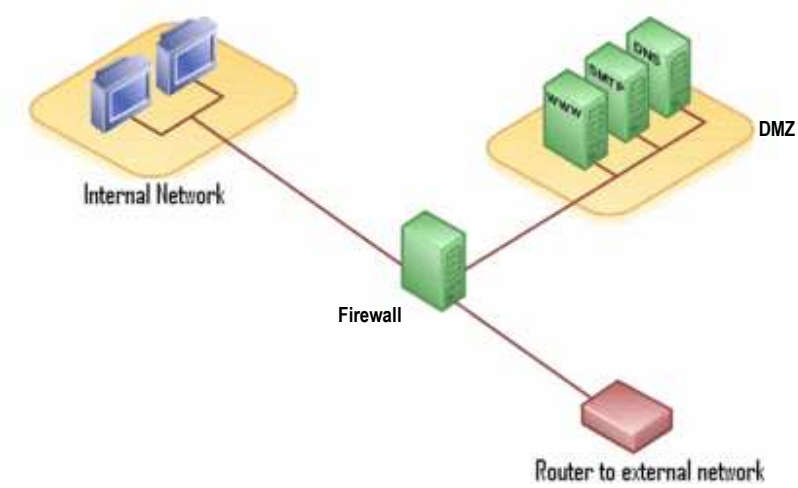
- propušta se sav promet koji nije eksplicitno blokiran - manje sigurna, ali jednostavnija politika.

Vatrozidi često imaju ugrađenu NAT funkcionalnost, a računalima u lokalnoj mreži iza vatrozida uobičajeno su dodijeljene privatne mrežne adrese. Kako je osnovna namjena vatrozida reguliranje prometa među mrežama različitih nivoa sigurnosti uobičajeno se koriste za uspostavu **DMZ (demilitarizirajuće zone)** - fizičke ili logičke podmreže srednjeg nivoa sigurnosti, koja se nalazi između sigurne unutrašnje mreže (npr. privatne lokalne mreže) i nesigurne vanjske mreže (npr. Interneta). Svrha demilitarizirajuće zone je dodavanje još jednog sigurnosnog sloja nekoj

lokalnoj mreži. Tipično DMZ sadrži uređaje koji trebaju biti dostupni Internet prometu, kao što su Web (HTTP) poslužitelji, FTP poslužitelji, SMTP (e-mail) poslužitelji i DNS poslužitelji.

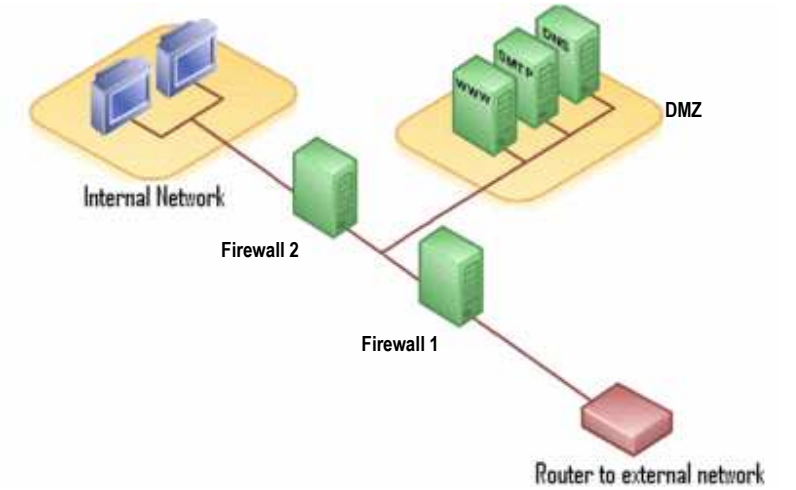
Mreža sa demilitarizirajućom zonom može se uspostaviti na više načina. Dvije najčešće metode su s jednim i sa dva vatrozida. Ove jednostavne arhitekture mogu se proširiti u složenije, ovisno o zahtjevima mreže.

Kod arhitekture s jednim vatrozidom koristi se vatrozid s barem 3 mrežne kartice. Jedna mrežna kartica služi za vezu prema ISP-u, na drugoj se formira interna mreža, a na trećoj DMZ (slika 2). Vatrozid mora nadzirati sav promet s Interneta i prema DMZ i prema Intranetu.




**Sl. 2 Mrežna arhitektura s DMZ i jednim vatrozidom**

Sigurnija i skuplja metoda je uspostava DMZ pomoću 2 vatrozida (slika 3). Prvi mora biti konfiguriran tako da propušta i promet namijenjen DMZ i onaj namijenjen internoj mreži. Drugi vatrozid smije propuštati samo promet namijenjen internoj mreži, a koji ne potječe iz DMZ.




**Sl. 3 Mrežna arhitektura s DMZ i dva vatrozida**

## 6.3 VPN

Tvrtke koje se fizički rasprostiru na više fizički udaljenih lokacija mogu se povezati u jedinstvenu mrežu korištenjem zakupljenih vodova (fiksne cijene najma) između lokacija. Većini tvrtki to je preskupo i presloženo rješenje, a nije praktično niti kod umrežavanja novih lokacija kao niti kod umrežavanja privremenih korisnika (npr. kupaca).

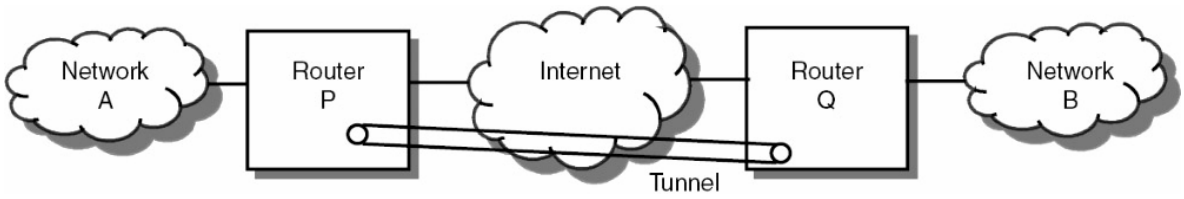
Rješenje koje se danas koristi u takvim situacijama je virtualna privatna mreža (Virtual Private Network – VPN). VPN za umrežavanje pojedinih lokacija tvrtke koristi postojeću Internet infrastrukturu, koja je mnogo prikladnije rješenje od korištenja zakupljenih vodova. Dva su problema kod korištenja Internet mreže za umrežavanje privatnih mreža: sigurnost i performanse. Stoga VPN mreža mora uključivati i sljedeće dodatke na protokole korištene u Internet mreži:

- Autentifikacija - potvrđuje autentičnost strana u komunikciji;
- Kontrola pristupa - onemogućuje neautorizirani pristup mreži;
- Tajnost i integritet podataka - zaštićuje podatke od čitanja ili mijenjanja kod prijenosa kroz javnu mrežu.

Za autentifikaciju i kontrolu pristupa koristi se niz protokola (Challenge Handshake Authentication Protocol - CHAP, Remote Authentication Dial-in User Service - RADIUS, korištenje digitalnih certifikata, biometrijske provjere, itd). Tajnost i integritet podataka osigurani su enkripcijom.

## 6.4 VPN arhitektura i protokoli

Svaka lokacija tvrtke vezana je uobičajenim vodom na pružatelja Internet usluge (ISP). Veze između lokacija uspostavljaju se korištenjem tuneliranja, tj. enkapsuliranjem podataka u IP pakete, koje odvaja promet između lokacija (sa svojim rasponom IP adresa) od podataka predviđenih za usmjeravanje na Internet mreži.

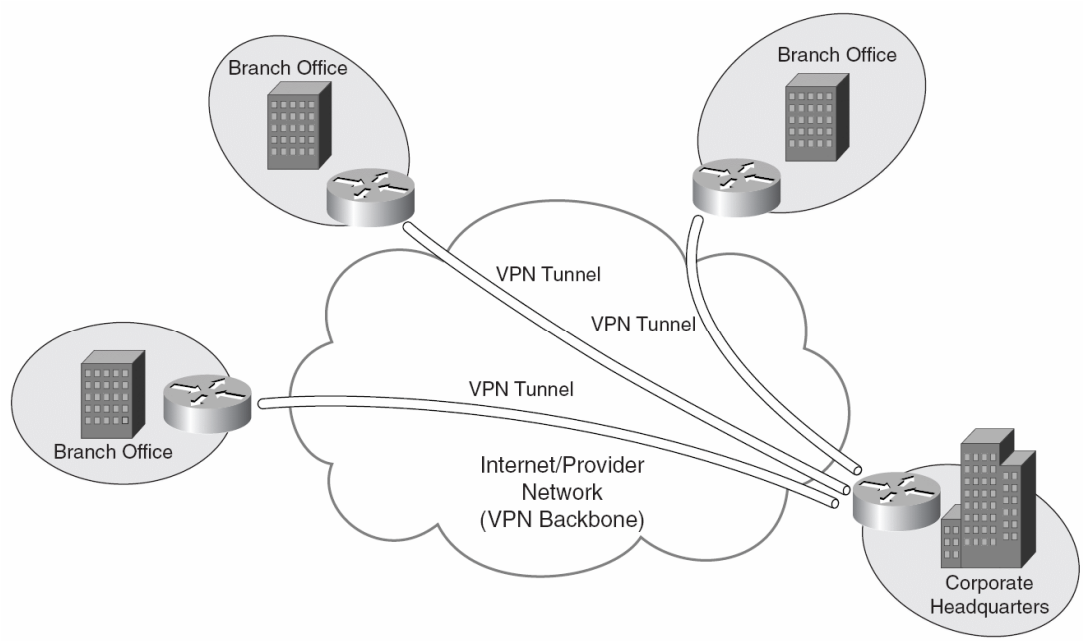



**Sl. 4 Tuneliranje između dvije VPN lokacije**

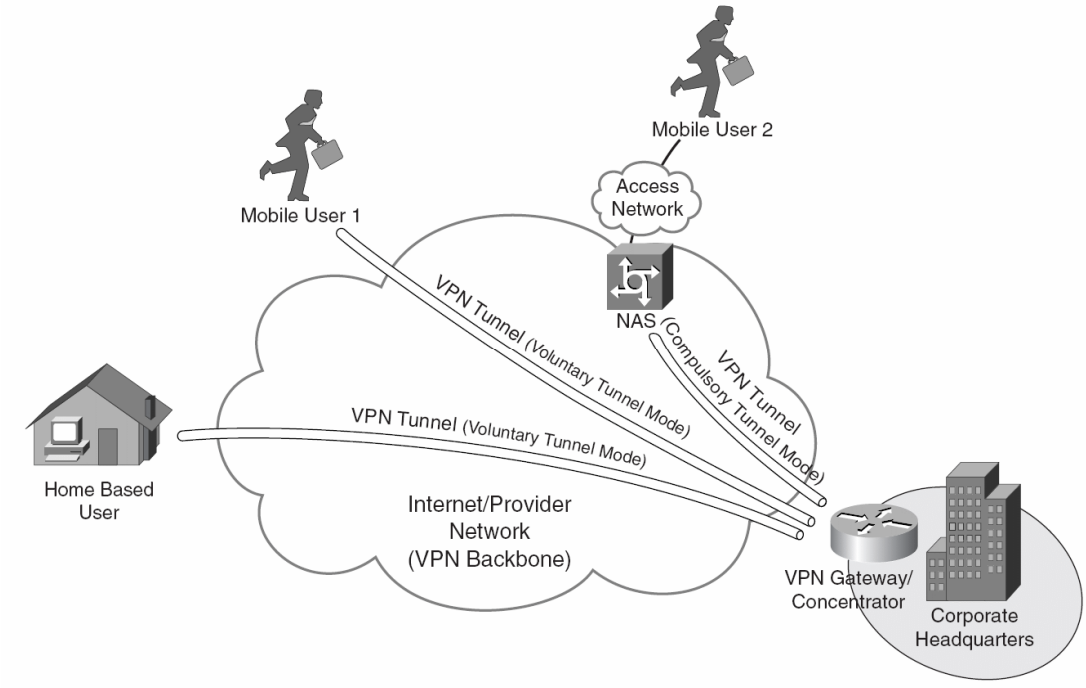
Proces tuneliranja između dvije VPN lokacije može se ukratko opisati kroz nekoliko faza (slika 4):

- Računalo iz mreže A komunicira s računalom iz mreže B; ono formira IP paket s IP adresom odredišnog računala iz mreže B, i prosljeđuje ga svojom lokalnom mrežom usmjerniku P.
- VPN usmjernik P formira IP paket koji u polju odredišne adrese sadrži adresu VPN usmjernika Q, a u podatkovnom dijelu kompletan paket primljen od računala iz mreže A.
- Internet mrežom taj se paket isporučuje VPN usmjerniku Q. On izdvaja iz podatkovnog dijela IP paketa originalni paket i isporučuje ga računalu iz mreže B.

Postoje dvije osnovne arhitekture VPN mreža: Site-to-Site (slika 5) i Remote Access (slika 6).




**Sl. 5 Site-to-Site VPN**




**Sl. 6 Remote Access VPN**

*Site-to-Site VPN*, odnosno VPN mreža od lokacije do lokacije, povezuje cijele podmreže u virtualnu privatnu mrežeu. Računala u podmrežama nemaju podršku za VPN već se o enkripciji i enkapsuliranju/dekapsuliranju podataka brinu VPN pristupni uređaji (VPN gateway), obično usmjernici ili vatrozidi preko kojih su podmreže spojene na javnu mrežu. Najčešći protokoli koji se koriste u Site-to-Site VPN arhitekturi su:

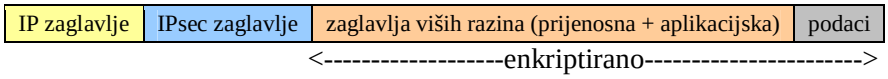
- IPsec – skup protokola za zaštitu IP prometa na javnoj mreži,
- L2TPv3 (Level 2 Transport Protocol version3) – koristi se najčešće za tuneliranje PPP okvira preko IP mreže, a moguće ga je koristiti i za Frame Relay i Ethernet.

Kod *Remote Access VPN*-a, tj. udaljenog VPN pristupa, pojedinačni nepokretni ili pokretni klijent se povezuje na podmrežu. U ovom slučaju taj klijent mora imati podršku za VPN. Najčešći protokoli koji se koriste u Remote Access VPN arhitekturi su:

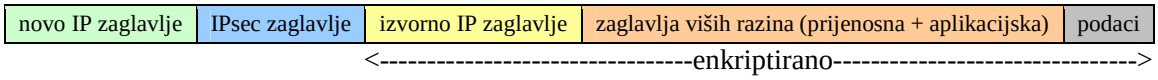
- PPTP (Point-to-Point Tunneling Protocol) – omogućuje tuneliranje klijentskih PPP okvira,
- L2TPv2/L2TPv3 (Layer 2 Tunneling Protocol versions 2 and 3) – IETF standard koji omogućava tuneliranje klijentskih PPP okvira, najčešće se zbog poboljšanja sigurnosti kombinira s IPsec protokolom na mrežnoj razini.
- IPsec - sam ili u kombinaciji s prethodnim protokolom
- SSL (Secure Sockets Layer) – protokol originalno razvijen u Netscape Communications, omogućava siguran pristup udaljenih ili čak mobilnih klijenata određenim aplikacijama.
- TLS (Transport Layer Security) – IETF standard, sličan SSLv3 standardu. Oba navedena standarda jako su prikladna i korištena jer ne zahtijevaju posebnu prilagodbu klijenata, s obzirom na to da se uglavnom koriste u web aplikacijama, a većina web preglednika ih podržava. Zbog toga se često koristi i termin *web* ili *clientless VPN*.

IPsec protokol je mrežni protokol, nastao kao rezultat rada na IPv6 protokolu, ali se koristi i na v4 protokolu i najčešći je izbor kod VPN mreža. Omogućuje klijentu ili usmjerniku autentifikaciju, provjeru integriteta i enkripciju IP paketa. Koriste se dva moguća načina rada:

- **prijenosni način:** enkriptiraju se samo podaci IP paketa (prijenosna razina i više), a iza IP zaglavlja se dodaje određeno IPsec zaglavlje (*AH-Authentication* Header ili *ESP-Encapsulating Security Payload*) te se u IP zaglavlju mijenja oznaka protokola više razine u oznaku za IPsec umjesto npr. TCP.




- **tunelski način:** kompletan IP paket, uključujući i zaglavlje, se enkriptira te mu se dodaje novo IP i IPsec zaglavlje (AH ili ESP).



# 7. BEŽIČNE LOKALNE MREŽE (WLAN)

## *7.1 Bežične lokalne mreže*

Bežične lokalne mreže WLAN (Wireless Local Area Network) su fleksibilni sustavi koji omogućavaju podatkovne komunikacije velikih brzina unutar manjih područja pokrivanja. WLAN mreže odašilju i primaju podatke slobodnim prostorom putem elektromagnetskih valova, što mobilnim terminalima omogućuje pristup mreži s bilo kojeg mjesta i u bilo koje vrijeme. Na ovakav način, WLAN kombinira podatkovnu povezanost s pokretljivošću korisnika.

Grade se s namjerom zamjene ili dogradnje ožičenih lokalnih mreža uz sve prednosti i dodatne funkcionalnosti koje prizlaze iz bežičnog povezivanja. Naime, tradicionalna čvrsto ožičena mreža je skupa, teško je instalirati, održavati, a posebno modificirati.

S obzirom na to, neke od prednosti WLAN mreža su sljedeće:

- mobilnost korisnika (stvarni rad u pokretu)
- laka pokretljivost (fizičko premještanje računala)
- fleksibilnost mreže u smislu rekonfiguracije i proširenja
- besplatno korištenje veze.

Bežično povezivanje uvjetuje i brojne nedostatke WLAN-a vezane za:

- sigurnost - Budući da se signal prenosi EM valovima kroz prostor, bežične mreže su znatno izloženije napadima od ožičenih.
- pouzdanost - Bežični signal izložen je brojnim smetnjama čiji se utjecaj nastoji smanjiti odgovarajućom modulacijom i jačinom signala.
- brzinu - Brzine bežičnih mreža su reda veličine 1 do 100 Mbit/s, što je znatno sporije od uobičajenih 100 Mbit/s pa do nekoliko Gbit/s kod ožičenih lokalnih mreža .
- domet - Domet signala kod bežičnih lokalnih mreža je reda veličine nekoliko desetaka metara (u zatvorenom prostoru zbog gušenja manji nego na otvorenom), što se može povećati dodavanjem obnavljača (eng. *repeater*) i pristupnih točaka.

## *7.2 Povijesni razvoj*

Prva eksperimentalna WLAN mreža realizirana je sedamdesetih godina prošlog stoljeća na Sveučilištu na Havajima (ALOHA mreža). Intenzivno istraživanje i razvoj WLAN mreža započinje početkom devedesetih godina, što je rezultiralo donošenjem niza IEEE 802.11 standarda koji se razlikuju u pogledu dometa, brzine rada i korištenog frekvencijskog područja. WLAN mreže koriste frekvencije signala iz ISM (Industrial, Scientific, Medical application of radio).

| Protokol | Datum standardizacije | Frekvencija rada | Brzina rada (max) |
|---|---|---|---|
| 802.11 | 1997. | 2.4GHz - 2.5GHz | 1Mbps (2 Mbps) |
| 802.11a | 1999. | 5 GHz | 25Mbps (54Mbps) |
| 802.11b | 1999. | 2.4 GHz | 5.5Mbps (11Mbps) |
| 802.11g | 2003. | 2.4GHz | 24Mbps (54Mbps) |
| 802.11n | 2009. | 2.4GHz ili 5GHz | 200Mbps (600Mbps) |

**Tablica 1. WLAN standardi**

Na fizičkom sloju u WLAN mrežama najzastupljenija tehnologija je radiofrekvencijska (RF – Radio Frequency) kod koje se podaci prenose radio valovima. Koristi se širokopojasna radiofrekvencijska tehnika i dvije osnovne tehnologije širokog spektra (Spread Spectrum):

- *FHSS (Frequency Hopping Spread Spectrum)* - sustav skakanja frekvencija - raspoloživi frekvencijski raspon se dijeli na kanale određenih frekvencija, te signal nosilac "skače" u kratkim vremenskim intervalima iz jednog kanala u drugi, prema pseudoslučajnom nizu dogovorenom između predajnika i prijemnika. Time se smanjuje utjecaj smetnji na određenim frekvencijama.

- *DSSS (Direct Sequence Spread Spectrum)* - sustav direktnog raspršenja - predajnik modulira signal šumom mnogo veće frekvencije (pseudoslučajni niz vrijednosti 1 i -1, pri čemu svaki traje mnogo kraće od informacijskog bita kojeg modulira) te nastaje signal širokog frekvencijskog spektra, sličan tzv. bijelom šumu. Prijemnik, koji je sinhroniziran s predajnikom, demodulira signal korištenjem istog pseudslučajnog niza vrijednsti 1 i -1.

Podsloj upravljanja pristupom prijenosnom mediju (MAC) podatkovnog sloja za WLAN mreže određen je standardom 802.11. Karakteristike prijenosnog medija ne omogućavaju detekciju kolizije kao kod ožičenih lokalnih mreža. Ovaj standard definira protokol pod nazivom **CSMA/CA** (Collision Avoidance), višestruki pristup mediju s detekcijom nosioca i izbjegavanjem sudara.

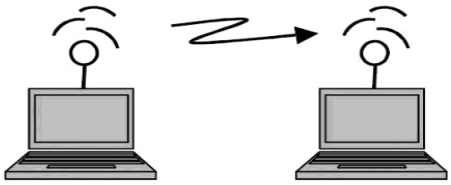
Protokol radi na sljedećem principu: stanica koja želi poslati podatke najprije osluškuje, te ako je medij slobodan, nakon slučajnog vremena obavlja rezervaciju slanjem okvira RTS (Request to Send) sa adresom odredišta i izvorišta. Ukoliko nije došlo do kolizije, odredišna stanica na to odgovara paketom CTS (Clear to Send) i time odobrabrava prijenos. U slučaju da je komunikacijski medij zauzet izvorišna stanica ulazi u proces slučajnog zadržavanja (back off) čekajući da se medij oslobodi. Nakon uspostave komunikacije primitak svakog paketa se mora potvrditi ACK porukom.

## *7.3 Načini djelovanja bežičnih lokalnih mreža*

Uređaji koji se uključuju u bežičnu mrežu moraju biti opremljeni odgovarajućom sklopovskom podrškom (većina prijenosnih računala) ili bežičnim sklopovima na USB ili PCMCIA sabirnicama.

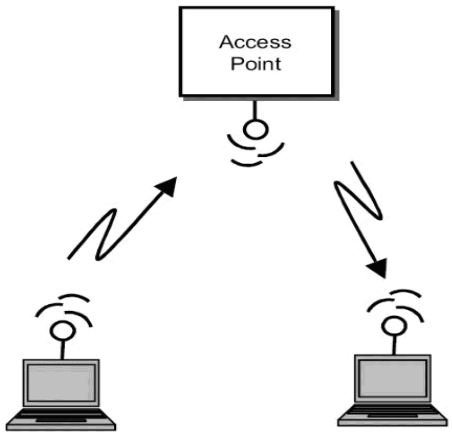
Standard 802.11 definira dva načina rada WLAN mreža:

**Ad hoc (peer-to-peer) način rada** - izravna (decentralizirana) komunikacija bežičnih stanica, bez korištenja pristupne točke (AP).



**Slika 1. Ad hoc način rada**

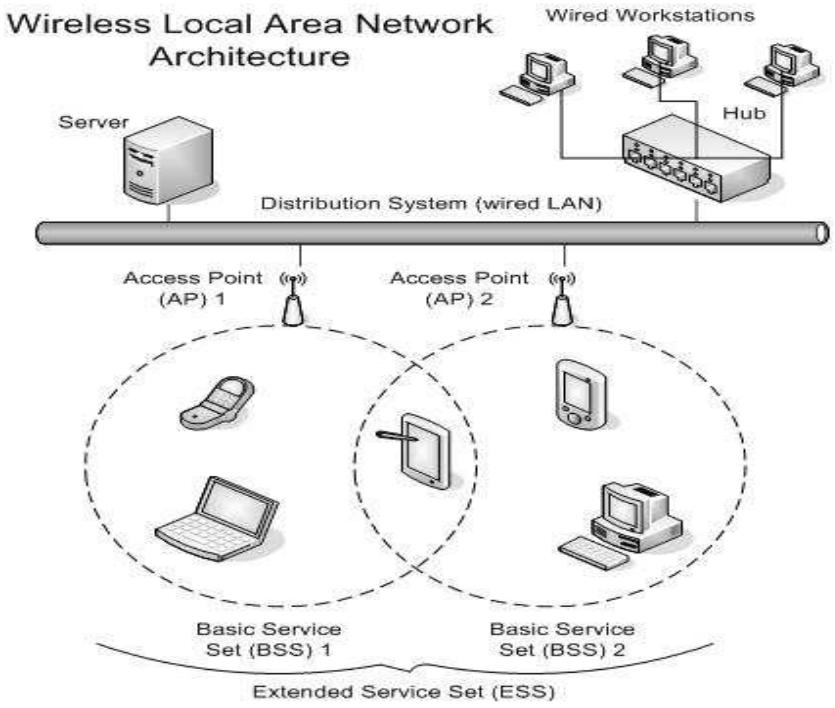
**Infrastrukturni način rada** - bežična mreža sadrži barem jednu pristupnu točku (AP - Access Point) koja djeluje kao posrednik pri komunikaciji između uređaja unutar bežične mreže.




**Slika 2. Infrastrukturni način rada**

Pristupna točka služi kao most između fiksne mreže i bežičnih stanica u njenom dosegu. To je primopredajni uređaj koji ima funkciju primanja, pohrane i prosljeđivanja podataka između WLAN-a i žične mrežne infrastukture. Ima područje djelovanja od nekoliko stotina metara i može podržati manje grupe pokretnih korisnika.

Područje djelovanja jedne pristupne točke naziva se *BSS (Basic Service Set)* - osnovni korisnički skup, i korisnicima omogućava bežično povezivanje na ožičenu lokalnu mrežu. Ukoliko postoji više pristupnih točaka čija se područja djelovanja međusobno preklapaju dobivamo jedinstven bežični sustav tzv. *ESS (Extended Service Set)* - prošireni korisnički skup, unutar kojeg se korisnici mogu kretati bez prekida veze (roaming).




**Slika 3. Arhitektura bežične lokalne mreže (BSS i ESS)**

Standardom je definirano 9 usluga koje uređaji moraju pružati, od kojih se tri važnija odnose na postavljanje i korištenje bežične mreže:

**Autentifikacija** – kako bi se onemogućile zlouporabe, uređaj koji se uključuje u bežičnu mreže mora imati lozinku koja je pridružena mreži, što se ispituje kod autentifikacije.

**Deautentifikacija** – usluga komplementarna prethodnoj, nakon deautentifikacije uređaj više ne može koristiti mrežu.

**Privatnost** – podaci koji se prenose mrežom zaštićuju se enkripcijom.

Kod novijih operativnih sustava podrška za bežične mreže je ugrađena, dok je kod starijih podržana od proizvođača bežične mrežne kartice. Pristupna točka može se konfigurirati izravnim spajanjem *crossover* kabelom i pripadajućim programom, kao i putem bežične veze i web servera koji postoji na uređaju. Konfiguracija obuhvaća postavljanje svih parametara mreže: identifikacija mreže, autentifikacija, liste MAC adresa klijenata koji mogu ili ne uključiti u mrežu, itd.

**Zadatak:**

Prema zadanoj shemi spojiti i konfigurirati zadanu mrežu.