Računalne mreže – razvoj i značajke

Ivica Jurkić | 31 ožujka, 2026

Ova knjiga je zamišljena kao niz članaka koji bi trebali predstaviti najosnovnije značajke računalnih mreža sa naglaskom na lokalne mreže (LAN). Knjiga bi trebala sadržavati pregled slijedećih poglavlja:

Razvoj mreža

Mediji

Mrežna oprema

Topologija LAN-ova

OSI referentni model

Protokoli

Adresiranje u LAN-u

Binarni brojevni sustav

Klase adresa

Subnetiranje

Bežične lokalne mreže

Mrežni servisi

ISDN

Routing protokoli

Računalna mreža nastaje povezivanjem dva i više računala. Svrha povezivanja računala je dijeljenje podataka i uređaja kojima se može pristupiti putem mreže (*printer*, *skener*, *ploter*,...) ili stvaranje distribuirane obrade podataka (računalni *klasteri*, projekt **SETI@home**,...).

Razvojem i širokom primjenom osobnih računala, javila se mogućnost kreiranja velike količine programa i multimedijalnog sadržaja (teksta, grafike, zvučnog i video sadržaja) koje je bilo poželjno dijeliti sa drugim korisnicima računala. U vrijeme prije izgradnje računalnih mreža taj sadržaj se razmjenjivao putem prijenosnih medija za pohranu podataka (magnetske trake, diskete, CD ROM,...). Obzirom na ograničenja medija za pohranu podataka, na taj način se mogla prenijeti manja količina podatka i na manje udaljenosti. Za veće udaljenosti, bilo je potrebno medij dostaviti na odgovarajući način (pošta, kurirska služba, itd...) za što je obično trebalo i puno vremena.

Povezivanjem računala u mrežu, putem medija kojim su računala povezana (bakreni vodič, optičko vlakno, bežični prijenos), u kraćem vremenskom periodu moguće je prenijeti veću količinu podataka.

U samom početku razvoja računalnih mreža ta brzina prijenosa podataka je bila podosta ograničena (u odnosu na današnje brzine). Poruke i podaci su se mogle prenositi u tekstualnom obliku brzinom od nekoliko znakova u sekundi. *Bandwidth* predstavlja količinu podataka koja može proći kroz neki medij za prijenos podataka u jedinici vremena i mjeri se u bitovima u sekundi (*bits per second* – **bps**). On često predstavlja samo teorijsku vrijednost. Propusnost (*throughput*) predstavlja realnu vrijednost količine prenesenih podataka u jedinici vremena i često je manja od *bandwidtha*.

Daljnjim razvojem mreža povećana je propusnost i ostvaren je prijenos veće količine podataka i

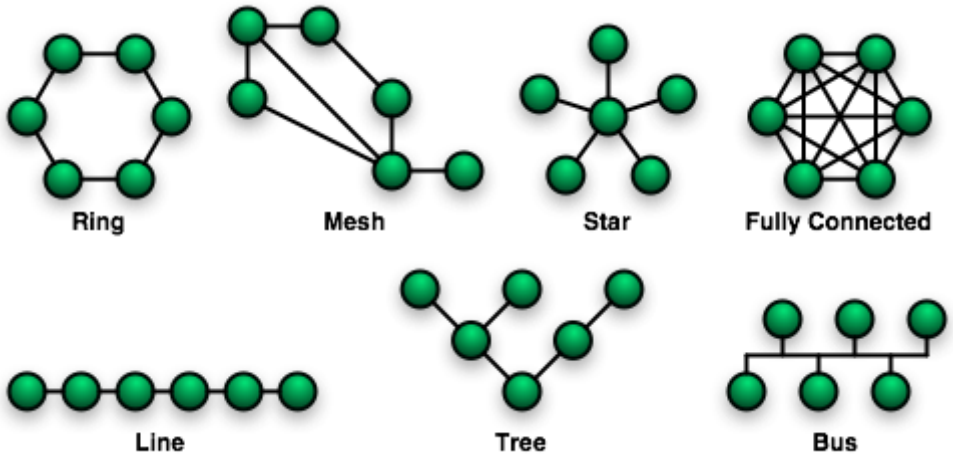
multimedijalnog sadržaja. Najprije na manje udaljenosti unutar lokalnih mreža (**LAN** – *Local Area Network*), a potom i na veće udaljenosti (**WAN** – *Wide Area Network*).

Prema veličini mreže možemo podijeliti na:

Prema sklopovskoj tehnologiji koju koriste, mreže možemo podijeliti na:

Računalne mreže mogu biti podijeljene prema i prema funkcionalnim povezanostima između pojedinih elemenata mreže:

Mrežna topologija predstavlja skicu rasporeda ili povezanosti članova neke mreže. Može biti **fizička** ili **logička**. Fizička topologija predstavlja nacrt fizičkog rasporeda čvorova u mreži, dok logička topologija predstavlja nacrt logičkog toka podataka između čvorova te mreže. Fizička topologija ne mora ujedno biti i logička topologija.



Prema fizičkoj mrežnoj topologije mreže možemo svrstati na:

Mrežni komunikacijski protokol predstavlja skup određenih pravila (za prikaz podataka, signalizaciju, autorizaciju i otkrivanje pogrešaka) koja su potrebna da bi se podaci mogli prenijeti preko komunikacijskog kanala. Pojednostavljeno, pojedini protokol je ''jezik'' kojim se članovi u mreži dogovaraju oko prijenosa podataka. Da bi se podaci uspješno prenijeli članovi moraju pronaći zajednički ''jezik''. Mreže možemo podijeliti i prema komunikacijskom protokolu (**TCP/IP**, **Ethernet**, **IPX**, **FDDI**, **Token Ring**, **X25**, **Frame relay**, **ATM**,...).

Više informacija na:

http://en.wikipedia.org/wiki/Computer_network

OSI referentni model (*Open Systems Interconnection Basic Reference Model*) je apstraktni, slojeviti model koji služi kao preporuka stručnjacima za razvoj računalnih mreža i protokola. **OSI** model je podjeljen u sedam slojeva, gdje svaki sloj opisuje skup povezanih funkcija koje omogućuju jedan dio računalne komunikacije. Svih sedam slojeva zajedno, prikazuju tok podataka od izvora prema odredištu.

OSI referentni model pruža važne smjernice u razvoju mrežnih protokola. Mrežni komunikacijski protokol predstavlja skup određenih pravila (za prikaz podataka, signalizaciju, autorizaciju i otkrivanje pogrešaka) koja su potrebna da bi se podaci mogli prenijeti preko komunikacijskog kanala.

Sedam slojeva OSI referentnog modela:

Slojevi unutar jednog modela komuniciraju samo sa prvim slojem poviše i prvim slojem ispod sebe. Gornji protokol ovisi o funkcionalnosti koji pruža protokol ispod njega. Ukoliko komunikaciju

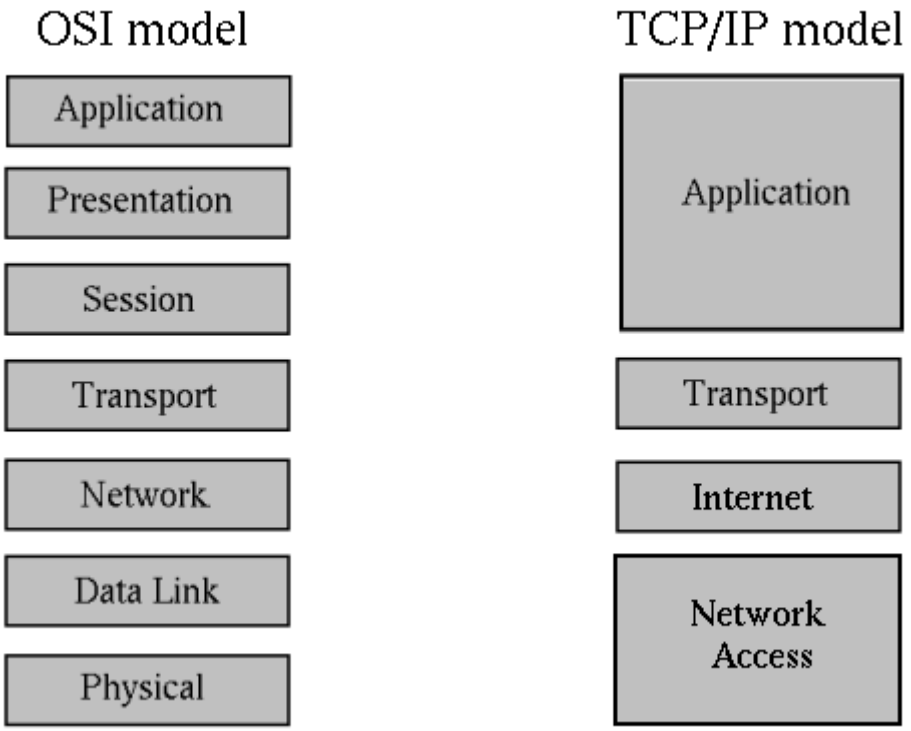
prikažemo sa dva **OSI** modela, možemo vidjeti da se slojevi jednog modela povezuju samo sa slojevima istog nivoa drugog modela. Npr., transportni sloj jednog modela šalje podatke transportnom sloju drugog modela. To se naziva *peer-to-peer* komunikacija. Svaki od modela u osnovi predstavlja jedan komunikacijski uređaj.

OSI model je razvijen kao preporuka koja olakšava razvoj protokola i komunikacije. Podjelom na slojeve omogućeno je da se, pridržavanjem smjernica, ubrza razvoj protokola za pojedini sloj, ne oviseći u velikoj mjeri o brzini razvoja protokola na drugim slojevima. Dodatno, cijeli zadatak je segmentiran, pa je više timova (tvrtki, organizacija) moglo raditi na rješavanju pojedinog problema. Na svakom od slojeva može djelovati više različitih protokola.

Osim **OSI** modela postoje i drugi slični modeli koji služe kao orjentir u razvoju mrežnih komunikacija. Veliki broj protokola je izgrađen prema **TCP/IP** modelu.

TCP/IP model ima manji broj slojeva, samo 4:

Ova 4 sloja obuhvaćaju sve funkcionalnosti **OSI** modela. Application sloj **TCP/IP** modela u sebi uključuje slične funkcije gornja 3 sloja **OSI** modela (*Application, Presentation, Session*). *Network Access* sloj **TCP/IP** modela u sebi uključuje slične funkcije donja 2 sloja **OSI** modela (*Data Link, Physical*).



Oba modela koriste slojeve za prikaz komunikacije i ti slojevi imaju slične uloge. Oba sloja koriste ***packet-switched*** tehnologiju.

Packet-switched tehnologija opisuje slanje podataka u malim zapakiranim jedinicama podataka zvanim **paket**. Paketi se usmjeravaju po mreži koristeći odredišnu adresu koja je sadržana u paketu. Put kojim paket dolazi od izvora do odredišta nije bitan. Bitno je da svi paketi stignu na odredište. Djeljenje podataka za slanje u pakete omogućuje se da se iste komunikacijske veze (linije) dijele između većeg broja korisnika mreže. Taj se oblik komunikacije još naziva i ***connectionless***. Većina komunikacija na internetu koristi ovaj oblik slanja podataka.

Svaki od slojeva unutar **OSI** modela ima neki oblik pakiranja podataka. ***Protokol Data Unit*** (**PDU**)

je naziv za pojedini oblik pakiranja podataka za odgovarajući sloj:

Postupak pakiranja podataka, od 7. sloja prema 1. sloju, u oblik pogodan za prijenos komunikacijskim vezama se naziva **enkapsulacija**. Odvija se na uređaju koji šalje podatke (izvor).

Obrnuti postupak, od 1. sloja prema 7. sloju, kojim se iz bitova izgrađuje okvir, iz okvira uzima paket, iz paketa segment,... se naziva **deenkapsulacija** i odvija se na uređaju koji prima podatke (odredište).

Uloge slojeva OSI referentnog modela:

Više informacija na:

http://en.wikipedia.org/wiki/OSI_model

Ethernet predstavlja skup mrežnih računalnih tehnologija primjenjenih unutar lokalnih mreža (**LAN** – *Local Area Network*). Na fizičkom sloju Ethernet definira raspored ožičenja, te vrste i razine signala za prijenos podataka. Na drugom sloju Ethernet definira način pristupa mediju za prijenos podataka (**MAC** – *Media Access Control*) i definira zajednički adresni format. Ethernet je standardiziran kroz **IEEE 802.3** standard.

Ethernet je razvijen sredinom 70-tih unutar tvrtke **Xerox**. U početku je imao brzinu prijenosa od 3Mbps i koristio je 8-bitno adresiranje. Današnji standardi propisuju brzine od 1Gbps i 48 bitno adresiranje (**MAC** adresa). U početku je kao standardni medij za prijenos podataka korišten koaksijalni kabel, dok se danas standardno koristi neki od oblika **UTP** (*unshielded twisted pair*) kabela. Pored navedenih, kao mediji u ethernetu se još koriste optička vlakna.

Ethernet mediji – coax

Ethernet mediji – UTP

Ethernet mediji – optičko vlakno

U početku razvoja, Ethernet je koristio **CSMA/CD** (*Carrier Sense Multiple Access With Collision Detection*) protokol za utvrđivanje redoslijeda pristupa dijeljenom mediju. Taj protokol omogućuje pristup mediju za slanje podataka ako je medij dostupan (nitko drugi ne šalje). Ako dvije stanice šalju istovremeno, dogodi se kolizija i nakon nekog vremena čekanja podaci se ponovo šalju (kad nitko drugi ne šalje).

Kad računalo želi poslati podatke, to se odvija kroz slijedeći algoritam:

Ukoliko na jednom mediju istovremeno postoje dva signala, onda se dogodila kolizija. Procedura detekcije kolizije:

Kroz **CSMA/CD** komunikacija je bila moguća samo kao *half-duplex* prijenos podataka, što znači da je samo jedna stanica mogla slati u jedinici vremena. Takve, prvotne mrežne topologije su bile izgrađene oko centralnog vodiča (*bus*) ili oko centralnog uređaja - **huba** - na kojeg su bili spojeni ostali mrežni uređaji tvoreći fizički oblik zvijezde. Odatle i naziv – *star* topologija.

Hub je uređaj koji pojačava signal i povećava domet, ali ujedno proslijeđuje kolizije. Veliki broj uređaja na jednom mrežnom segmentu je dovodio do velikog broja kolizija i time smanjivao pozitivne karakteristike mreže.

Daljnjim razvojem tehnologije, pojavili su se, prvo *bridge*, a kasnije i *switch*. To su uređaji koji izoliraju kolizijske domene (područja kolizija). Switch je u osnovi bridge sa više portova (spojnih mjesta). Kao i hub switch ima više portova za spajanje mrežnih uređaja (računala). Razlika između huba i switcha je da se komunikacija dva uređaja preko huba čuje na svim portovima huba i time onemogućuje istovremena komunikacija neka druga dva uređaja preko tog huba, dok je ista komunikacija preko switcha izolirana samo na portove na kojima su spojeni uređaju koji trenutno komuniciraju. Istovremeno je moguća komunikacija neka druga dva uređaja preko druga dva porta

istog switcha.

Switchevi omogućuju *full-duplex* način komunikacije. Kod *full-duplex* načina rada oba uređaja koji komuniciraju mogu slati i primati podatke istovremeno, a da se ne dogodi kolizija.

Podaci koji šalju ethernetom su pakirani u okvire. Format okvira je za naveći broj ethernet tehnologija isti, tako da je moguća komunikacija između etherneta različitih brzina i tehnologija.

Ethernet okvir

Ethernet je danas postao *de facto* standard u primjeni u lokalnim mrežama. Jednostavan je za primjenu i održavanje, te uz današnje cijene opreme, dosta jeftin. Velika mu je prednost mogućnost jednostavnog proširenja mreže zamjenom postojećih ili dodavanjem novih switcheva. Od velike je pogodnosti što veliki broj proizvođača matičnih ploča ugrađuju mrežne kartice u ploče bez potrebe njihovog naknadnog dodavanja.

Više informacija na:

http://en.wikipedia.org/wiki/Ethernet

U današnje vrijeme, ukupna količina kreiranog sadržaja koju je potrebno razmjeniti koristeći računalne mreže (lokalne i internet) je gotovo nemjerljiva. Sustav koji omogućava razmjenu podataka je u neprestanom razvoju već nekoliko desetljeća i sastoji se od različitih vrsta opreme. Jedna od glavnih vidova podjele te opreme je podjela na **pasivnu** i **aktivnu** mrežnu opremu.

Ova podjela može biti zasnovana na dva kriterija:

Jedna od definicija navodi da aktivnu opremu sačinjavaju svi elektronički uređaji koji prihvaćaju i distribuiraju promet unutar računalnih mreža (imaju memoriju i procesor), dok pasivnu opremu sačinjava žični sustav (bakar i optika) koji služi za povezivanje aktivne opreme.

Pasivna oprema se sastoji od kablova, konektora, razvodnog panela (*patch panel, switching panel, punch-down panel*), komunikacijskih ormara i sustava za napajanje električnom energijom (vodovi, sklopke i naponske letve, sustav za hlađenje). *Hub* se može smatrati pasivnom opremom sa gledišta da nema nikakvu logičku funkciju usmjeravanja prometa. On samo pojačava primljeni signal i prosljeđuje ga dalje na sve svoje portove.

Kablovi služe za prijenos signala između računala i komunikacijske opreme. Za različite tipove signala se koriste različiti kablovi: bakar za prijenos napona i optički kabel za prijenos svijetlosnog signala.

Primjeri kabela:

- **koaksijalni kabel**: sastoji se od izoliranog (C), središnjeg bakrenog vodiča (D) oko kojeg je upletena bakrena ovojnica (B). Sve zajedno je izolirano vanjskom plastičnom izolacijom (A).

- konektori za koaksijalni kabel:

- **uvrnuta parica** (*Twisted Pair*): može biti bez zaštite od vanjskih smetnji (**UTP** – *Unshielded Twisted Pair*) ili sa zaštitom od vanjskih smetnji (**STP** – *Shielded Twisted Pair*). Sastoji se od 8 žica isprepletenih u parove (parice). Ta 4 para žica su omotana vanjskom ovojnicom, a mogu biti omotani u zaštitu protiv smetnji (STP).

- konektor i utičnica za UTP kabel:

- **optičko vlakno**: može biti *singlemode* (svjetlost ulazi u vodič pod samo jednim kutem) i *multimode* (svjetlost može ući u vodič pod više kuteva u određenom rasponu). Sastoji se od jezgre (core) koja vodi svijetlo i skupa ovojnica koji služe za zaštitu te jezgre.

Konektori za optička vlakna:

ST konektor

Ostala pasivna oprema:

- **patch panel**: služi za koncentriranje dolaznih kablova iz utičnica razmještenih po prostorijama koje pokriva lokalna mreža. Iz *patch* panela se tzv. *patch* kablovima povezuju računala spojena na dolazne kablove sa aktivnom opremom (obično *switch*).

- **komunikacijski ormar**: služi za smještaj pasivne i aktivne mrežne opreme (kablovi, *patch* paneli, *switchevi, routeri,* serveri,...).

- **naponska letva**: služi kao izvor napajanja za aktivnu opremu. Postavljaju se u komunikacijski ormar vodoravno ili okomito.

- **hub**: služi za pojačavanje primljenog signala (napona) kojeg šalje na sve svoje portove. Nema mogućnosti usmjeravanja prometa. O osnovi je to *repeater* (pojačivač signala) sa više portova (*multiport repeater*).

Aktivnu komunikacijsku opremu sačinjavaju uređaju koji koriste izvor električne energije i koji omogućuju aktivno upravljanje mrežnim prometom. Zajednička im je značajka da imaju procesor i memoriju. Na osnovu svojih značajki, namjene, operativnog sustava i ugrađenih programa donose odluku o putanji mrežnog prometa kojeg generiraju ili koji kroz njih prolazi.

Aktivna oprema se sastoji od računala i servera koji stvaraju promet, te **preklopnika** (*switch*) i **usmjerivača** (*router*) koji usmjeravaju promet od izvora do odredišta.

Switch služi za povezivanje dvaju računala unutar iste mreže (LANa) ili za povezivanje računala i *routera* za promet koji je namjenjen drugim mrežama. *Switch* povezuje parove koji komuniciraju na osnovu njihove fizičke adrese (**MAC** – *Media Access Control adresa*). *Switch* omogućuje komunikaciju više parova istovremeno. Primljeni promet na jednom portu prebacuje samo na jedan odgovarajući izlazni port (prema odredišnoj *MAC* adresi). Postoje različiti tipovi *switcheva* koji mogu imati i dodatne funkcionalnosti (usmjeravanje prometa po logičkim IP adresama).

Routeri služe za usmjeravanje prometa prema logičkim adresama (IP adrese). Iz zaglavlja primljenog paketa pročitaju odredišnu IP adresu i usporede je sa zapisom unutar svojih routing tabela. Ako pronađu odgovarajući zapis, takav paket prosljeđuju prema izlaznom portu na kojemu se nalazi dostupna odredišna mreža. U suprotnom se taj paket odbacuje. *Routeri* mogu imati više različitih vrsta portova. Najčešće su to *ethernet* portovi namjenjeni za komunikaciju sa lokalnim mrežama (LAN) i serijski portovi za komunikaciju sa udaljenim mrežama (WAN, Internet). *Routeri* međusobno razmjenjuju informacije o dostupnim mrežama.

Ako izuzmemo računala, aktivna i pasivna oprema uglavnom pokriva prva 3 sloja **OSI** referentnog modela. Pasivna oprema pripada prvom (fizičkom sloju), dok aktivna pokriva 2. (*switch – data link* sloj) i 3. sloj (*router*- mrežni sloj). Da bi ostvarili komunikaciju moramo zadovoljiti tražene standarde kroz svih 7. slojeva. Pri tome vodimo računa o tehničkim i funkcionalnim zahtjevima te komunikacije, te kompatibilnosti tehnologija koje ćemo u njoj koristiti.

Npr., ukoliko želimo omogućiti veće brzine prometa, veću pouzdanost i pokrivanje veće udaljenosti koristit ćemo optički kabel, taj kabel zahtijeva određene konektore za spajanje na aktivnu opremu (ovisno o vrsti porta), uređaj biramo prema funkciju koja nam je potrebna (*switching, routing*), broju priključaka i količini prometa, itd... Prema tome, aktivnu i pasivnu opremu biramo prema raznovrsnim zahtjevima komunikacije koju želimo ostvariti.

Mrežna topologija definira više različitih kategorija po kojima možemo utvrditi sastavne dijelove i način rada računalne mreže. Na osnovu tih kategorija možemo npr., razložiti mreže na manje sastavne dijelove i napraviti raspored (tlocrt) tih elemenata. Isto tako možemo opisati način pristupa tih manjih dijelova cijeloj mreži. Najčešća podjela mrežne topologije se odnosi na fizičku topologiju i logičku topologiju.

Mrežna topologija opisuje raspored i veze između pojedinih čvorova (računala, mrežnih uređaja,...), te putanju podataka unutar neke mreže. Fizička mrežna topologija prikazuje tlocrt fizičkog rasporeda

čvorova u mreži i njihove povezanosti.

Imamo više različitih fizičkih topologija:

Point-to-point mrežna topologija se sastoji od dva čvora i veze (*linka*) između njih. Ti čvorovi međusobno neposredno komuniciraju.

Veza između čvorova može biti stalna (*permanent*) ili dinamička (*circuit switched, packet switched*). *Circuit switched* je veza kod koje se uspostavlja komunikacijski kanal prije nego što može krenuti razmjena podataka (telefonski poziv). *Packet switched* je veza kod koje se dijelovi podataka pakirani u pakete usmjeravaju preko dijeljenih veza između dva čvora koji komuniciraju. Za povezivanje se može koristiti bilo koji od medija.

Bus mrežna topologija se sastoji od centralnog vodiča na koji su spojeni čvorovi koji komuniciraju. Taj vodič ima dva kraja koji moraju biti pravilno *terminirani* da bi se onemogućila refleksija ili odbijanje signala i time smanjile smetnje na mediju.

Svi podaci u razmjeni se šalju preko tog centralnog vodiča i taj promet "čuju " svi ostali čvorovi na tom mrežnom segmentu. Prekid u busu dovodi do prestanka u komunikaciji između svih čvorova. Kao medij se koristi koaksijalni kabel.

Star mrežna topologija se stastoji od središnjeg čvora (koncentratora) na kojega su kablovima direktno spojeni ostali čvorovi na mreži. Ulogu koncentratora obično imaju *hub* (rijetko) ili *switch* (češće).

Čvorovi međusobno komuniciraju šaljući podatke kroz *switch*. Ako je koncentrator *hub*, istovremeno mogu komunicirati samo dva čvora. Ako je koncentrator *switch*, istovremeno mogu komunicirati više parova čvorova. Ako centralni čvor prestane raditi, cijela mreža ne radi. Prekid rada bilo kojeg drugog čvora na mreži, osim centralnog, ne utječe na komunikaciju ostalih čvorova u tom mrežnom segmentu. Ova topologija, sa svojim podvrstama, je najčešći oblik povezivanja unutar lokalnih mreža (LAN). Kao medij za povezivanje se koriste različiti tipovi UTP kabela.

Fizička **ring** topologija se sastoji od čvorova koji su povezani samo sa dva susjedna čvora, a prvi i posljednji su međusobno povezani tvoreći fizički krug.

Podaci putuju u krug od jednog do drugog čvora i obično u samo jednom pravcu. Postoji i dvostruka ring topologija (dual-ring) sa po dvije veze između svaka dva čvora. Obično se koristi samo jedan prsten, dok drugi služi kao backup u slučaju kvara na prvom. Kao medij se koriste različiti oblici bakrenih i optičkih vodiča.

Tree topologija se sastoji od centralnog (root) čvora koji je najviši u hijerarhijskom rasporedu čvorova i na njega spojenih čvorova koji se nalaze na sloju niže od njega. Čvorovi nižeg sloja opet mogu imati na sebe spojene čvorove još nižeg sloja, itd...

Da bi neka mreža imala odlike tree topologije potrebno je da ima najmanje tri sloja. Ukupan broj point-to-point veza između čvorova će biti za jedan manji od broja čvorova. Kao medij se koriste različiti oblici bakrenih i optičkih vodiča.

Mesh topologija se sastoji od čvorova koji mogu imati direktne veze sa više (*partial*) ili sa svim čvorovima u mreži (*full mesh*).

Potpuna *mesh* topologija je preskupa i presložena za primjenu tako da se koristi samo na mjestima gdje je to krajnje nužno (obično nuklearne centrale) i gdje nema veliki broj čvorova koje je potrebno povezati.

Logička mrežna topologija prikazuje tlocrt putanje podataka koji putuju između čvorova na mreži. Logičke topologije su najčešće povezane sa načinom na koji se pristupa mediju za slanje podataka (*MAC – Media Access Control*). One se oslanjaju na primjenu unutar komunikacijskih protokola, a ne na sami fizički tlocrt mreže.

Npr., nije nužno da logička ring topologija bude istovremeno i fizička ring topologija. Kod *IBM Token*

Ring (802.5) topologije, mreža ima izgled prstena na drugom sloju (*Data Link* sloju) dok je na prvom sloju (fizičkom) oblika zvijezde (*star topology*). Token služi kao znak za dozvolu predaje podataka na mrežu i šalje se kružno od čvora do čvora, ali nije isključivo vezan za fizičku *ring* topolologiju. Može se primjenjivati i na drugima. Logičke topologije je moguće dimanički konfigurirati pomoću *routera* i *switcheva.*

Više na:

http://en.wikipedia.org/wiki/Network_topology

Da bismo mogli razlikovati računala na mreži potreban nam je sustav koji će ih imenovati na način da svako od računala ima neku jedinstvenu oznaku. U lokalnim mrežama, taj cilj postižemo koristeći mrežno adresiranje. Kod *etherneta*, adresiranje je sastavljeno od fizičkog i logičkog adresiranja.

Fizičko adresiranje se odvija na drugom sloju OSI referentnog modela. Za njega je zadužen podsloj *Data Link* sloja koji se naziva *Media Acess Control (**MAC**)*. MAC podsloj je orjentiran prema fizičkom sloju i ima zadaću upravljati pristupom mediju. Svaka mrežna kartica u sebi sadrži jedinstveni identifikator – MAC adresu (*hardwareska* adresa, *ethernet* adresa). Ona je sadržana u svim mrežnim karticama i svim ugrađenim mrežnim adapterima u mrežnim uređajima (*router*, *switch*). Zapisana je unutar hardwarea mrežnih kartica (unutar **ROM** -a na kartici; *Read Only Memory* – oblik memorije dostupan samo za čitanje, obično čip na kartici).

MAC adresa je broj koji označava neku mrežnu karticu. Sastoji se od 48 bitova (6 okteta) koji se zapisuje u obliku 12 hexadecimalnih znamenki na više različitih načina grupiranja i odvajanja znamenki:

MAC adresa je logički podjeljena u dva dijela. Prva tri okteta (24 bita ili prvih 6 hexadecimalnih znamenki) predstavljaju oznaku proizvođača mrežnih kartica i za sve kartice tog proizvođača su isti. Druga tri okteta (drugih 6 hexadecimalnih znamenki) su jedinstveni za svaku karticu i dodjeljuje ih proizvođač.

Iako je zamišljeno da MAC adresa u potpunosti jedinstveno predstavlja neki mrežni uređaj, to nije tako, jer na većini današnjih mrežnih kartica postoji mogućnost promjene MAC adrese. Taj postupak se naziva MAC *spoofing*.

Kod MAC adresiranja postoji nekoliko načina grupiranja adresa ili pozivanja rezerviranih MAC adresa. Najznačajnija je *broadcast* adresa koji služi da bi se neki okvir (okvir – oblik pakiranja podataka na drugom sloju) poslao na sve adrese u tom mrežnom segmentu (npr., unutar LAN-a). *Broadcast* MAC adresa se sastoji od svih jedinica na pozicijama bitova MAC adrese i u hexadecimalnom obliku se zapisuje kao **ff-ff-ff-ff-ff-ff**.

Da bi slali podatke u *ethernetu*, potrebno je da uređaj poznaje i *hardwaresku* i logičku (IP) adresu. *Address Resolution Protocol* (**ARP**) je protokol pomoću kojega pronalazimo MAC adresu računala kojemu šaljemo podatke ukoliko je poznata samo njegova IP adresa.

IP adresa (Internet Protocol) je adresa mrežnog sloja. Ona je logička adresa koja se dodjeljuje uređaju kojega želimo spojiti na mrežu. Adrese koje se usmjeravaju preko interneta trebaju biti jedinstvene. Pošto je IP adresa logička adresa koja se može mijenjati i često se dinamički dodjeljuje, ne može se reći da ona jedinstveno identificira određeni mrežni uređaj. Umjesto toga, ona samo omogućuje pronalaženje uređaja i usmjeravanje toka podataka do njega.

Trenutno su u upotrebi dvije verzije IP protokola: verzija 4 (IPv4) i verzija 6 (IPv6). IPv4 adresa se sastoji od 32 bita, a IPv6 adresa ima 128 bitova. IPv6 je razvijen zbog nedostatka adresa u IPv4 verziji.

Zbog lakšeg rada sa IPv4 adresama, one se bilježe brojevima decimalnog brojevnog sustava. 32 bita IPv4 adrese su podjeljena u 4 okteta. Svaki od okteta je odjeljen od slijedećeg sa točkom. Zatim je svaki od okteta iz binarnog brojevnog sustava prebačen u decimalni sustav. Na taj način smo dobili adresu sastavljenu od 4 decimalna broja odjeljena točkom i sa njom je lakše podešavati uređaje. Taj

način označavanja se još naziva i *dotted decimal*. Primjer IP adrese je 192.168.1.2.

Decimalne vrijednosti svakog od okteta se mogu kretati od 0 do 255. Od 8 bitova koji se nalaze unutar okteta moguće je dobiti 256 različitih brojčanih vrijednosti (2^8=256). Prva vrijednost je 0, a posljednja 255, sveukupno 256. Broj 2 se uzima kao baza kalkulacije jer jedan bit može imati 2 stanja: 0 ili 1.

IPv4 adresa je logički podjeljena u dva dijela: dio koji je namjenjen adresiranju mreže u kojoj se uređaj nalazi i dio koji koji označava sam uređaj. Maska podmreže (*subnet mask*) nam omogućuje razlučiti koji je koji dio IPv4 adrese.

Adrese su podjeljene po klasama. Najčešće se koriste A, B i C klase adresa. Klasi A IPv4 adresa pripadaju sve adrese kojima prvi oktet počinje sa brojem između 1 i 126 (npr., 15.8.3.240, 111.16.12.9, itd). Zadana (*default*) subnet maska definira prvi oktet kao mrežni dio adrese, a ostatak je *host* dio (255.0.0.0 ili /8). "/8" označava broj bitova sa vrijednosti 1 unutar *subnet* maske.

Adresa koja počinje sa 127 je rezervirana IPv4 adresa. 127.0.0.1 je *loopback* adresa i služi za provjeru da li je TCP/IP instaliran i funkcionalan na računalu. Nalazi se na svakom računalu sa intaliranim TCP/IP protokolom.

Klasi B IPv4 pripadaju sve adrese kojima prvi oktet počinje brojem između 128 i 191 (npr, 131.56.14.3, 176.192.128.4, itd). Zadana *subnet* maska definira prva dva okteta kao mrežni dio adrese, a ostatak je *host* dio (255.255.0.0 ili /16).

Klasi C IPv4 pripadaju sve adrese kojima prvi oktet počinje brojem između 192 i 223 (npr., 198.184.16.5, 218.115.68.90, itd). Zadana *subnet* maska definira prva tri okteta kao mrežni dio adrese, a ostatak je *host* dio (255.255.255.0 ili /24).

Zbog kroničnog nedostatka adresa za IPv4, adrese su podjeljene u javne i privatne. Javne su one adrese koje se mogu usmjeravati preko interneta. Privatne IPv4 adrese se ne mogu usmjeravati preko interneta, već se podešavaju u zatvorenim privatnim mrežama unutar tvrtki ili organizacija.

Da bi računalo sa privatnom adresom komuniciralo sa onima na internetu, koriste se tehnologije mrežnog prevođenja adresa (**NAT** – *Network Address Translation*). Router na kojemu je podešen NAT mjenja privatnu adresu sa svojom javnom koja se usmjerava internetom. Nakon dobivenog odgovora, od udaljenog računala, ponavlja postupak, ovaj put mjenjajući javnu adresu sa odgovarajućom privatnom adresom računala koje je uputilo zahtjev. Na taj način se štede IPv4 adrese jer se veliki broj privatnih adresa može mjenjati sa jednom ili manjim brojem javnih adresa.

Kao privatne adrese mogu se koristiti odgovarajuće rezervirane adrese. Svaka od klasa adresa ima rezervirane privatne adrese:

Adrese se mogu podešavati ručno za svakog od klijenata ili oni mogu dinamički naučiti o svojim mrežnim postavkama. **DHCP** (*Dynamic Host Configuration Protocol*) je protokol koji se koristi da bi klijenti na mreži dobili različite parametre koji su im potrebni da bi mogli raditi u IP mreži. Neki od parametara dodjeljeni uz pomoć DHCP-a su IP adresa, *subnet* maska, zadani *gateway* (adresa uređaja koji komunicira sa drugim mrežama), adrese **DNS** servera (**DNS** – *Domain Name System* radi pretvaranje imena domene u IP adresu), itd... Ovaj protokol značajno smanjuje vrijeme potrebno mrežnim administratorima za podešavanje mreže na klijentima.

Podmreža ili ***subnet*** (*eng. subnet = sub-network*) predstavlja manju mrežu unutar neke veće mreže. Najmanja mreža, koje nema dodatnih podmreža, se naziva ***broadcast* domena**, što u osnovi predstavlja jednu lokalnu mrežu – **LAN**. Unutar *broadcast* domene mrežni uređaji (računala, komunikacijska oprema,...) međusobno komuniciraju direktno, koristeći fizičke (***MAC- Media Access Control***) adrese.

Početna i završna adresa unutar podmreže imaju posebna značenja i uglavnom se ne koriste kao adrese pojedinog mrežnog uređaja. Početna adresa je adresa podmreže (***Network ID***) koja identificira cijelu podmrežu. Kad želimo označiti cijelu podmrežu koristimo adresu podmreže.

Završna ili ***broadcast*** adresa (***Broadcast ID***) je adresa na kojoj mrežni promet primaju sva računala unutar podmreže. Kad želimo poslati podatke svim uređajima u podmreži koristimo *broadcast* adresu.

Usmjerivači (***routeri***) se koriste za povezivanje podmreža. Njihova uloga je da promet primljen sa jedne mreže, a koji je namjenjen drugoj mreži, preusmjere na tu drugu mrežu. *Broadcast* promet je namjenjen svim računalima unutar samo jedne mreže. *Routeri* ne preusmjeravaju promet s neke mreže na tu istu mrežu i ne prenose *broadcast* promet sa jedne mreže na drugu. Za *routere* uglavnom vrijedi pravilo da izoliraju *broadcast* domene. U određenim slučajevima moguće je dopustiti *routerima* prijenos *broadcast* prometa (npr. za **DHCP** - ***Dynamic Host Configuration Protocol*** - automatsko dodjeljivanje mrežnih postavki mrežnim uređajima).

Subnet može:

Subnetiranje se koristi za bolju kontrolu mrežnog prometa, omogućuje razvrstavanje mrežnog prometa na osnovu postavki mreže, te povećava sigurnost mreže tako što objedinjuje računala (***hostove***) u logičke grupe.

IP (***Internet Protocol***) adresa, u verziji 4 IP protokola, je duga 32 bita. Dio bitova unutar IP adrese definira mrežu (***network***), a ostatak bitova definira dio adrese namjenjen označavanju mrežnih uređaja (***hostova***). Svaka IP adresa dolazi uz pripadajuću masku podmreže (***subnet mask***). Uz pomoć *subnet* maske možemo razlučiti koji dio adrese je *network* dio, a koji je *host* dio. Primjenjujući *subnet* masku dolazimo do adrese mreže i *broadcast* adrese.

IP adrese su podjeljene u nekoliko klasa. Najčešće se koriste klase A, B i C. Svaka od klasa ima zadanu (*default*) *subnet* masku.

Subnet maska se bilježi i u ***dotted decimal*** notaciji. *Dotted decimal* bilježenje IP adrese je nastalo radi lakšeg rada i upravljanja sa IP adresama.

Kao i drugi podaci u računalu, IP adresa i *subnet* maska su binarnog oblika. Kod *subnet* maske, bitovi mreže su označeni brojem 1, a host bitovi su označeni nulom. Da bi ljudi lakše radili sa IP adresama i *subnet* maskama, njihova 32 bita su podjeljena u 4 grupe po 8 bitova koji su odvojene točkom. Svaka od tih grupa je iz binarnog prebačena u decimalni sustav.

Prema tome, zadana subnet maska za klasu A je iz oblika:

11111111000000000000000000000000

prešla u oblik

11111111.00000000.00000000.00000000

pa na kraju u oblik

255.0.0.0

Sukladno prethodnom, *default subnet* maska za klasu **B** je **255.255.0.0**, a za klasu **C** je **255.255.255.0**.

Primjer 1. Određivanje mrežne adrese

Primjenom *subnet* maske na neku *host* adresu rezlučiti ćemo kojoj mreži taj *host* pripada, tj. koja je njegova mrežna adresa.

Zadana je IP adresa:

192.168.1.5

Ova adresa je privatna adresa klase C. Zadana (*default*) *subnet* maska za klasu C je /24. /24 znači da su 24 bita rezervirana za definiranje mrežnog dijela IP adrese. Ostalih 8 (od ukupno 32) je rezervirano za *host* dio adrese.

Network bitovi su predstavljeni sa 1, a host bitovi sa 0.

Ovo je binarni prikaz default subnet maske klase C:

11111111111111111111111100000000

U *dotted decimal* zapisu je to:

255.255.255.0

Da bismo doznali tražene informacije potrebno je zadanu adresu također pretvoriti u binarni oblik:

192.168.1.5 = 11000000101010000000000100000101

Na dobivene binarne brojeve primjenjujemo logičku operaciju **I** ***(AND)***. Logička operacija **I** daje vrijednost 1 ako svi operandi imaju vrijednost 1 (npr., u operaciji 2+3=5; 2 i 3 su operandi).

Primjer logičke operacije ***AND***

Primjenjeno na naš primjer:

	11000000101010000000000100000101 (192.168.1.5)
AND	11111111111111111111111100000000 (255.255.255.0)
	11000000101010000000000100000000 (192.168.1.0)

Tražena adresa mreže je **192.168.1.0**

Unutar klasa IP adresa postoje određene adrese koje se ne usmjeravaju preko interneta. One su namjenjene samo za uporabu unutar izoliranih, privatnih mreža. Takve adrese se nazivaju **privatne adrese**. Ukoliko računalo sa privatnom adresom "želi" izaći na inteternet, njegova privatna adresa se zamjenjuje sa javnom adresom koju je moguće usmjeravati preko interneta. Taj postupak se naziva ***Network Address Translation (NAT).***

Slijedeći blokovi adresa su rezervirani za privatnu uporabu:

Također, unutar svake podmreže postoje adrese koje se ne mogu dodjeliti *hostovima*. Ako neka mrežna adresa u svom *host* dijeli ima sve 0, onda ona predstavlja mrežnu adresu, a ako u svom host dijelu ima sve 1, onda je ona *broadcast* adresa.

Ova pojava dovodi do gubitka velikog broja adresa jer mrežne i broadcast adrese nisu upotrebljive za označavanje hostova. Noviji standardi rješavaju ovaj problem, ali se zbog starijih, neprilagođenih mrežnih uređaja još uvijek primjenjuje pravilo o nekorištenju mrežnih i broadcast adresa za označavanje *hostova*.

Gubitak IP adresa je postao veliki problem jer se javio nedostatak javnih IP adresa potrebnih za adresiranje uređaja na internetu.

Primjer 2. Gubitak IP adresa

Trebamo adresirati 38 uređaja, adresom klase C.

Klasa C ima 8 bitova za označavanje *hostova* (prva 24 bita su mrežni bitovi).

Ukupan broj hostova je $2^8 = 256$. Označavanje hostova počinje sa brojem 0, a ne sa brojem 1, pa to onda daje raspon od 0 do 255.

Baza je broj 2 zato što svaki bit može imati dvije vrijednosti: 0 ili 1. Eksponent je 8 jer imamo ukupno 8 bitova za određivanje broja *hostova*.

Ako uzmemo mrežnu adresu 192.168.1.0/24 i njome adresiramo 38 hostova dobit ćemo adrese:

Sve adrese od 192.168.1.39 do 192.168.1.254 su neiskorištene. (192.168.1.255 se ne koristi jer je to broadcast adresa). Na ovaj način smo izgubili 216 adresa.

Da bi izbjegli gubitak adresa iz prethodnog primjera, možemo zadanu IP adresu dodatno *subnetirati*. To radimo na način da od host *bitova* uzmemo dio bitova i dodjelimo ih mrežnom dijelu adrese.

Primjer 3. Subnetiranje

Obraditi ćemo adrese iz prethodnog primjera: iz mreže 192.168.1.0 trebamo odrediti podmrežu (*subnet*) koja će imati dovoljno adresa za adresiranje 38 hostova.

Mrežu 192.168.1.0 ćemo podjeliti u podmreže, tako što ćemo iz host dijela adrese uzeti odgovarajući broj bitova i dodijeliti ih mrežnom dijelu adrese.

Adresa 192.168.1.0 je adresa klase C, sa *default subnet* maskom /24.

Ostaje nam 8 bitova za hostove.

Od tih 8, dio treba ostaviti za hostove, a dio dodjeliti mreži.

Potrebno je adresiranje 38 hostova.

Rješenje je da od *host* bitova, 6 bitova ostavimo za adresiranje računala, a 2 bita možemo pripojiti mrežnom dijelu. Sa 2 bita dodjeljena mreži 192.168.1.0, može se dobiti ukupno 4 podmreže.

Nažalost, zbog starijih standarda koje smo spomenuli ranije, sve te podmreže nisu iskoristive za adresiranje. Podmreže koje imaju vrijednost bitova sve 0 ili sve 1, ne mogu se koristiti za adresiranje podmreža. Isto vrijedi i za *hostove*. Ako su vrijednost host dijela sve 0, onda je to adresa podmreže, a ako su sve 1, onda je to *broadcast* adresa.

Zbog toga ukupan broj podmreža dijelimo na iskoristivi i na neiskoristivi dio. Do iskoristivog dijela dođemo po formuli:

2^n-2

n je broj bitova za podmreže (ista se primjenjuje i za računanje broja *hostova*, pa je tada **n** broj bitova za *hostove).*

Od ukupnog broja se oduzimaju dvije podmreže – mrežna i *broadcast* adresa. Isto vrijedi kod računanja *hostova*.

4 podmreže koje smo dobili imaju svaka po 64 *hosta* i to su:

Prva i zadnja se ne koriste (*network i broadcast*) i ostaju nam 2. i 3. podmreža. Druga mreža je, u biti, prva iskoristiva mreža. Adresa te mreže je 192.168.1.64, a *broadcast* adresa je 192.168.1.127.

Prva adresa koja se može iskoristiti za adresiranje *hostova* je 192.168.1.65.

U zadatku se traži 38 host adresa, pa je raspon nama potrebnih adresa od 192.168.1.65 do 192.168.1.102.

Na ovaj način smo sačuvali dio adresa jer 3. podmrežu (drugu iskoristivu) možemo iskoristiti za adresiranje neke druge mreže. U prvom slučaju smo izgubili 216 adresa, a ovdje je izgubljeno 128 (1. i 4. podmreža). Gubitak je moguće još smanjiti podešavanjem novijih ruotera za uporabu (uvjetno) neiskoristivih adresa.

U prethodnom primjeru smo vidjeli da je ista *subnet* maska primjenjena na sve podmreže. Problem može nastati ako su naše potrebe za adresiranjem više mreža sa različitim brojem hostava, a na raspolaganju imamo samo određen raspon adresa sa *defaultnom subnet* maskom (kao u prethodnom primjeru: adresa je 192.168.1.0/24, a trži se 38 host adresa).

Za riješenje tog problema se koristi **VLSM** (***Variable Length Subnet Mask***). **VLSM** predstavlja način podjele IP adresa prema pojedinim zahtjevima svake mreže, a ne prema nekim općenitim normama adresiranja (npr., ne prema zadanoj *subnet* maski neke mreže).

Primjer 4. **VLSM**

Recimo da se pored potrebe adresiranja 38 hostova i jednoj mreži, što smo obradili u prethodnom primjeru, javila potreba adresiranja još nekoliko podmreža sa različitim brojem hostova:

Izračun za mrežu b sa 15 *hostova*

Prva iskoristiva mreža, iz prijašnjeg primjera, je iskorištena za adresiranje 38 hostova. Zaključili smo da je raspon mrežnih adresa 2. iskoristive mreže od 192.168.1.128 – 192.168.1.19.

Nama je potrebno adresirati još 3 mreže sa po 15, 10 i 2 *hosta*. Prvo ćemo subnetirati za mrežu sa najvećim brojem *hostova* (15) i dalje padajući po veličini.

Za adresiranje 15 *hostova* potrebno je od host dijela adrese uzeti 5 bitova za *host* adrese,a 3 nam ostaju za podmreže. Sa 5 bitova možemo adresirati 2^5=32 *hosta* (nama je potrebno 15). Nismo uzeli 4 bita je prema formuli 2^n-2=2^4-2=14 ostaje nam samo 14 *host* adresa, što nije dovoljno.

Adresa mreže koju možemo koristiti je 192.168.1.128. Subnet maska te mreže je /26 (24 default bita + 2 bita prethodnog subnetiranja). U *dotted decimal* notaciji je to 255.255.255.192

Subnet maska nove podmreže je /27 (24 default bita + 3 bita podmreže koja su ostala nakon što smo 5 bitova rezervirali za hostove). Ili 255.255.255.224

Sumarno:

Raspon adresa slijedeće iskoristive podmreže je: 192.168.1.160 – 192.168.1.191

Rasponi

nisu iskoristivi jer su sadržani unutar 4. *subneta* iz primjera 3. (*broadcast* podmreža 192.168.1.192 – 192.168.1.255).

Izračun za mrežu c sa 10 *hostova*

Trebamo adresirati 10 *hostova.*

Zadnja iskoristiva mreža ima raspon 192.168.1.160 – 192.168.1.191.

Za adresiranje 10 *hostova* trebamo 4 bita (2^n-2=2^4-2=14 mogućih *host* adresa).

Subnet maska je /28 (24 *default* bita + 4 bita podmreže koja su ostala nakon što smo 4 bita rezervirali za hostove).

Podmreže su raspona

Sumarno:

Izračun za mrežu d sa 2 *hosta*

2 bita za *hostove* = 2 *host* adrese (2^n-2=2^2-2=2)

6 bitova za mrežu

/30 *subnet* maska (24 + 6)

Sumarno:

U ovim primjerima su korištene IP adrese klase C koje se i inače najčešće koriste u privatnim mrežama. Na isti način se subnetira za bilo koju klasu adresa.

Primjer 5. Subnetiranje adrese klase B

Trebamo adresirati 485 *hostova.*

Zadana mrežna adresa je 172.16.0.0/16

Za 485 *hostova* trebamo 9 bitova rezervirati za *host* dio. 7 ostaje za mreže.

Ukupan broj *hostova* po jednoj podmreži mreži je 2^n-2=2^9-2=510.

Ukupan broj podmreža je 2^n-2=2^7-2=126.

/23 je *subnet* maska (16+7); ili 255.255.254.0

Raspon *subneta:*

Sumarno:

Classfull adresiranje koristi *default subnet* masku za neku adresu. Nedostatak mu je što se, bez obzira na stvarne potrebe, troši prevelik broj IP adresa. Ako se ukine sustav razvrstavanja adresa po klasama, moguće je uštediti te adrese.

Classless Interdomain Routing (CIDR) je uveden kao mehanizam koji poboljšava iskoristivost adresnog prostora i skalabilnost usmjeravanja prometa preko interneta. Kod **CIDR**-a je napravljen odmak od tradicionalne podjele mreža na klase, te su mreže predstavljene IP adresom i brojem bitova u *subnet* maski (npr. 192.168.1.0/24).

Više na:

http://www.semsim.com/ccna/tutorial/subnetting/subnetting.html

Cilj usmjeravanja (engl. routing) prometa u mreži je osigurati dostupnost toka podataka od izvorišta do odredišta i pri tome optimalno iskoristiti mrežu te osigurati zadovoljavajuću kvalitetu usluge. Tu funkciju ostvaruju **usmjernici** (engl. router). Usmjernici za usmjeravanje koriste **usmjerivačke protokole**. Usmjerivački protokoli omogućuju mreži dinamičko prilagođavanje uvjetima. Odluke o usmjeravanju ne moraju biti unaprijed određene i nepromjenjive.

Postoje dvije osnovne vrste usmjerivačkih protokola, a dijele se prema načinu izračunavanja optimalnog puta na:

Protokoli vektora udaljenosti određuju najbolji put na osnovu informacije koliko je udaljeno odredište paketa. Udaljenost može biti broj usmjernika do odredišta, a može biti i kombinacija nekih vrijednosti koje će definirati tu udaljenost. Susjednim usmjernicima se šalje cijela tablica usmjeravanja. Ovi protokoli su jednostavni i učinkoviti u malim mrežama te su laki za konfiguriranje. Najpoznatiji protokol vektora udaljenosti je RIP (Routing Information Protocol) i bit će razmatran u kasnije. Za velike mreže protokoli vektora udaljenosti imaju loša konvergencijska svojstva pa su zato razvijeni usmjerivački protokoli s boljim svojstvima, a to su protokoli stanja veze.

Protokoli stanja veze rade na način da svaki usmjernik zna topologiju mreže i ne šalje se cijela tablica usmjeravanja, nego se svim usmjernicima u mreži šalje samo informacija o stanju veze u obliku malih LSA (Link State Advertisement) paketa. Na osnovu dobivenih informacija usmjernici ponovo izračunaju puteve. Ova metoda je pouzdanija, troši manje pojasne širine (engl. bandwidth) mreže i jednostavnije je otkloniti nastalu pogrešku, nego u slučaju protokola vektora udaljenosti. Negativne strane ovakvog pristupa su što se koristi kompleksniji algoritam što znači veće opterećenje procesora usmjernika i veća potrošnja memorije. U nastavku će biti razmatran OSPF kao predstavnik protokola stanja veze.

Usmjerivački protokoli se također dijele na:

Unutarnji se koriste za usmjeravanje prometa unutar autonomnog sustava (npr. unutar CARNet mreže), a vanjski se koriste za usmjeravanje prometa između autonomnih sustava (npr. između CARNeta i GEANTa). **Autonomni sustav** (AS) se najčešće poklapa s administrativnim granicama mreže.

Primjeri unutarnjih usmjerivačkih protokola su već spomenuti RIP i OSPF, a možemo spomenuti i IS-IS. Primjer vanjskog protokola usmjeravanja je BGP.

RIP (Routing Information Protocol) je najstariji usmjerivački protokol koji se primjenjuje na internetu.

Formalno je definiran RFC-om 1058 i RFC-om 2453 (RIP verzija 2). Razvijen je za lokalne mreže, počeo se isporučivati s BSD inačicom UNIX operacijskog sustava, 80-ih godina i zasniva se na razašiljanju (engl. broadcast).

RIP šalje nove usmjerivačke poruke u pravilnim intervalima ili kada se promjeni topologija mreže. Kada usmjernik dobije usmjerivačku poruku koja uključuje promjene, nadograđuje tablicu usmjeravanja da bi prikazao novi put. Vrijednost metrike za put se uvećava za 1 i pošiljatelj se smatra sljedećim korakom.

Kod RIP protokola usmjernici čuvaju samo najbolji put, tj. put sa najmanjom vrijednošću metrike, prema odredištu, tj. ako nova informacija nudi bolji put ona zamjenjuje staru. Nakon nadogradnje tablice usmjeravanja, usmjernik informira susjedne usmjernike o promjeni.

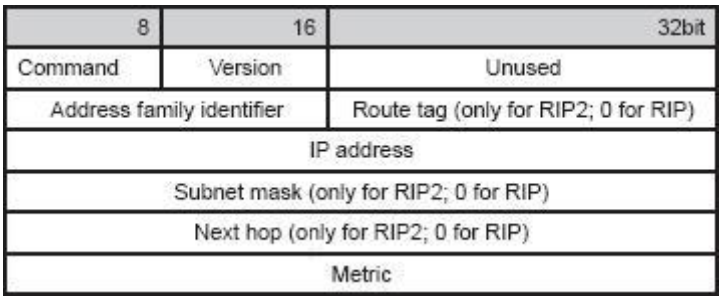
RIP kao metriku koristi broj skokova tj. odabire smjer s najmanjim brojem skokova kao najbolji. Broj skokova je broj usmjernika koji paket treba proći na putu do odredišta. Svaki skok na putu od izvorišta do odredišta vrijedi 1, ako nije drugačije definirano. Kada usmjernik dobije usmjerivačku poruku koja sadrži novo ili promijenjeno odredišno mrežno sučelje dodaje 1 vrijednosti metrike naznačenoj u usmjerivačkoj poruci i unosi mrežu u tablicu usmjeravanja. Unutar RIP tablice usmjeravanja najdulji put može biti 15 skokova. Ako je broj skokova veći od 15 smatra se da je odredište nedohvatljivo.

Kada usmjernik detektira prekid jedne od svojih veza korigira svoju tablicu usmjeravanja tako da postavi broj koraka za taj smjer na 16 i susjednim usmjernicima šalje svoju tablicu usmjeravanja. Svaki usmjernik koji primi ovu poruku korigira vlastitu tablicu usmjeravanja i šalje ju dalje. Promjena se tako propagira mrežom.

RIP ima i mnogo drugih stabilnosnih dodataka koji su zajednički za mnoge usmjerivačke protokole. Ove mogućnosti osiguravaju stabilnost zbog potencijalno brzih promjena u topologiji mreže. Neke od tih mogućnosti su:

Routing-Update Timer broji interval između periodičkih nadopuna. Ako nije drugačije definirano postavljen je na 30s. RIP svakih 30 sekundi šalje tablicu usmjeravanja svojim susjedima. Ukoliko nakon 180 sekundi nije dobio potvrdu smjera u tablici, smjer se proglašava neispravnim tj. postavlja se broj skokova na veće od 15, a ukoliko u daljnjih 120 sekundi ne dobije potvrdu smjera smjer se briše iz tablice usmjeravanja. Ako usmjernik detektira prekid veze, on nakon što ažurira vlastitu tablicu, odmah šalje svoju tablicu susjednim usmjernicima ne čekajući istek 30 sekundi.

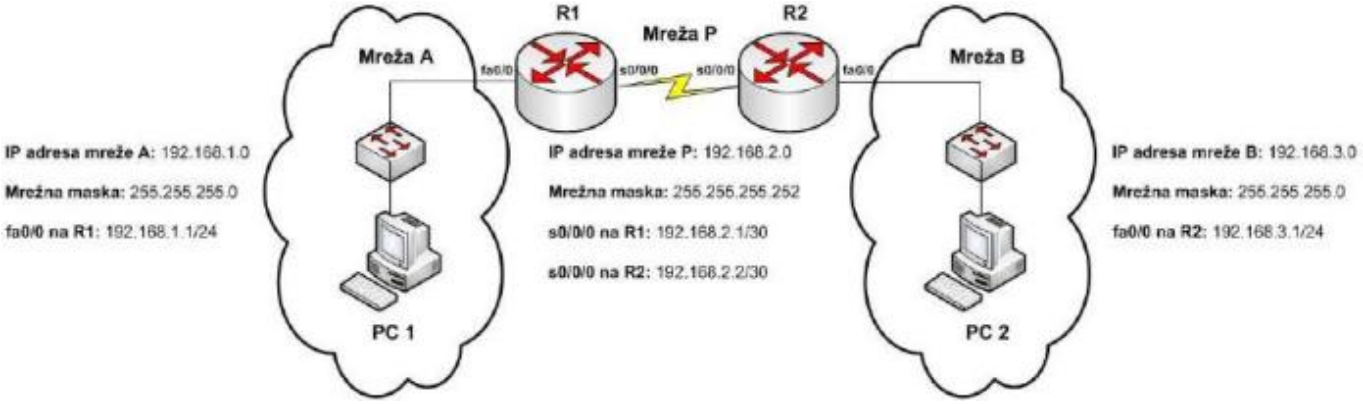
Format RIP verzije 2 paketa prikazan je na slici:



RIPv2 paket se sastoji od sljedećih polja:

Konfiguracija RIP protokola na Cisco usmjerniku

Bit de prikazana konfiguracija RIP protokola usmjeravanja na Cisco usmjerniku za mrežu prikazanu na slici:



Pretpostavljamo da su adrese dodijeljene po adresnoj shemi sa slike te da se nalazimo u privilegiranom načinu rada (engl. privileged mode). Privilegirani način rada je naznačen znakom "#".

Konfigurirat ćemo RIP na usmjerniku R1:

Naredbom configure terminal ulazimo u konfiguracijski način rada (engl. configuration mode) koji je naznačen s ImeUsmjernika(config)#.

Naredbom router rip ulazimo u konfiguracijski način rada RIP protokola.

Sada nizom network naredbi navodimo adrese svih mreža koje pripadaju usmjerniku R1.

Time je završena konfiguracija RIP protokola na usmjerniku R1.

Analogno na usmjerniku R2 izvršimo sljededi niz naredbi:

Time je završena konfiguracija RIP protokola na usmjerniku R2.

Nakon što usmjernici razmijene tablice usmjeravanja računala mreža A i B mogu međusobno komunicirati.

OSPF (Open Shortest Path First) usmjerivački protokol je otvoren, što znači da su njegove specifikacije javne. Definiran je RFC-om 2328 (OSPFv2). Koristi Dijkstra SPF algoritam za pronalaženje najkraćeg puta.

OSPF je protokol stanja veze koji zahtjeva slanje obavijesti o stanju veze (LSA-s) ostalim usmjernicima unutar istog hijerarhijskog prostora. Metrika OSPF-a računa se po formuli:

$$C = \frac{10^8}{\text{Pojasna širina (bit/s)}}$$

Iz formule je razvidno da je cijena puta obrnuto proporcionalna pojasnoj širini neke veze. Dakle, veza 100 Mb/s ima veću cijenu, nego veza 1 Gb/s, a paket će biti usmjeren na put s manjom cijenom.

OSPF radi hijerarhijski. Najveća jedinica hijerarhije je **autonomni sustav**. Iako je OSPF unutarnji usmjerivački protokol, sposoban je komunicirati s drugim autonomnim sustavima. Autonomni sustavi su podijeljeni u **područja** (engl. area), a usmjernici mogu biti članovi više područja.

Granični usmjernici (engl. Area Border Routers) održavaju topološku bazu za svako područje. **Topološka baza** sadrži skup LSA-ova svih usmjernika u istom području. Ako su usmjernici unutar istog područja onda imaju jednake topološke baze. Topologija područja je nevidljiva entitetima izvan tog područja. Razdvajanje područja stvara dva različita tipa OSPF usmjeravanja, ovisno o tome jesu li izvorište i odredište u istim ili različitim područjima. **Intraprostorno usmjeravanje** se javlja kada su izvorište i odredište u istom području, a **interprostorno usmjeravanje** kada su u različitim područjima. **Područje okosnice** (engl. Backbone Area) OSPF-a je odgovorno za distribuiranje usmjerivačkih informacija između područja tj. sav promet koji povezuje

neka druga područja prolazi preko njega. Sva područja moraju biti povezana na područje okosnice i svaki usmjernik unutar područja okosnice zna topologiju cijele mreže.

Ako postoji veći broj usmjernika u nekom području mora se pronaći način kako optimalno razmijeniti podatke između njih. Kada bi svaki usmjernik slao podatke svim ostalima to bi stvorilo velik broj međusobnih veza i velik, nepotreban, promet. To se rješava proglašenjem **glavnog usmjernika** (engl. Designated Router - DR) i **pomoćnog glavnog usmjernika** (engl. Backup Designated Router - BDR) za svako OSPF područje mreže. Svaki usmjernik na tom području uspostavlja vezu samo prema DR-u i BDR-u, a oni preplavljuju (engl. flooding) mrežu podacima i šalju informacije svim ostalim usmjernicima.

DR i BDR se tijekom razmjena "Hello" poruka automatski proglašavaju ovisno o prioritetu svih usmjernika u mreži. Administrator može mijenjati prioritet, a kao DR i BDR uzimaju se oni usmjernici s boljim sklopovljem.

Format OSPF paketa je prikazan na slici:

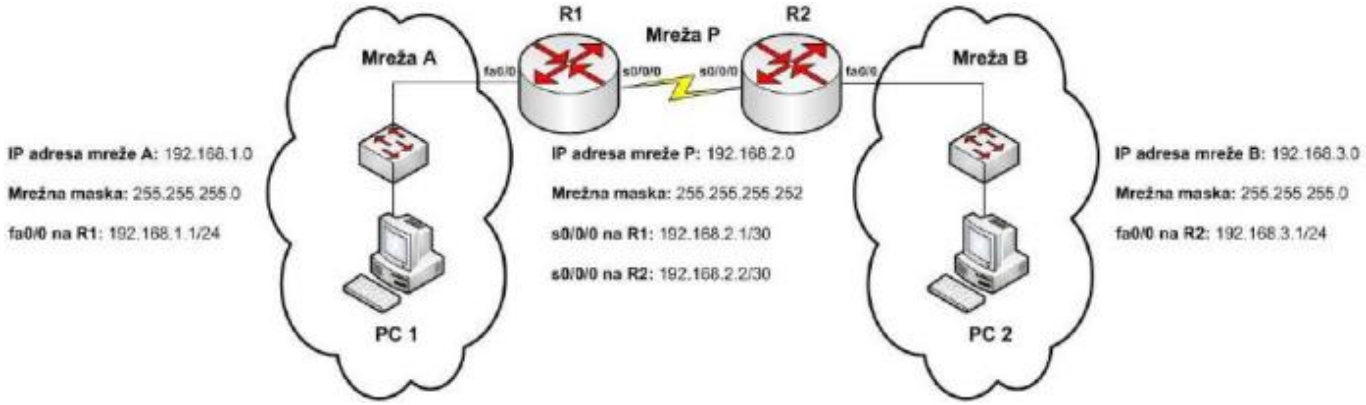
8	16	32bit
Version No.	Packet Type	Packet length
Router ID		
Area ID		
Checksum		AuType
Authentication (64 bits)		

Značenja polja su:

OSPF je dobar za srednje i velike mreže, minimalno opterećuje mrežu, omogućava praktički neograničen rast mreže, ali ima i nedostataka, neki od njih su:

Konfiguracija OSPF protokola na Cisco usmjerniku

Bit de prikazana konfiguracija OSPF protokola usmjeravanja na Cisco usmjerniku za mrežu prikazanu na slici:



Pretpostavljamo da su adrese dodijeljene po adresnoj shemi sa slike te da se nalazimo u privilegiranom načinu rada (engl. privileged mode). Privilegirani način rada je naznačen znakom "#".

Sada ćemo konfigurirati OSPF protokol na usmjerniku R1:

Naredbom router ospf 1 ulazimo u konfiguracijski način rada OSPF protokola i definiramo da će broj OSPF procesa biti 1 (na usmjerniku može biti više OSPF procesa).

Sada nizom network naredbi navodimo adrese svih mreža koje pripadaju usmjerniku R1, a nakon toga wildcard masku te OSPF područje kojemu pripada usmjernik.

Time je završena konfiguracija OSPF protokola na usmjerniku R1.

Analogno na usmjerniku R2 izvršimo sljedeći niz naredbi:

Time je završena konfiguracija OSPF protokola na usmjerniku R2.

Važno je napomenuti da usmjernici moraju biti u istom području da bi usmjeravali promet između mreža A i B.

Ako su na usmjerniku iskonfigurirani RIP i OSPF istovremeno koristit će se OSPF jer ima manju administrativnu distancu.

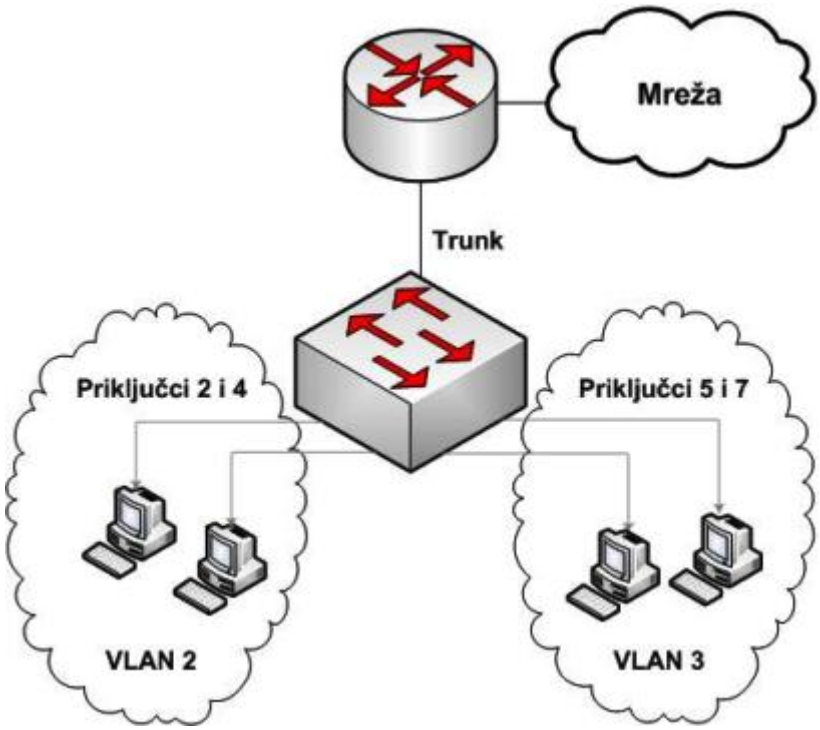
Virtualna lokalna mreža (engl. Virtual Local Area Network – VLAN) je način logičke segmentacije mreže koja se može dinamički mijenjati i nije ovisna o fizičkoj topologiji mreže. Tehnologija virtualnih lokalnih mreža je definirana standardom IEEE 802.1Q (poznat i kao dot1q).

VLAN predstavlja skupinu računala koji mogu biti u jednoj ili više odvojenih mreža, a koje su konfigurirane na način da im je omogućena međusobna komunikacija kao da se nalaze u istoj fizičkoj mreži.

Kada se ne koriste VLAN-ovi jedan prospojnik (engl. switch) je jedna domena prostiranja (engl. broadcast domain). Ako imamo veći broj korisnika, a to znači i veću domenu prostiranja postoji veća mogućnost tzv. broadcast storma koji može značajno narušiti performanse mreže. Dobro je povezati korisnike koji pripadaju istoj skupini i često komuniciraju (npr. rade isti posao), a bez uporabe VLAN-ova nemoguće je fizički udaljene skupine korisnika povezati u istu domenu.
Gledano sa sigurnosnog aspekta ako je veliki broj korisnika u istoj domeni postoji velika mogućnost napada ili krađe podataka.

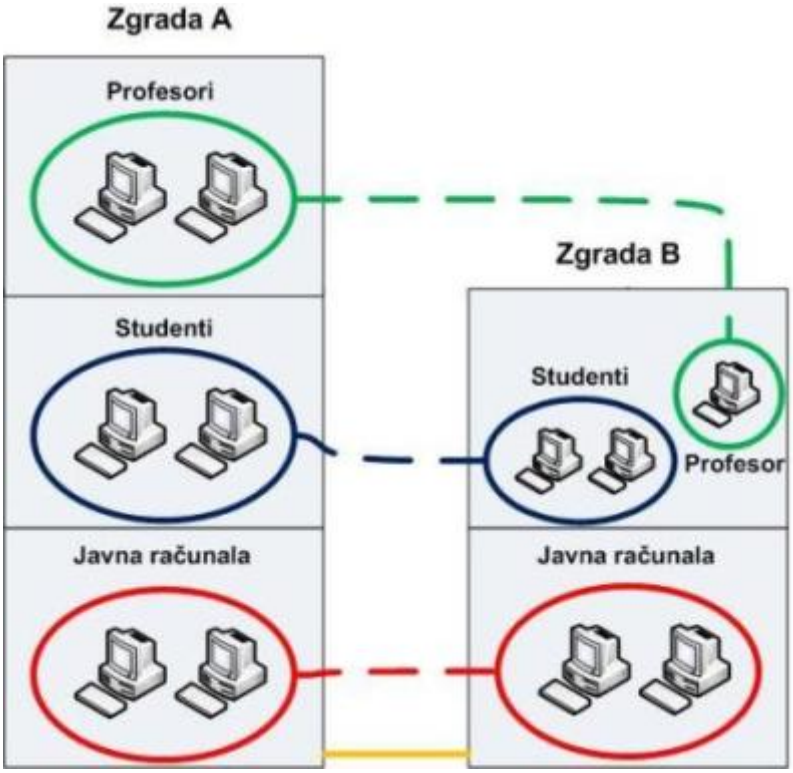
Zbog svega navedenog, poželjno je razdvojiti određenu vrstu korisnika i izolirati ju od ostalih, a za to se u današnjim računalnim mrežama koristi tehnologija virtualnih lokalnih mreža.

Koncept VLAN-ova prikazan je na slici:



Dobar primjer koji pokazuje opravdanost korištenja VLAN-ova je organizacija mreže fakulteta (prikazana na slici dolje). Profesori iz zgrada A i B su stavljeni u isti VLAN i tako odvojeni od studentskih i javnih računala. Dakle, iako su javna, studentska i računala profesora spojena na isti prospojnik, njihov promet je odvojen i praktički je nemoguće nekome iz jednog VLAN-a vidjeti promet

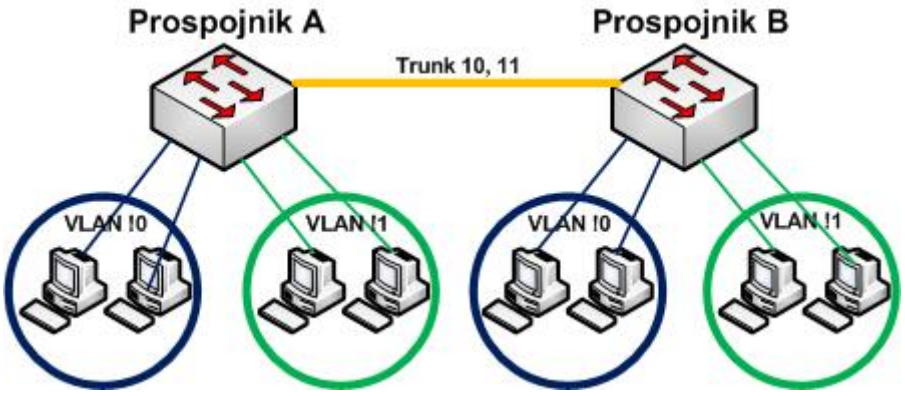
drugog VLAN-a (osim preko nekog uređaja mrežne razine što je objašnjeno kasnije u članku).



Povezivanje računala obavlja se konfiguracijom prospojnika. Priključci (engl. port) na prospojniku se u odgovarajući VLAN smještaju statički. Administrator mreže mora za svaki priključak odrediti pripadnost određenom VLAN-u.

Postoje dva tipa veza (priključaka):

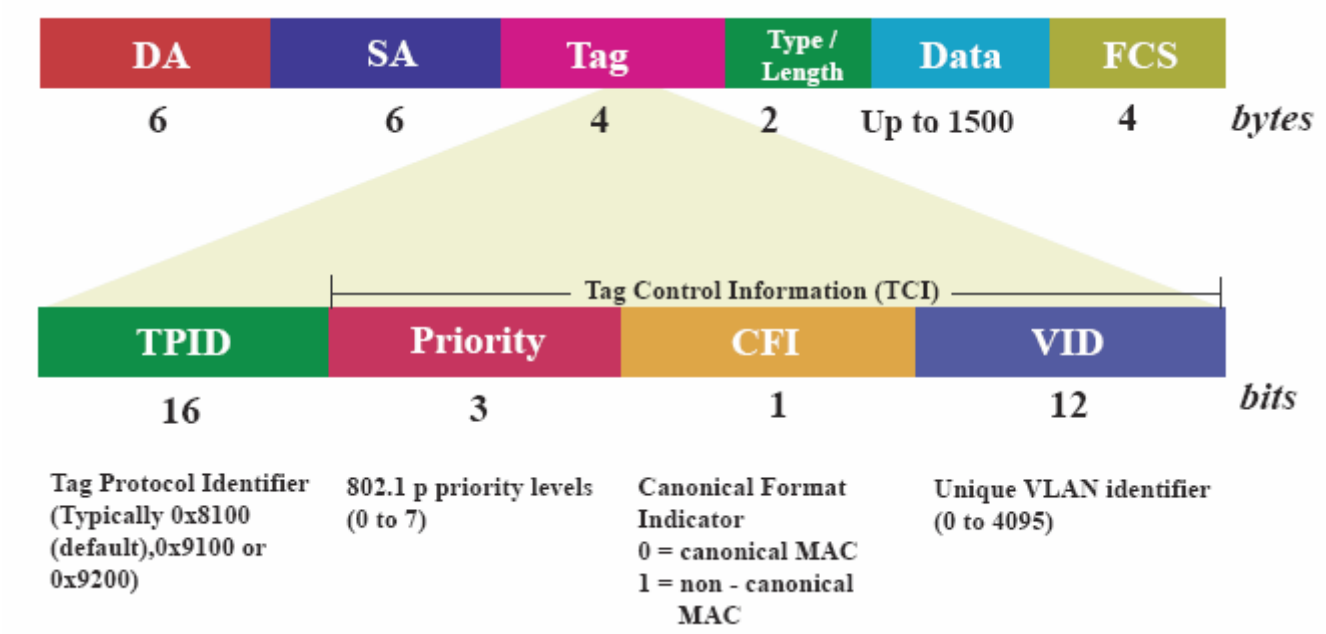
Trunk veza (engl. trunk link) je označena (engl. tagged) veza kojom se spajaju prospojnici međusobno ili prospojnik i usmjernik (engl. router). Kroz trunk veze se propušta promet na način da se točno zna koji promet je namijenjen kojem VLAN-u. Ovime npr. računala spojena na VLAN 10 prospojnika A i računala spojena na VLAN 10 prospojnika B mogu komunicirati međusobno kao da su u lokalnoj mreži. (slika dolje). Na trunk vezi mora se specificirati koji VLAN-ovi se propuštaju.



Access veza (engl. access link) je neoznačena (engl. untagged) veza na kojoj promet ulazi ili izlazi bez oznake VLAN-a. To su priključci prospojnika na koje se povezuju računala ili drugi uređaji. Ako se promet sa određenog access priključka šalje kroz trunk vezu tom prometu se dodaje oznaka (engl. tag) definiranog VLAN-a.

Priključci prospojnika koji se nalaze u različitim VLAN-ovima ne mogu komunicirati izravno, već im je za to potreban uređaj koji radi na mrežnoj (L3) razini (usmjernik ili L3 prospojnik).

Za razlikovanje pripadnosti određenog podatka nekom VLAN-u koristi se 802.1Q zaglavlje (engl. header) koje sadrži informaciju o oznaci VLAN-a. Svi podaci koji se šalju kroz trunk vezu šalju se sa ovakvim zaglavljem te se na odredištu u skladu s time prosljeđuju u odgovarajući VLAN. Format 802.1Q zaglavlja prikazan je na slici:



Kada se koristi L3 prospojnik on radi slično kao usmjernik tj. ima tablicu usmjeravanja, razdvaja domene prostiranja i prospaja promet između različitih VLAN-ova.

Postoje dvije vrste implementacije prospajanja na L3 razini:

Sklopovska implementacija – koristi se ASIC (application-specific integrated circuit) čip koji se brine o prospajanju.

Programska implementacija – koristi se CPU uređaja u kombinaciji s programskom podrškom.

Kada se koristi usmjernik sučelje usmjernika (engl. interface) treba podijeliti na onoliko podsučelja koliko postoji VLAN-ova. Svakom od tih virtualnih podsučelja se dodjeljuje IP adresa iz raspona pojedinog VLAN-a, a to je ujedno adresa predefiniranog izlaza (engl. default gateway) za taj VLAN. Osim adrese na podsučelju je potrebno definirati kojem VLAN-u pripada te koji trunking protokol koristi.

Konfiguracija VLAN-ova na Cisco prospojniku

VLAN-ovi 2 i 3 kreirani su ovim nizom naredbi:

Priključci prospojnika dodaju se u željeni VLAN ovim nizom naredbi:

Naredbom switchport mode access definirano je da je priključak kojeg konfiguriramo access tipa. Naredbom switchport access vlan 2 priključak kojeg konfiguriramo dodan je u VLAN 2.

Trunk priključak konfigurira se sljedećim nizom naredbi:

Naredbom switchport mode trunk definirano je da je priključak Gi0/1 trunk tipa.